CYTOMIC

Guía de administración Cytomic EPDR_

Aviso legal.

Marcas registradas.

Información de contacto.

Oficinas centrales:
Cytomic (Unidad de Negocio de Panda Security)
Calle Santiago de Compostela 12
Bilbao (Bizkaia) 48003 España.
https://www.pandasecurity.com/spain/about/contact/

Versión: 3.61.00-00

Autor: Cytomic

Fecha: 20/12/2019

Acerca de la Guía de administración de Cytomic EPDR

- Para obtener la versión más reciente de esta guía consulta la dirección web:

https://info.cytomicmodel.com/resources/guides/EPDR/latest/es/EPDR-guia-ES.pdf

- Para consultar un tema específico, accede a la guía online del producto en la dirección web:

https://info.cytomicmodel.com/resources/help/EPDR/latest/es/index.htm

Información sobre las novedades de la versión

Para conocer las novedades de la ultima versión de Cytomic EPDR consulta la siguiente URL:

https://info.cytomicmodel.com/releasenotes/?product=EPDR&lang=es

Información técnica sobre módulos y servicios compatibles con Cytomic EPDR.

- Para acceder a la Guía para el usuario de Cytomic Insights consulta la siguiente URL:

https://info.cytomicmodel.com/resources/guides/Insights/es/INSIGHTS-guia-ES.pdf

- Para acceder a la Guía para el usuario de Cytomic Data Watch consulta la siguiente URL:

https://info.cytomicmodel.com/resources/guides/DataWatch/es/DATAWATCH-guia-ES.pdf

- Para acceder a las guías de Cytomic SIEMConnect consulta las siguientes URLs:

https://info.cytomicmodel.com/resources/guides/SIEMConnect/es/SIEMCONNECT-Manual-ES.PDF

https://info.cytomicmodel.com/resources/guides/SIEMConnect/es/SIEMCONNECT-ManualDescripcionEventos-ES.pdf

Soporte técnico

Cytomic ofrece un soporte técnico global cuyo objetivo principal es responder a cuestiones especificas sobre el funcionamiento de sus productos. El equipo de soporte técnico también genera documentación sobre detalles técnicos del producto, que ofrece a través de su portal eKnowledge Base.

- Para acceder a información específica del producto consulta la siguiente URL:

https://www.pandasecurity.com/spain/support/adaptive-defense-360-aether.htm

- Para acceder al portal eKnowledge Base consulta la siguiente URL:

https://www.pandasecurity.com/spain/support/#enterprise

Encuesta sobre la Guía de administración de Cytomic EPDR

Evalúa esta guía para administradores y enviamos sugerencias y peticiones para próximas versiones de la documentación en:

https://es.surveymonkey.com/r/feedbackEPDRGuideES

Tabla de contenidos

Parte 1: Introducción a Cytomic EPDR

Parte 2: La consola web de administración

Parte 8: Información complementaria sobre Cytomic EPDR

Parte 1

Introducción a Cytomic EPDR

Capítulo 1

Prólogo

La Guía de administración contiene información básica y procedimientos de uso para obtener el máximo beneficio del producto Cytomic EPDR.

CONTENIDO DEL CAPÍTULO

¿A quién está dirigida esta guía?

Esta documentación está dirigida a los administradores de red que gestionan la seguridad informática de su organización.

Para interpretar correctamente la información ofrecida por el producto y extraer conclusiones que ayuden a fortalecer la seguridad de su empresa son necesarios conocimientos técnicos sobre entornos Windows a nivel de procesos, sistema de ficheros y registro, así como entender los protocolos de red utilizados con mayor frecuencia.

¿Que es Cytomic EPDR?

Cytomic EPDR es un servicio gestionado que protege los equipos informáticos de las empresas, acota el alcance de los problemas de seguridad encontrados y ayuda a establecer planes de respuesta y prevención frente a las amenazas desconocidas y a los ataques dirigidos avanzados (APTs).

Cytomic EPDR está dividido en dos áreas funcionales bien diferenciadas:

- Cytomic EPDR
- Plataforma Cytomic

Cytomic EPDR

Es el producto que implementa todas las características orientadas a garantizar la seguridad de los puestos de usuario y servidores, sin requerir la intervención del administrador de la red.

Plataforma Cytomic

Es el ecosistema donde se ejecutan los productos de Cytomic. Cytomic entrega en tiempo real, de forma ordenada y con un gran nivel de detalle toda la información generada por Cytomic EPDR sobre los procesos, los programas ejecutados por los usuarios y los dispositivos que pertenecen a la infraestructura IT de las organizaciones.

Cytomic es una plataforma eficiente, extensible y escalable, diseñada para cubrir las necesidades de la gran cuenta y de MSPs.

Iconos

En esta guía se utilizan los siguientes iconos;

Aclaraciones e información adicional, como, por ejemplo, un método alternativo para realizar una determinada tarea.

Sugerencias y recomendaciones.

Consejo importante de cara a un uso correcto de las opciones de Cytomic EPDR.

Consulta en otro capítulo o punto del manual.

Capítulo 2

Información básica de Cytomic EPDR

Cytomic EPDR es una solución completa de seguridad para puestos de usuario y servidores, formada por múltiples tecnologías que ofrecen a los clientes un completo servicio de protección contra el malware, sin necesidad de instalar, gestionar o mantener nuevos recursos hardware en la infraestructura de la organización.

CONTENIDO DEL CAPÍTULO

Beneficios de Cytomic EPDR

Cytomic EPDR es una solución basada en múltiples tecnologías de protección que permite sustituir el producto de antivirus tradicional por un completo servicio de seguridad gestionada.

Ejecución de software lícito

Cytomic EPDR supervisa y clasifica todos los procesos ejecutados en el parque informático en base a su comportamiento y naturaleza. Gracias a este servicio los puestos de usuario y servidores son protegidos limitando la ejecución de los programas instalados a aquellos que han sido previamente certificados como seguros.

Adaptación al entorno de la empresa

A diferencia de los antivirus tradicionales, Cytomic EPDR utiliza un nuevo concepto de seguridad que le permite adaptarse con precisión al entorno particular de cada empresa. Para ello, supervisa la ejecución de todas las aplicaciones y aprende constantemente de las acciones desencadenadas por los procesos lanzados en los puestos de usuario y servidores.

Tras un breve periodo de aprendizaje, Cytomic EPDR es capaz de ofrecer un nivel de protección muy superior al de un antivirus tradicional.

Alcance y solución de problemas de seguridad

La oferta de seguridad se completa con herramientas monitorización, análisis forense y resolución, que acotan el alcance de los problemas detectados y los solucionan.

La monitorización aporta datos valiosos sobre el contexto en el que se sucedieron los problemas de seguridad. Con esta información, el administrador podrá determinar el alcance de los incidentes e implantar las medidas necesarias para evitar que vuelvan a producirse.

Multiplataforma

Cytomic EPDR es un servicio multiplataforma alojado en la nube y compatible con Windows, macOS, Linux, Android y con entornos virtuales y VDI, tanto persistentes como no persistentes. Por esta razón es suficiente una única herramienta para cubrir la seguridad de todos los equipos de la empresa.

Cytomic EPDR no necesita nueva infraestructura IT en la empresa para su gestión y mantenimiento, y por esta razón reduce el TCO de la solución a niveles muy bajos.

Características de Cytomic EPDR

Cytomic EPDR ofrece un servicio de seguridad garantizada frente a amenazas y ataques avanzados dirigidos a las empresas a través de cuatro pilares:

Figura 2.1: Los cuatro pilares de la protección avanzada de Cytomic EPDR

- **Visibilidad**: trazabilidad de cada acción realizada por las aplicaciones en ejecución.
- **Detección**: monitorización constante de los procesos en ejecución y bloqueo en tiempo real de ataques *Zero-day*, ataques dirigidos y otras amenazas avanzadas, diseñadas para pasar desapercibidas a los antivirus tradicionales.
- **Resolución y Respuesta:** información forense para investigar en profundidad cada intento de ataque, y herramientas de mitigan sus efectos.
- **Prevención**: evita futuros ataques modificando la configuración de los distintos módulos de protección y parcheando las vulnerabilidades de los sistemas operativos y de las aplicaciones instaladas.

Características de la plataforma Cytomic

Cytomic es la nueva plataforma de gestión, comunicación y tratamiento de la información desarrollada por Cytomic, que agrupa y centraliza los servicios comunes a todos sus productos.

La plataforma Cytomic gestiona las comunicaciones con los agentes desplegados en los equipos protegidos de los clientes, y presenta en la consola de administración, de forma ordenada y comprensible, toda la información recogida por Cytomic EPDR para su posterior análisis por parte del administrador de la red.

Este diseño modular de la solución evita la instalación de nuevos agentes o productos en los equipos del cliente por cada módulo adicional contratado. Todos los productos de Cytomic que funcionan sobre la plataforma Cytomic comparten un mismo agente en el equipo del usuario y una misma consola web de administración, facilitando su gestión y minimizando los recursos de los equipos.

Principales beneficios de Cytomic

A continuación, se presentan los principales servicios ofrecidos por Cytomic para todos los productos de Cytomic que sean compatibles con la plataforma:

Plataforma de gestión Cloud

Cytomic es una plataforma que reside en la nube, incorporando importantes ventajas de cara a su manejo, funcionalidad y accesibilidad:

- No requiere servidores de gestión que alojen la consola de administración en las instalaciones del cliente: al funcionar desde la nube, es directamente accesible por todos los equipos suscritos al servicio, desde cualquier lugar y en cualquier momento, sin importar si están dentro de la oficina o desplazados.
- El administrador de la red puede acceder a la consola de administración desde cualquier momento y en cualquier lugar, simplemente con un navegador compatible desde un equipo portátil, un equipo de sobremesa o incluso un dispositivo móvil como una tablet o un smartphone.
- Es una plataforma ofrecida en régimen de alta disponibilidad, operativa el 99'99% del tiempo. El administrador de la red queda liberado de diseñar y desplegar costosos sistemas en redundancia para alojar las herramientas de gestión.

Comunicación con la plataforma en tiempo real

El envío de configuraciones y tareas programadas desde y hacia los equipos de la red se realiza en tiempo real, en el momento en que el administrador aplica la nueva configuración a los dispositivos seleccionados. El administrador puede ajustar los parámetros de la seguridad de forma casi instantánea para solucionar posibles brechas de seguridad o adaptar el servicio de seguridad al constante cambio de la infraestructura informática de las empresas.

Multi producto y Multiplataforma

La integración de los productos de Cytomic en una misma plataforma ofrece las siguientes ventajas al administrador:

- **Minimiza la curva de aprendizaje**: todos los productos comparten una misma consola, de esta forma se minimiza el tiempo que el administrador requiere para aprender el manejo de una nueva herramienta, redundando en menores costes de TCO.
- **Único despliegue para múltiples productos**: solo es necesario un único programa instalado en cada equipo para ofrecer la funcionalidad de todos los productos compatibles con Cytomic Platform. De esta forma se minimizan los recursos utilizados en los equipos de los usuarios en comparación con la utilización de productos independientes.
- **Mayores sinergias entre productos**: todos los productos reportan en una misma consola: el administrador dispone de un único panel de control donde observa toda la información generada, minimizando el tiempo y el esfuerzo invertido en mantener varios repositorios de información independientes y en consolidar la información generada en fuentes distribuidas.
- **Compatible con múltiples plataformas**: no es necesario contratar distintos productos para cubrir todo el espectro de dispositivos de la compañía: Cytomic Platform funciona para Windows, Linux, macOS y Android, además de entornos virtuales y VDI tanto persistentes como no persistentes.

Configuraciones flexibles y granulares

El nuevo modelo de configuración permite acelerar la gestión de los equipos mediante la reutilización de configuraciones, haciendo uso de mecanismos específicos como la herencia y la asignación de configuraciones a equipos individuales. El administrador de la red podrá asignar configuraciones mucho más específicas y con menor esfuerzo.

Información completa y a medida

Cytomic Platform implementa mecanismos que permiten configurar la cantidad de datos mostrados a lo largo de una amplia selección de informes, según las necesidades del administrador o del consumidor final de la información.

La información se completa además con datos sobre los equipos, hardware y software instalado, así como un registro de cambios, que ayudarán al administrador a valorar el estado de la seguridad del parque informático administrado.

Arquitectura de Cytomic

La arquitectura de Cytomic está diseñada de forma escalable para ofrecer un servicio flexible y eficiente. La información se envía y se recibe en tiempo real desde / hacia múltiples fuentes y destinos de forma simultánea. Los orígenes y destinos pueden ser equipos vinculados al servicio, consumidores externos de información como sistemas SIEM o servidores de correo, instancias web para las peticiones de cambios de configuración y presentación de información de los administradores de red, entre otros.

Además, Cytomic implementa un backed y una capa de almacenamiento que utiliza una amplia variedad de tecnologías que le permite manipular los múltiples tipos de datos de forma ágil.

En la figura 2.2 se presenta un diagrama a alto nivel de Cytomic Platform.

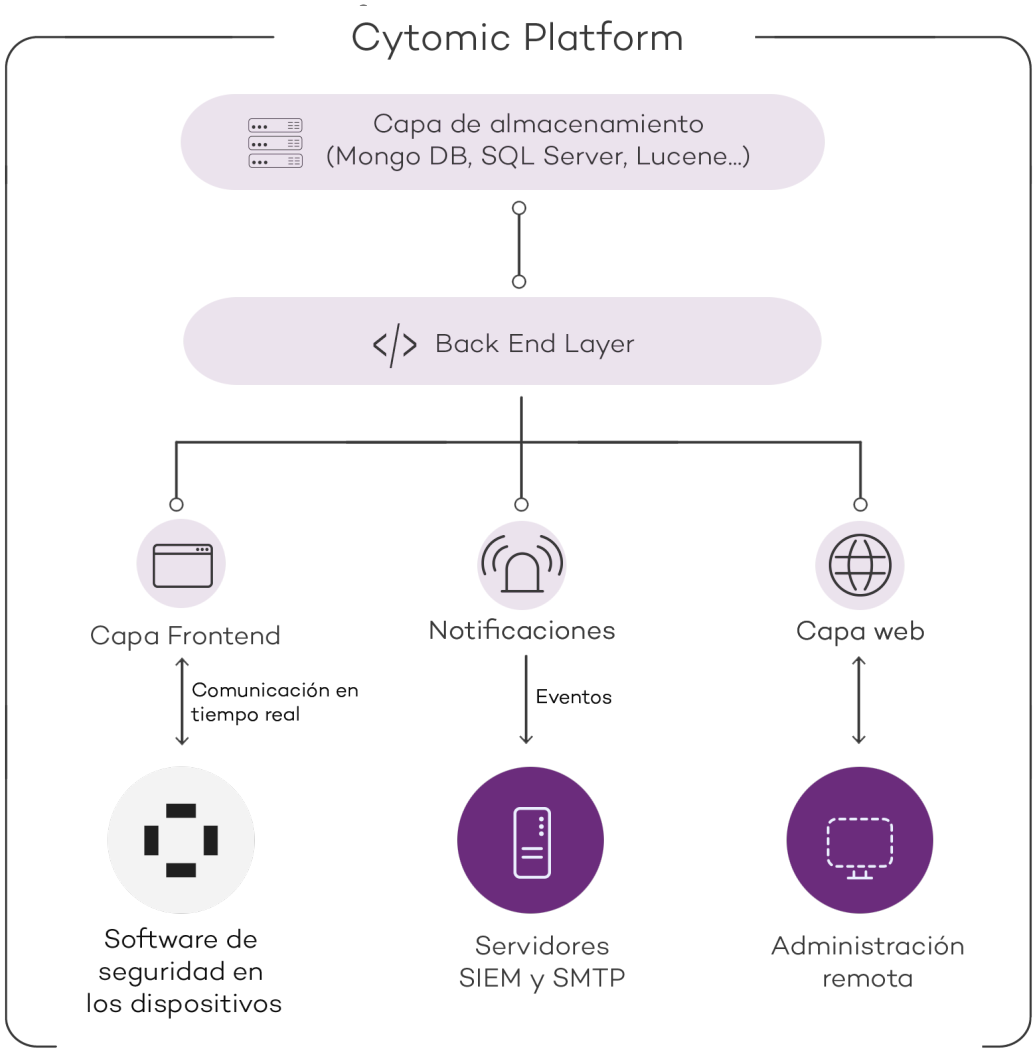


Figura 2.2: estructura lógica de la plataforma Cytomic

Cytomic en los equipos de usuario

Los equipos de la red protegidos con Cytomic EPDR llevan instalado un software, formado por dos módulos independientes pero relacionados, que aportan toda la funcionalidad de protección y gestión:

- **Módulo Agente de comunicaciones Cytomic (agente Cytomic)**: es el encargado de servir de puente entre el módulo de protección y la nube, gestionando las comunicaciones, eventos y configuraciones de seguridad implementadas por el administrador desde la consola de administración.
- **Módulo Protección Cytomic EPDR**: es el encargado de proteger de forma efectiva el equipo del usuario. Para ello se sirve del agente de comunicaciones para recibir las configuraciones y emite estadísticas y datos de las detecciones y elementos analizado.

Agente de comunicaciones en tiempo real Cytomic

El agente Cytomic se encarga de las comunicaciones entre los equipos administrados y el servidor de Cytomic EPDR, y de establecer un diálogo entre los equipos que pertenecen a una misma red del cliente.

Este módulo también gestiona los procesos de la solución de seguridad y recoge los cambios de configuración que el administrador haya realizado a través de la consola Web, aplicándolos sobre el módulo de protección.

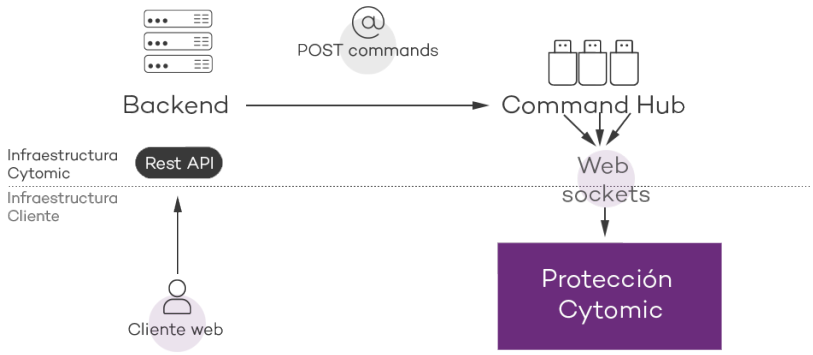


Figura 2.3: recorrido de los comandos introducidos con la consola de administración

La comunicación entre los dispositivos y el Command Hub se implementa mediante conexiones websockets persistentes y en tiempo real, estableciendo una conexión por cada uno de los equipos para el envío y recepción de datos. Para evitar que dispositivos intermedios provoquen el cierre de las conexiones, se genera un flujo de keepalives constante.

Las configuraciones establecidas por el administrador de la red mediante la consola de administración Cytomic EPDR se envían mediante una API REST al backend; éste las reenvía al Command hub generando un comando POST, el cual finalmente ejecuta un push de la información a todos los dispositivos suscritos. Con un buen funcionamiento de las líneas de comunicación, los equipos recibirán la configuración en tiempo real.

Componentes principales

Cytomic EPDR es un servicio de seguridad que se apoya en el análisis del comportamiento de los procesos ejecutados en el parque de cada cliente. En este análisis se aplican técnicas de Machine Learning en infraestructuras Big Data alojadas en la nube.

La figura **2.4** representa el esquema general de Cytomic EPDR y los componentes que lo forman:

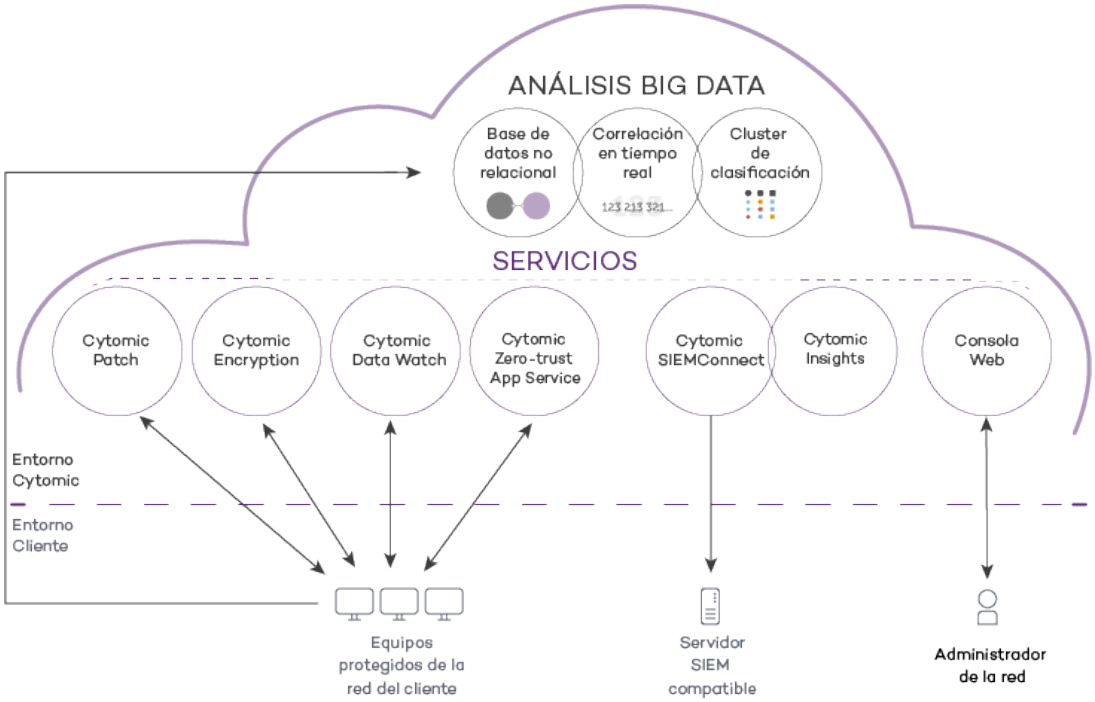


Figura 2.4: esquema general Cytomic EPDR

- **Infraestructura de análisis big data**, formada por bases de datos no relacionales, servicios de correlación de eventos monitorizados en tiempo real y un cluster de clasificación de los procesos monitorizados.
- **Servicio Zero-trust Application Service**: clasifica todos los procesos ejecutados sin ambigüedades ni falsos positivos ni negativos.
- **Cytomic SIEMConnect (opcional)**: integra Cytomic EPDR con soluciones SIEM de proveedores externos.
- **Servicio Cytomic Data Watch (opcional)**: servicio de visibilidad, inventario y supervisión de la información personal que almacenan los ficheros PII.
- **Servicio Cytomic Insights (opcional)**: servicio de informes para generar inteligencia de seguridad avanzada.
- **Servicio Cytomic Patch (opcional)**: parcheo de sistemas operativos Windows y aplicaciones de terceros.
- **Servicio Cytomic Encryption (opcional)**: cifra los dispositivos de almacenamiento interno de los equipos Windows para minimizar la exposición de datos en caso de perdida o robo, o al desechar dispositivos de almacenamiento sin borrar completamente su contenido.
- **Consola web**: servidor de la consola de administración.
- **Servidor SIEM** de la empresa (opcional).
- Equipos protegidos mediante el software Cytomic EPDR instalado.

- Equipo del administrador de red que accede a la consola Web.

Infraestructura de análisis Big Data

Es el clúster de servidores en la nube que recibe todas las acciones ejecutadas por los programas del usuario y monitorizadas por el módulo de protección instalado en los equipos del cliente. Mediante técnicas de inteligencia artificial evalúa el comportamiento de dichos programas y emite una clasificación por cada proceso en ejecución. Esta clasificación se devuelve al módulo de protección en el equipo, y se toma como base para ejecutar las acciones configuradas por el administrador, con el objetivo de mantener el equipo protegido.

El clúster de Cytomic EPDR está formado por una granja de servidores alojada en la nube que forma un entorno de explotación Big Data. En este entorno se aplican de forma continua una mezcla de tecnologías basadas en algoritmos Machine Learning. Estos algoritmos clasifican los programas ejecutados tomando sus atributos estáticos, su información de contexto de ejecución y las acciones de los procesos monitorizados ejecutados en los equipos de los usuarios.

Las ventajas de este nuevo modelo de análisis de procesos frente al adoptado por los antivirus tradicionales basados en el envío de muestras al proveedor y análisis manual son:

- Todos los procesos de los equipos protegidos son monitorizados y analizados: se elimina la incertidumbre de los antivirus tradicionales, capaces únicamente de reconocer el malware sin considerar el resto de aplicaciones.
- El retraso en la clasificación de los procesos vistos por primera vez (ventana de oportunidad) es mínimo ya que Cytomic EPDR envía en tiempo real las acciones que ejecuta cada proceso. Los servidores en la nube trabajan de forma constante con esta información, disminuyendo de manera sustancial el tiempo necesario para emitir una clasificación, y por tanto el tiempo de exposición a las amenazas.
- La monitorización continúa de cada proceso permite a Cytomic EPDR clasificar como malware elementos que inicialmente eran considerados goodware. Este cambio de comportamiento es muy habitual en los ataques dirigidos y otras amenazas avanzadas diseñadas para operar por debajo del radar.
- El análisis en la nube libera al cliente de instalar y mantener infraestructura de hardware y software junto al pago de licencias y la gestión de garantías del hardware, con lo que el TCO de la solución desciende significativamente.

Servidor Web de la consola de administración

Toda la gestión de Cytomic EPDR se realiza a través de la consola Web accesible para el administrador desde la URL **https://manage.cytomicmodel.com**

La consola Web es compatible con los navegadores más comunes y es accesible desde cualquier lugar y en cualquier momento con cualquier dispositivo que tenga instalado un navegador compatible.

*Para verificar si tu navegador es compatible con el servicio consulta el apartado "***Acceso a la consola web***" en la página* **520**.

La consola Web es "responsive", de modo que se puede utilizar sin problemas desde móviles y tablets.

Equipos protegidos con Cytomic EPDR

Cytomic EPDR requiere de la instalación de un componente software en todas las máquinas del parque informático susceptibles de sufrir problemas de seguridad. Este componente está formado por dos módulos: el agente de comunicaciones Cytomic y el módulo de la protección Cytomic EPDR.

Cytomic EPDR se instala sin problemas en máquinas con otras soluciones de seguridad de la competencia.

El módulo de la protección Cytomic EPDR contiene las tecnologías encargadas de proteger los equipos del cliente. Cytomic EPDR reúne en un mismo producto todos los recursos necesarios para detectar el malware de nueva generación y ataques dirigidos (APT), al tiempo que incorpora herramientas de gestión de la productividad y de resolución para desinfectar los equipos comprometidos y determinar el alcance de los intentos de intrusión en la red del cliente.

Servicios Cytomic EPDR

Cytomic ofrece otros servicios, algunos de carácter opcional, que integran la solución con la infraestructura IT del cliente, y obtener de forma directa la inteligencia de seguridad generada en los laboratorios de Cytomic.

Servicio Zero-trust Application Service

Este servicio incluido por defecto en el producto tiene como objetivo permitir la ejecución únicamente de los programas certificados por Cytomic. Para conseguirlo, se utiliza una mezcla de tecnologías locales en el equipo del usuario y en la infraestructura de análisis big data que clasifican de forma automática el 99'08% de los procesos ejecutados. Para el resto de procesos se aplican clasificaciones manuales ejecutadas por expertos en malware. Con este enfoque se consiguen clasificar el 100% de los binarios ejecutados en los equipos de los clientes sin falsos positivos ni negativos.

Los ficheros ejecutables encontrados en el equipo del usuario y desconocidos para la plataforma se envían de forma automática a la infraestructura de análisis big data para su análisis.

Los ficheros desconocidos se envían una sola vez para todos los clientes que usan Cytomic EPDR, por lo tanto, el impacto en el rendimiento de la red del cliente es prácticamente nulo. Además, se han implementado mecanismos de gestión del ancho de banda y límites por equipo y hora.

Servicio Cytomic Insights (opcional)

Cytomic EPDR envía de forma automática y transparente toda la información recogida de los equipos de usuario al servicio Cytomic Insights, un sistema de almacenamiento y explotación del conocimiento.

Las acciones de los procesos ejecutados en el parque de IT se envían a Cytomic Insights donde se estudian y relacionan para extraer inteligencia de seguridad. El administrador dispondrá de información adicional sobre las amenazas y sobre el uso que los usuarios dan a los equipos de la empresa. Esta nueva información se presenta de forma flexible y visual para favorecer su comprensión.

El servicio Cytomic Insights es accesible directamente desde el panel de control de la propia consola Web de Cytomic EPDR.

Consulta la Guía de usuario Cytomic Insights accesible desde la web de producto para configurar y sacar provecho del servicio de análisis de conocimiento y búsquedas avanzadas.

Servicio Cytomic SIEMConnect (opcional)

Cytomic EPDR se integra con las soluciones SIEM de proveedores externos implementadas por los clientes en sus infraestructuras de IT. La actividad de las aplicaciones que se ejecutan en el parque informático se entrega al servidor al SIEM, ampliada con todo el conocimiento ofrecido por Cytomic EPDR, y lista para ser utilizada.

A continuación, se listan los sistemas SIEM compatibles con Cytomic EPDR:

- QRadar
- AlienVault
- ArcSight
- LookWise

- Bitacora

Consulta la Guía de usuario Cytomic SIEMConnect para una descripción detallada de la información recogida por Cytomic EPDR y enviada al sistema SIEM del cliente.

Servicio Cytomic Data Watch (opcional)

Es un módulo de seguridad integrado en la plataforma Cytomic EPDR que ayuda a cumplir con las regulaciones en materia de retención de datos personales (PII) almacenados en la infraestructura IT de las empresas.

Cytomic Data Watch descubre, audita y monitoriza en tiempo real el ciclo de vida completo de los ficheros PII: desde datos en reposo, las operaciones efectuadas sobre ellos y su transferencia al exterior. Con esta información, Cytomic Data Watch genera un inventario por cada equipo de la red que permite mostrar la evolución de los ficheros que contienen información personal.

*Consulta el capítulo "**Cytomic Data Watch (Supervisión de información sensible)**" en la página **255** para una descripción detallada del servicio.*

Servicio Cytomic Patch (opcional)

Este servicio reduce la superficie de ataque de los puestos de usuario y servidores Windows actualizando el software vulnerable (sistemas operativos y aplicaciones de terceros) con los parches publicados por los proveedores correspondientes.

Además, permite localizar los programas que han entrado en EoL (End Of Life) considerados peligrosos por no tener mantenimiento de su proveedor original y ser el blanco de los hackers que aprovechan las vulnerabilidades conocidas y sin corregir. El administrador puede localizar con facilidad todos los programas en EoL y planificar una sustitución controlada de los mismos.

En caso de incompatibilidades o mal funcionamiento de las aplicaciones parcheadas, Cytomic Patch permite ejecutar un Rollback / desinstalación de los parches que lo permitan o excluirlos previamente para evitar su instalación.

Servicio Cytomic Encryption (opcional)

El cifrado de la información contenida en los dispositivos de almacenamiento interno de los equipos es un recuso fundamental a la hora de proteger los datos que contienen en caso de robo o pérdida y cuando la empresa recicla dispositivos de almacenamiento sin borrar completamente. Cytomic EPDR utiliza la tecnología BitLocker para cifrar el contenido de los discos duros a nivel de sector y gestiona de forma centralizada las claves de recuperación en caso de pérdida o cambio de configuración de hardware.

El módulo Cytomic Encryption permite utilizar el modulo de plataforma segura TPM si está disponible, y ofrece varias configuraciones de autenticación para añadir flexibilidad a la protección de los datos contenidos en el equipo.

Perfil de usuario del producto

Aunque Cytomic EPDR es un servicio gestionado que ofrece seguridad sin intervención del administrador de la red, también provee información muy detallada y comprensible sobre la actividad de los procesos ejecutados por los usuarios en toda la infraestructura de IT de la empresa. Esta información puede ser utilizada por el administrador para precisar el impacto de problemas de seguridad y adaptar sus protocolos, evitando así la repetición de situaciones similares en el futuro.

Dispositivos e idiomas soportados

*Para una descripción detallada de las plataformas y requisitos consulta el capítulo "**Requisitos de hardware, software y red**" en la página **515**.*

Compatibilidad con sistemas operativos

- Windows Workstation
- Windows Server
- Sistemas virtuales y VDI persistentes y no persistentes
- macOS
- Linux
- Tablets y móviles Android

Compatibilidad con navegadores web

La consola de administración es compatible con las últimas versiones de los navegadores mostrados a continuación:

- Chrome
- Internet Explorer
- Microsoft Edge
- Firefox
- Opera

Idiomas soportados en la consola web

- Español
- Inglés
- Sueco
- Francés
- Italiano
- Alemán
- Portugués
- Húngaro
- Ruso
- Japonés
- Finlandés (solo consola local)

Capítulo 3

El ciclo de protección adaptativa

El malware de nueva generación está enfocado en pasar inadvertido dentro de los sistemas informáticos durante largos periodos de tiempo para poder obtener beneficios económicos de las empresas. El ciclo de protección adaptativa es el nuevo paradigma que surge en respuesta a esta evolución. Cytomic EPDR implementa los recursos necesarios para detectar y proteger a las empresas de estas nuevas amenazas, así como resolver los problemas ocasionados y adaptar la estrategia de seguridad para evitar infecciones futuras.

CONTENIDO DEL CAPÍTULO

Las nuevas necesidades de seguridad

En la actualidad se generan más de 200.000 nuevos virus diariamente, una parte muy sustancial de ellos diseñados para ejecutarse en los equipos de los usuarios durante periodos de tiempo alargados y en segundo plano, sin dar muestras de su existencia.

Esta nueva estrategia del malware está volviendo gradualmente ineficiente el enfoque tradicional de protección mediante archivos de identificadores locales o en la nube: el creciente número de malware desarrollado puede considerarse en si mismo un ataque global por fuerza bruta a los proveedores de seguridad, que busca ampliar la ventana de oportunidad sobrepasando los recursos que éstos dedican a analizar el malware. Por esta razón, la media de tiempo transcurrido desde que el primer equipo es infectado a nivel mundial hasta que los proveedores de seguridad son conscientes de este nuevo malware y consiguen identificarlo es cada vez mayor. Alimentar los archivos de identificadores y desplegarlos en los equipos de los usuarios incrementa todavía mas el tiempo total de exposición, especialmente en aquellos proveedores que todavía confían la seguridad de sus clientes en los ficheros de firmas y no han migrado su inteligencia de seguridad a la nube.

Con esta nueva situación, la estrategia de seguridad a adoptar pasa por minimizar el tiempo de exposición al malware, exposición estimada actualmente en 259 días para ataques dirigidos, cada vez más frecuentes y que tienen como principales objetivos el robo de datos y el espionaje industrial.

Cytomic EPDR propone un nuevo enfoque de seguridad basado en el ciclo de protección adaptativa: un conjunto de servicios de protección, detección, monitorización, análisis forense y resolución. Todos los servicios están integrados y centralizadas en una única consola Web de administración para mostrar el ciclo completo en tiempo real.

Con este nuevo enfoque se evitan o minimizan al máximo las brechas de seguridad, reduciendo de forma drástica las pérdidas de productividad y el riesgo de robo de información confidencial en las empresas; el administrador es liberado de la compleja tarea de determinar qué es peligroso y por qué razón, recuperando espacio y recursos para gestionar y vigilar el estado de la seguridad.

El departamento de IT podrá tomar decisiones que permitan adaptar la política de seguridad de la empresa con la misma agilidad que mutan los patrones de ataque del malware avanzado.

El ciclo de protección adaptativa

El objetivo de Cytomic EPDR es el de facilitar al departamento de IT la creación de un espacio donde definir y establecer las políticas de seguridad de la empresa que respondan rápida y adecuadamente a los nuevos tipos de amenazas.

Este espacio es producto, por una parte, de la liberación de responsabilidades del equipo técnico en la compañía a la hora de decidir qué ficheros son seguros y cuales son peligrosos, y por qué motivo: **con Cytomic EPDR el departamento técnico de la empresa recibirá una clasificación sin ambigüedades de absolutamente todos los programas ejecutados en el parque informático gestionado.**

Por otra parte, el departamento de IT también recibirá un conjunto de herramientas para la visualización del estado de la seguridad, la resolución de los problemas ocasionados por el malware avanzado y el estudio de forma detallada del comportamiento de APTs y otras amenazas.

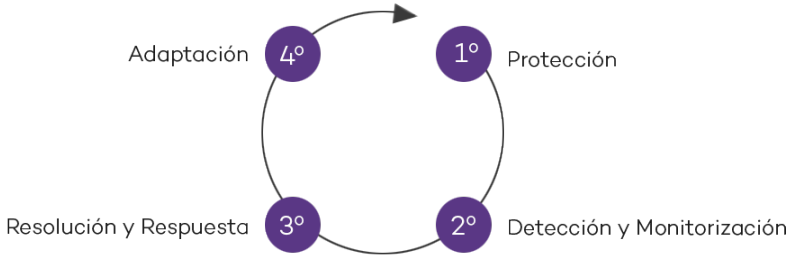


Figura 3.1: el ciclo de protección adaptativa

Con toda esta información y herramientas, el administrador podrá cerrar el ciclo completo de la seguridad en la empresa: monitorizar el estado del parque informático gestionado, en caso de producirse brechas de seguridad revertir los equipos afectados a una situación previa, y conocer el alcance de aquellas para poder implementar las medidas de contingencia apropiadas. Todo este ciclo encaja dentro de un proceso de refinamiento contante, que resultará en un entorno informático seguro, flexible y productivo para los usuarios de la empresa.

Este ciclo constante de protección adaptativa implementado por las empresas con ayuda de Cytomic EPDR se puede resumir en la figura 3.1.

Fase I: Protección completa del parque informático

La primera fase del ciclo de protección adaptativa incluye las herramientas necesarias para proteger y defender de forma efectiva el parque informático de ataques e intentos de infección.

Protección antivirus permanente e inteligencia colectiva

La protección antivirus permanente es el módulo de seguridad tradicional que cubre los vectores de infección más utilizados por los hackers. Se alimenta tanto del archivo de identificadores publicado por Cytomic para su descarga en local como del acceso en tiempo real a la Inteligencia Colectiva.

En el contexto actual de crecimiento continuo del malware, los servicios alojados en la nube han cobrado especial importancia frente a las actualizaciones del fichero de firmas local. Por esta razón, la protección de antivirus de Cytomic EPDR se basa fundamentalmente en la Inteligencia Colectiva,

una plataforma de conocimiento en la nube que aumenta exponencialmente la capacidad de detección.

Esta plataforma consta de servidores que clasifican y procesan de forma automática toda la información que la comunidad de usuarios proporciona sobre las detecciones que se han producido en sus equipos. La protección Cytomic EPDR instalada en los equipos consulta a la Inteligencia Colectiva cuando lo necesita, consiguiendo así maximizar su capacidad de detección y sin afectar negativamente al consumo de recursos.

Cuando se detecta un nuevo ejemplar de malware en el equipo de un miembro de la comunidad de usuarios, Cytomic EPDR envía la información a los servidores de Inteligencia Colectiva alojados en la nube, de forma automática y anónima. Esta información es procesada para generar una solución no sólo al usuario afectado, sino también al resto de usuarios de la comunidad, en tiempo real.

Cytomic EPDR utiliza la Inteligencia Colectiva para aumentar la capacidad de detección y evitar penalizaciones en el rendimiento del equipo del cliente. Todo el conocimiento está en la nube y todos los usuarios pueden beneficiarse de ello.

*Para más información sobre el servicio de antivirus de Cytomic EPDR en plataformas Windows consulta el capítulo "***Configuración de estaciones y servidores***" en la página* **225**.

*Para más información sobre el servicio de antivirus de Cytomic EPDR en plataformas Android consulta el capítulo "***Configuración de seguridad Android***" en la página* **251**.

Protección contra técnicas de ocultación y virus de macro

Al margen de la estrategia tradicional de detección que compara el payload del fichero objeto de estudio con el contenido en el fichero de firmas, Cytomic EPDR implementa varios motores de detección que analizan el comportamiento de los procesos de forma local.

De esta manera, se detectan comportamientos extraños en los principales motores de scripting (Visual basic Script, Javascript y Powershell) incorporados en todos los sistemas Windows actuales y en macros maliciosas embebidas en ficheros ofimáticos como Word, Excel, PowerPoint etc.

Como complemento, se incorporan además los tradicionales motores heurísticos y de detección de ficheros maliciosos por características estáticas.

Bloqueo de programas

Para incrementar la seguridad de partida en los equipos Windows de la red, el administrador podrá prohibir la ejecución de los programas que previamente haya clasificado como peligrosos o no compatibles con la actividad desarrollada en la empresa.

Las causas que pueden llevar a un administrador a prohibir la ejecución de un determinado programa pueden ser variadas: programas que consumen mucho ancho de banda, que acceden a

contenidos susceptibles de contener amenazas de seguridad, o que acceden a contenidos que afectan al rendimiento de los usuarios o de sus equipos.

Protección del correo y la Web

Cytomic EPDR se aleja del tradicional enfoque de seguridad basado en plugins que añaden la funcionalidad de protección a determinados programas (clientes de correo o navegadores). En su lugar, la protección intercepta a bajo nivel de todas las comunicaciones que usan protocolos comunes como HTTP, HTTPS o POP3. De esta manera, se ofrece una protección homogénea y permanente para todas las aplicaciones de correo y Web pasadas presentes y futuras: no se necesitan configuraciones específicas ni actualizaciones cuando los proveedores de los programas de correo y navegación publiquen nuevas versiones incompatibles con plugins anteriores.

Cortafuegos y sistema de detección de intrusos (IDS)

Cytomic EPDR incorpora tres herramientas básicas para filtrar el tráfico de red que reciben o envían los equipos protegidos, que se ajustan de forma automática en función del tipo de red a la que se conecta la estación de trabajo o servidor:

- **Protección mediante reglas de sistema**: describen las características de una comunicación entre dos equipos: puertos, IPs, protocolos etc. con el objetivo de permitir o denegar los flujos de datos que coincidan con las reglas establecidas.
- **Protección de programas**: permiten o deniegan la comunicación de determinados programas instalados en el equipo de usuario con el resto de la red.
- **Sistema de detección de intrusos**: detecta y rechaza patrones de tráfico mal formado que afecten a la seguridad o al rendimiento del equipo protegido.

Control de dispositivos

Dispositivos de uso común como las llaves USB, las unidades de CD/DVD, dispositivos de imágenes, bluetooth, módems o teléfonos móviles también pueden constituir una vía de infección para los equipos.

Cytomic EPDR permite establecer el comportamiento de estos dispositivos en los equipos protegidos, bloqueando su acceso o permitiendo su uso de forma parcial (solo lectura) o completa.

Filtrado de Spam, Virus y contenidos en servidores Exchange

Cytomic EPDR analiza los servidores Exchange en busca de virus, herramientas de hacking y programas potencialmente no deseados, con destino los buzones de los usuarios de la red.

Eliminar el correo basura -spam- es una labor que requiere mucho tiempo y además supone un peligro de estafa. Cytomic EPDR implementa una protección anti-spam para servidores Exchange para optimizar el tiempo de trabajo de los usuarios y aumentar la seguridad de los equipos de la red.

Cytomic EPDR protege los servidores de correo Exchange mediante dos tecnologías:

- Protección de buzones.
- Protección de transporte.

Protección de buzones

Aplica a los servidores Exchange con el rol de Mailbox, y analiza las carpetas / buzones en background o cuando el mensaje es recibido y almacenado en la carpeta del usuario.

La protección de buzones manipula los diferentes elementos del cuerpo del mensaje analizado para sustituir aquellos clasificados como peligrosos por otros seguros e introducir únicamente los primeros en la cuarentena.

La protección de buzones analiza las carpetas de usuario del servidor Exchange en segundo plano, aprovechando los tiempos de menor carga del servidor. Este análisis se ejecuta de forma inteligente, evitando volver a analizar los mensajes ya examinados. Con cada nuevo archivo de identificadores publicado se analizarán los buzones y la cuarentena en segundo plano.

Protección de transporte

Aplica a los servidores Exchange con el rol de Acceso de clientes, Edge Transport y Mailbox y analiza el tráfico que atraviesa al servidor.

En la protección de transporte no se permite la manipulación del cuerpo de los mensajes. De esta forma, el cuerpo de un mensaje peligroso se trata como un único bloque y las acciones que Cytomic EPDR permite ejecutar aplican al mensaje por completo: borrar el mensaje, meterlo en cuarentena, dejar pasar sin modificar etc.

Control de acceso a páginas Web

Cytomic EPDR agrupa las páginas web en varias categorías para que el administrador de la red pueda restringir el acceso a las que considere oportunas, así como a las URLs que especifique de forma manual. Con esta protección se optimiza del ancho de banda de la red y la productividad de la organización, evitando el acceso a recursos web sin relación con la actividad desarrollada en la empresa.

Además, se permite definir una configuración de horarios para restringir el acceso a determinadas categorías de páginas Web y listas negras durante las horas de trabajo, y autorizarlo en el horario no laborable o en el fin de semana.

Fase II: Detección y monitorización

La segunda fase del ciclo de protección adaptativa asume que el malware o el ataque dirigido consiguió sortear las barreras establecidas en la fase de Protección e infectó con éxito una o varias máquinas de la red, pasando esta infección desapercibida para el usuario del equipo.

En esta fase, Cytomic EPDR implementa una serie de tecnologías que permiten al administrador de la red localizar el problema.

Protección permanente avanzada

La protección avanzada monitoriza de forma continuada todos los procesos que se ejecutan en los equipos Windows de la red del cliente. Cytomic EPDR recoge todas las acciones desencadenadas por los procesos del usuario y los envía a la nube de Cytomic, donde se examinan mediante técnicas automáticas de Machine Learning en entornos Big Data para emitir una clasificación (goodware o malware) con un 99'9991 (menos de 1 error cada 100.000 ficheros analizados) de precisión, evitando de esta manera falsos positivos.

Para los casos más complicados Cytomic cuenta con un laboratorio de expertos especialistas en análisis de malware, con el único objetivo de clasificar todos los ejecutables localizados en el menor tiempo posible, desde la primera vez que fueron vistos en la red del cliente.

Cytomic EPDR admite tres modos de bloqueo para los procesos que todavía no han sido clasificados (desconocidos) y para los ya clasificados como malware:

- Audit
- Hardening
- Lock

Audit

En el modo Audit Cytomic EPDR solo informa de las amenazas detectadas, pero no bloquea ni desinfecta el malware encontrado. Este modo es útil para probar la solución de seguridad o para comprobar que la instalación del producto no compromete el buen funcionamiento del equipo.

Hardening

En aquellos entornos donde se producen cambios constantes del software instalado en los equipos de los usuarios o se ejecutan muchos programas desconocidos (como por ejemplo programas de creación propia) puede no ser viable esperar a que Cytomic EPDR aprenda de ellos para clasificarlos.

El comportamiento del modo Hardening consiste en balancear el riesgo de infección de los equipos y la productividad de los usuarios, limitando el bloqueo de los programas desconocidos a aquellos que a priori se consideran peligrosos. De esta forma se distinguen cuatro escenarios:

- **Ficheros ya clasificados por Cytomic EPDR como goodware**: se permite su ejecución.

- **Ficheros ya clasificados por Cytomic EPDR como malware**: son enviados a cuarentena o desinfectados.
- **Ficheros sin clasificar que vienen del exterior (Internet, correo, dispositivos USB, otros equipos de la red del cliente)**: se bloquea su ejecución hasta que el sistema emita una clasificación. En función de ésta se permitirá su ejecución (goodware) o serán movidos a cuarentena (malware).).

En muchas ocasiones la clasificación es casi inmediata; un programa descargado de Internet y desconocido para Cytomic EPDR será bloqueado en un primer momento, pero minutos después se podrá ejecutar si resultó ser goodware.

- **Ficheros sin clasificar ya instalados en el equipo del usuario antes de la implantación de Cytomic EPDR**: se permite su ejecución, aunque sus acciones se monitorizan y se envían al servidor para su estudio. Una vez clasificados se permitirá su ejecución (goodware) o se bloqueará (malware).

Lock

Para entornos donde la seguridad sea la máxima prioridad, y con el objetivo de ofrecer una protección de máximas garantías, Cytomic EPDR incluye el modo Lock. En este modo se bloquea la ejecución del software en proceso de clasificación y todo aquel que ya ha sido clasificado como malware. Únicamente se permite ejecutar el software lícito.

*Más del 99% de los programas encontrados en los equipos de los usuarios ya están clasificados en los sistemas de Cytomic EPDR por lo que los bloqueos por desconocidos afectan a una minoría de programas. Para más información sobre la configuración de los distintos modos de bloqueo consulta el apartado "***Protección avanzada (Equipos Windows)***" en la página* **229**.

Protección contra exploits

Cytomic EPDR implementa tecnologías para proteger los equipos de la red frente a las amenazas que aprovechan vulnerabilidades en el software. Estas vulnerabilidades son utilizadas (explotadas) para provocar comportamientos anómalos en las aplicaciones, produciendo fallos de seguridad.

Las amenazas de tipo exploit utilizan tanto vulnerabilidades conocidas como de día cero (0-day) o desconocidas, como parte de una cadena de eventos conocida como CKC (Cyber Kill Chain), que ejecutan para comprometer los equipos de la red. Cytomic EPDR bloquea de forma efectiva y en tiempo real esta cadena de eventos para impedir que los ataques de tipo exploit prosperen y dejarlos sin efecto.

Para detectar las técnicas de explotación de vulnerabilidades usadas por los hackers, Cytomic EPDR implementa nuevos hooks en el sistema operativo, que utiliza para monitorizar localmente y de forma constante las acciones de los procesos ejecutados en el equipo del usuario. Este enfoque se aleja del esquema tradicional implementado por otros productos de seguridad, que buscan patrones y detecciones estáticas de pares CVE - payload mediante ficheros de firmas.

Cytomic EPDR ofrece una protección anti exploit generalista gracias a la constante adaptación de la tecnología encargada de detectar el uso de técnicas avanzadas de explotación de vulnerabilidades, algunas de las cuales se muestran a continuación:

- Attack Surface Reduction (ASR)
- Data Execution Prevention (DEP)
- Structured Exception Handling Overwrite Protection (SEHOP)
- NullPage Security Mitigation
- Heapspray Allocation
- Export Address Table Filtering (EAF)
- Mandatory Address Space Layout Randomization (ASLR)
- Bottom Up ASLR Security Mitigation
- Load Library Check - Return Oriented Programming (ROP)
- Memory Protection Check - Return Oriented Programming (ROP)
- Caller Checks - Return Oriented Programming (ROP)
- Simulate Execution Flow - Return Oriented Programming (ROP)
- Stack Pivot - Return Oriented Programming (ROP)
- EternalBlue
- Process Doppelgänging

Detección de amenazas sin fichero (fileless / malwareless)

Algunas amenazas avanzadas sortean las estrategias de detección de malware basadas en archivos de identificadores evitando almacenar ficheros en el disco duro del equipo infectado. Estas amenazas únicamente residen en la memoria RAM del equipo, y con esta estrategia se vuelven muy complicadas de detectar y de cuantificar el alcance de sus acciones mediante procesos de análisis forense estándar.

La protección avanzada de Cytomic EPDR es capaz de evitar esta estrategia monitorizando de forma continuada todos los procesos ejecutados y analizando su comportamiento. Los procesos que muestren una secuencia de acciones declarada como peligrosa serán clasificados como malware, independientemente del número de ficheros que depositen en el sistema de almacenamiento del equipo de usuario o servidor. De esta misma manera, al quedar almacenadas todas las acciones del proceso en la nube de Cytomic, es posible ejecutar un análisis forense completo.

Monitorización de ficheros de datos (Cytomic Data Watch)

Cytomic EPDR registra todos los accesos a ficheros de datos del usuario por parte de los procesos ejecutados en el equipo. Aunque el malware consiga infectar el equipo, es posible precisar con exactitud qué ficheros modificó y en qué momento. También es posible determinar si envió ficheros

fuera de la empresa a través de Internet, las direcciones IP de destino y otra información valiosa que facilita tanto el análisis forense posterior como las acciones de resolución. A continuación, se muestran los tipos de ficheros de datos que se monitorizan:

- Documentos de suites ofimáticas.
- Documentos en formato PDF.
- Documentos de aplicaciones CAD.
- BBDD de escritorio.
- Almacenes de contraseñas de navegadores.
- Almacenes de contraseñas de clientes de correo.
- Almacenes de contraseñas de clientes de FTP.
- Almacenes de contraseñas de Directorio Activo.
- Almacenes de certificados y certificados de usuario.
- Almacenes de Digital Wallet.
- Configuración de navegadores.
- Configuración de firewall.
- Configuración de GPO.

Parcheo de vulnerabilidades (Cytomic Patch)

Cytomic Patch mantiene de forma automática una base de datos de los parches y actualizaciones publicadas por los proveedores del software para los sistemas operativos Windows instalados en el parque informático. Comparando esta base de datos con los parches ya instalados en los equipos se muestran aquellos que contienen software vulnerable, y que por lo tanto son susceptibles de recibir ataques de programas maliciosos para infectar la red de la empresa.

Para evitar esto, Cytomic Patch permite crear tareas programadas e inmediatas de parcheo de los equipos, reduciendo de esta forma la superficie de ataque de puestos de usuario y servidores.

Visibilidad del estado de la red

Cytomic EPDR implementa recursos para poder valorar el estado de la seguridad de la red en un solo vistazo, a través de informes y de un panel de control (dashboard) formado por diferentes widgets.

Lo importante en esta etapa no solo es determinar si la red del cliente está siendo atacada y en qué grado o forma, sino contar con la información necesaria para poder valorar una probabilidad de infección.

En los paneles de Cytomic EPDR se incluye información clave en este sentido:

- Cuáles son los procesos desconocidos para Cytomic EPDR encontrados en los equipos de la red, y

que están siendo investigados para su posterior clasificación en Cytomic, junto con una valoración preliminar de su peligrosidad.

- Actividad detallada en forma de listados de acciones de aquellos programas desconocidos que finalmente resultaron ser malware.
- Detecciones realizadas en los diferentes vectores de infección protegidos.

Con este módulo el administrador tiene una visión global de los procesos que se ejecutan en su red: por el lado del malware ya conocido que intentó infectar algún equipo y fue detenido en el módulo de protección; y por el lado del malware desconocido y diseñado para pasar inadvertido por las tecnologías de detección tradicionales, y que consiguió sortear los sistemas de detección configurados.

El administrador tendrá la posibilidad de reforzar la seguridad de su red impidiendo toda ejecución de software desconocido o, por el contrario, balancear el nivel de bloqueo en favor de una mayor flexibilidad a la hora de ejecutar ciertos programas no conocidos.

*Para más información consulta el capítulo "**Visibilidad del malware y del parque informático**" en la página **379**.*

Fase III: Resolución y respuesta

En caso de producirse una brecha de seguridad, es necesario actuar en dos líneas: revertir de forma rápida el estado de los equipos afectados previo a la infección, y calcular el impacto del ataque: si hubo fuga de datos, hasta donde consiguió penetrar el ataque, qué equipos resultaron comprometidos etc. Cytomic EPDR incorpora herramientas para estos dos escenarios.

Respuesta

Mediante la herramienta de análisis forense el administrador puede ver todas las acciones ejecutadas por el malware en el equipo infectado, así como información fundamental a la hora de valorar la peligrosidad de la amenaza: vector de infección (como llegó el malware a la red de la organización), patrón de propagación a otros equipos y accesos al disco duro en busca de información confidencial, entre otros.

Cytomic EPDR genera un entorno seguro para que el administrador ejecute el análisis forense, aislando los equipos afectados de la red. De esta manera, se impiden las comunicaciones con el exterior para evitar la fuga de información, pero se mantiene la conexión con la nube de Cytomic para investigar el suceso sin desplazarse físicamente al equipo afectado.

Además, Cytomic Insights y Cytomic Data Watch extienden y ayudan a interpretar los datos recogidos por Cytomic EPDR. El administrador tiene acceso a información representada gráficamente de todos los procesos ejecutados por el usuario, y no solo de los clasificados como

malware. También se identifican los ficheros que contienen datos personales (PII) y los procesos que acceden a ellos y los envían fuera de la red de la organización.

Resolución

Cytomic EPDR cuenta con herramientas de desinfección propias de un antivirus tradicional junto a la cuarentena, que almacena los elementos sospechosos o eliminados.

"**Herramientas de resolución**" *en la página* **493**.

Fase IV: Adaptación / Prevención

Una vez finalizado el estudio del incidente con las herramientas de Resolución y respuesta de la Fase III y localizadas las causas que propiciaron la infección, el administrador deberá ajustar la política de seguridad de la empresa para que no se vuelvan a producir situaciones equivalentes en el futuro.

La fase de Adaptación puede reunir una gran cantidad de iniciativas en función de los resultados revelados por el análisis forense: desde cursos de educación y sensibilización en el correcto uso de Internet para los empleados de la empresa, hasta la reconfiguración de los routers corporativos o de los permisos de los usuarios en sus máquinas personales.

Desde el punto de vista de los dispositivos, Cytomic EPDR puede reforzar la seguridad cambiando la configuración de la protección avanzada: si los usuarios de la empresa tienden a utilizar siempre el mismo software, o algunos de ellos suelen instalar programas de dudosa procedencia, una opción para minimizar el riesgo de estos equipos es implementar el modo Lock de la protección avanzada. De esta forma se limita la exposición al malware en los equipos más problemáticos impidiendo la ejecución de los programas que no sean legítimos.

Desde el punto de vista del equipo de usuario o servidor, Cytomic EPDR puede reforzar la seguridad de múltiples maneras:

- **Cambio en la configuración de la protección avanzada.**

Si los usuarios de la empresa tienden a utilizar siempre el mismo software, o algunos de ellos suelen instalar programas de dudosa procedencia, una opción para minimizar el riesgo de estos equipos es implementar el modo Lock de la protección avanzada. De esta forma se limita la exposición al malware en los equipos más problemáticos y se impide la ejecución de los programas que no sean legítimos.

- **Cambio de la configuración de la protección antivirus**

Cambiar la frecuencia de los análisis bajo demanda o activar la protección de vectores de infección como Web o correo ayudarán a proteger los equipos que reciban malware por estas dos vías.

- **Limitación de la navegación Web a categorías concretas**

Reconfigurar las categorías accesibles a la navegación para limitar el acceso a páginas de origen dudoso, cargadas de publicidad y propensas a ofrecer descargas en apariencia inocentes (descarga de libros, programas piratas etc.) pero que pueden infectar de malware los equipos.

- **Filtrado de la llegada de correo con Phising o Spam**

Un vector muy utilizado para ataques de tipo phising es el correo. Refuerza la configuración del filtrado de contenidos y del filtro anti spam para limitar la cantidad de correo no solicitado que llega a los buzones de los usuarios, reduciendo así la superficie de ataque.

- **Bloqueo parcial o total de pen drives y otros dispositivos externos**

Otro de los vectores de infección más típicos son las memorias y los módems USB que los usuarios tienen en propiedad. Limita o bloquea completamente su uso para evitar la infección por estas vías.

- **Limitación de las comunicaciones (Firewall e IDS)**

El firewall es una herramienta orientada a reducir la superficie de exposición de los equipos y evita la comunicación de programas que, de por sí, no son malware pero que pueden suponer una ventana abierta a la entrada del mismo. Si se ha detectado una intrusión de malware por programas de tipo chat o P2P, una correcta configuración de las reglas del firewall evitará la comunicación de estos programas con el exterior.

El firewall y el IDS también pueden ser utilizados para minimizar la propagación del malware una vez ha infectado al primero de los equipos de la red. Examina las acciones que desencadenó con la herramienta de análisis forense para generar nuevas reglas de cortafuegos que limiten la comunicación entre equipos o los protejan de ataques de red.

- **Cambio de la configuración de Cytomic Patch**

Cambiar la configuración de las tareas de parcheo permite minimizar el tiempo que los programas instalados incorporan vulnerabilidades aprovechables por el malware. Ampliar el número de tipos de parches a instalar incrementa la seguridad de la red, garantizando que todo el software instalado incorpora las últimas actualizaciones publicadas por los proveedores.

Desinstalar o actualizar los programas que han entrado en EoL minimiza la superficie de ataque de los equipos: se retira el software que ya no recibe actualizaciones de los proveedores, y por lo tanto tiene una mayor probabilidad de incorporar fallos y vulnerabilidades no resueltas y aprovechables por el malware.

- **Cifrado de la información contenida en los dispositivos de almacenamiento interno de los equipos con Cytomic Encryption.**

Minimiza la exposición de la información almacenada por la empresa en equipos susceptibles de ser robados o extraviados, y evita el acceso a datos confidenciales mediante herramientas de recuperación de ficheros borrados en unidades descartadas. Adicionalmente, para evitar la

utilización de los discos duros en un equipo distinto al que cifró su contenido o cambiar su secuencia de arranque es recomendable utilizar el módulo TPM incorporado en la placa base del equipo o actualizar el hardware a uno que incluya este recurso.

- **Bloqueo de programas peligrosos, no relacionados con la actividad de la empresa o con un fuerte impacto en el rendimiento del equipo, de la infraestructura de red o del propio usuario.**

Minimiza la superficie de ataque de los equipos de la red impidiendo la ejecución de programas que acceden a contenidos susceptibles de contener virus y otras amenazas de seguridad. Mejora la productividad de los usuarios, del rendimiento de la red y de los equipos administrados impidiendo la ejecución de programas que descargan grandes volúmenes de datos o consumen muchos recursos del equipo del usuario.

Parte 2

La consola web de administración

Capítulo 4: La consola de administración

Capítulo 5: Control y supervisión de la consola de administración

Capítulo 4

La consola de administración

Cytomic EPDR utiliza las últimas tecnologías de desarrollo web para ofrecer una consola de administración alojada en la nube que permite interactuar cómoda y ágilmente con el servicio de seguridad. Sus principales características son:

- **Adaptable:** diseño "responsive" que se adapta al tamaño del dispositivo empleado para administrar el servicio.
- **Amigable**: interface desarrollado con tecnología Ajax que evita las recargas de páginas completas.
- **Flexible**: interface adaptable que almacena los ajustes realizados para posteriores accesos.
- **Homogénea**: patrones de usabilidad bien definidos para minimizar la curva de aprendizaje del administrador.
- **Interoperable**: datos exportables en formato `csv` con campos extendidos para su posterior consulta.

CONTENIDO DEL CAPÍTULO

Beneficios de la consola web

La consola Web es la herramienta principal del administrador para la gestión de la seguridad. Al tratarse de un servicio Web, hereda una serie de características que influirán de manera positiva en la forma de trabajo del departamento de IT.

- **Única herramienta para la gestión completa de la seguridad**

El administrador podrá distribuir de forma centralizada el paquete de instalación Cytomic EPDR en los equipos de la red, establecer las configuraciones de seguridad, monitorizar el estado de la protección de los equipos y disponer de herramientas de resolución y análisis forense en caso de incidentes de seguridad. Toda la funcionalidad se ofrece desde una única consola Web, favoreciendo la integración de las distintas herramientas y minimizando la complejidad de utilizar varios productos de distintos proveedores.

- **Gestión centralizada de la seguridad para oficinas remotas y usuarios desplazados**

La consola Web está alojada en la nube, por lo que no son necesarias configuraciones de VPN ni redirecciones de puertos en los routers corporativos para su acceso desde el exterior de la oficina. Tampoco son necesarias inversiones en infraestructuras IT, tales como servidores, licencias de sistemas operativos o bases de datos, ni es necesaria una gestión del mantenimiento / garantía para asegurar el funcionamiento del servicio.

- **Gestión de la seguridad desde cualquier lugar y en cualquier momento**

La consola Web es de tipo "responsive / adaptable" con lo que se ajusta al tamaño del dispositivo utilizado por el administrador. De esta manera se puede gestionar la seguridad desde cualquier lugar y en cualquier momento, mediante un smartphone, un notebook o un PC de escritorio.

Requisitos de la consola web

Para acceder a la consola Web utiliza la siguiente URL:

https://manage.cytomicmodel.com

Es necesario cumplir con el siguiente listado de requisitos:

- Contar con unas credenciales validas (usuario y contraseña).

*Para más información sobre cómo crear una Cuenta Cytomic de acceso a la consola Web consulta el apartado "**Crear una Cuenta Cytomic**" en la página **523**.*

- Un navegador compatible certificado.
- Conexión a Internet y comunicación por el puerto 443.

Federación con IDP

Cytomic EPDR delega la gestión de las credenciales en un Proveedor de Identidades (Identity Provider, IDP), una aplicación centralizada responsable de gestionar las identidades de los usuarios de la consola web.

Con una única Cuenta Cytomic el administrador de la red tiene acceso a todos los productos contratados con Cytomic de forma segura y sencilla.

Estructura general de la consola Web

La consola Web cuenta con recursos que facilitan una experiencia de gestión homogénea y coherente, tanto para administrar la seguridad de la red como para resolver los incidentes y realizar un análisis forense.

El objetivo de la consola web es entregar al administrador una herramienta sencilla, pero a la vez flexible y potente, que le permita comenzar a gestionar la seguridad de la red de forma productiva en el menor período de tiempo posible.

A continuación, se incluye una descripción de los elementos de la consola y su modo de uso.

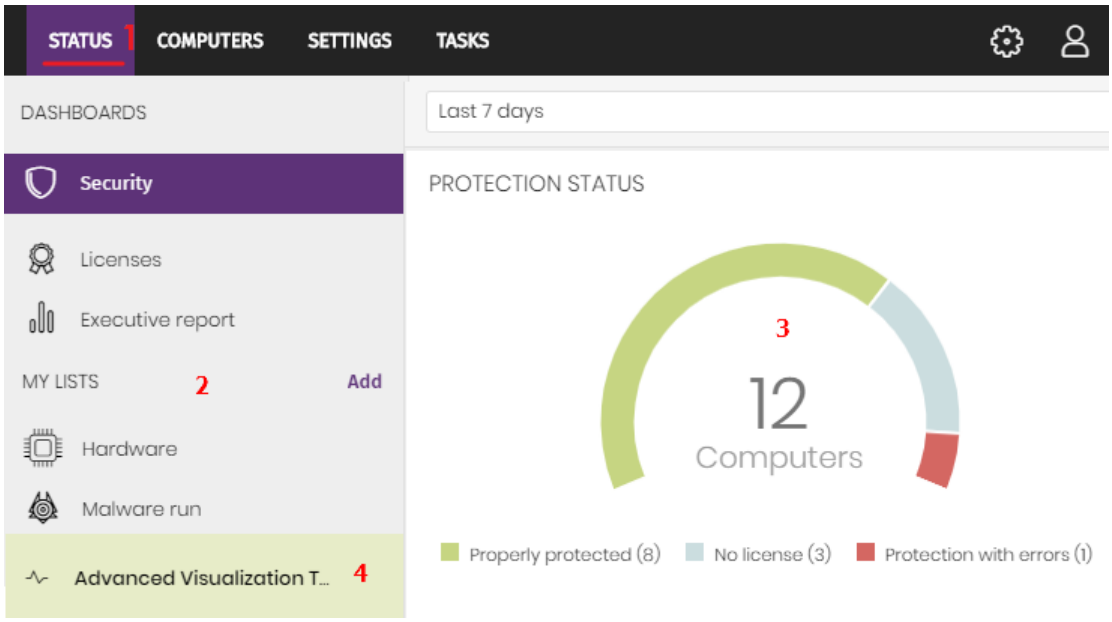


Figura 4.1: vista general de la consola de administración Cytomic EPDR

Menú superior (1)

La consola distribuye toda su funcionalidad en varias zonas accesibles desde el menú superior:

- Botón Cytomic Cloud
- Estado
- Equipos
- Configuración
- Tareas
- Configuración general
- Cuenta de usuario

Botón Cytomic Cloud

Haz clic en el botón situado en el lateral izquierdo del menú superior para elegir el producto de seguridad contratado y gestionarlo o modificar la configuración de la Cuenta Cytomic.

Menú superior Estado

Muestra el panel de control de la consola desde la cual el administrador tiene acceso de un vistazo a toda la información de seguridad, tanto en forma gráfica mediante widgets como mediante los listados situados en el menú lateral. Consulta el apartado "**Esquema general de la zona Estado**".

Menú superior Equipos

Ofrece las herramientas básicas para definir la estructura de los equipos de la red que mejor se ajuste a la configuración de seguridad diseñada para el parque informático. Elegir una correcta estructura de dispositivos es fundamental a la hora de asignar configuraciones de seguridad. Consulta el apartado "**La zona equipos**" en la página **151**.

Menú superior Configuración

Permite al administrador de la red definir el comportamiento de Cytomic EPDR en los equipos de usurario y servidores donde se encuentra instalado. La asignación de la configuración se establece de forma global para todos los equipos de la red, o únicamente para algunos equipos concretos mediante plantillas, dependiendo del tipo de configuración a establecer. Estas plantillas de configuración se pueden asignar a uno o más equipos de la red que tengan requerimientos de seguridad similares, permitiendo minimizar el tiempo del administrador dedicado a gestionar la seguridad de su red de equipos.

*Consulta el capítulo "**Gestión de configuraciones**" en la página **195** para obtener información detallada sobre cómo crear una configuración en Cytomic EPDR.*

Cytomic EPDR permite configurar los siguientes aspectos del servicio:

- **Usuarios**: gestiona las cuentas que podrán acceder a la consola de administración, así como las acciones permitidas dentro de ella (roles) y su actividad. Consulta el capítulo "**Control y supervisión de la consola de administración**" en la página **69**.
- **Ajustes por equipo**: define las plantillas de configuración donde se indica cada cuanto se actualizará el software de seguridad Cytomic EPDR instalado en los equipos de usuario y servidores. También establece la configuración global frente a manipulaciones externas y desinstalaciones no autorizadas. Consulta el capítulo "**Configuración remota del agente**" en la página **211**.
- **Configuración de red**: define plantillas de configuración que establecen el idioma del software Cytomic EPDR instalado en los equipos de usuario y servidores, y el tipo de conexión que se utilizará para conectar con la nube de Cytomic. Consulta el capítulo "**Configuración remota del agente**" en la página **211**.
- **Servicios de red**: define el comportamiento del software Cytomic EPDR en lo referente a la comunicación con los equipos vecinos de la red del cliente:
  - **Proxy**: define de forma global los equipos que realizarán tareas de proxy para facilitar el acceso a la nube de equipos con Cytomic EPDR instalado y asilados de la red. Consulta el apartado "**Rol de Proxy**" en la página **212**.
  - **Caché**: define de forma global los repositorios de ficheros de firmas, parches de seguridad y componentes utilizados para actualizar el software Cytomic EPDR instalado en los equipos de la red. Consulta el apartado "**Rol de Caché / repositorio**" en la página **213**.
  - **Descubrimiento**: define de forma global los equipos de la red encargados de rastrear la aparición

de dispositivos sin proteger. Consulta el apartado "**Rol de descubridor**" en la página **215**.

- **Entornos DVI**: define el número de equipos alojados en infraestructuras de virtualización no persistentes para facilitar la asignación de licencias.
- **Mis Alertas**: establece el tipo de alertas que el administrador recibirá en su buzón de correo. Consulta el capítulo "**Alertas**" en la página **473**
- **Estaciones y servidores**: define plantillas de configuración que establecen el comportamiento de Cytomic EPDR para proteger a los equipos Windows de la red frente a las amenazas y el malware. Consulta el capítulo "**Configuración de estaciones y servidores**" en la página **225**.
- **Bloqueo de programas**: define plantillas de configuración que establecen el comportamiento de Cytomic EPDR para bloquear la ejecución de programas. Consulta el capítulo "**Configuración del bloqueo de programas**" en la página **373**
- **Dispositivos Android**: define plantillas de configuración que establecen el comportamiento de Cytomic EPDR para proteger a los tablets y teléfonos móviles Android frente a las amenazas y el malware y al robo de estos dispositivos. Consulta el capítulo "**Configuración de seguridad Android**" en la página **251**.
- **Gestión de parches**: define las plantillas de configuración que establecen el comportamiento del descubrimiento de nuevos parches de seguridad publicados por los proveedores de software y del sistema operativo Windows. Consulta el capítulo "**Cytomic Patch (Actualización de programas vulnerables)**" en la página **307**.
- **Data Control**: define las plantillas de configuración que permiten realizar un seguimiento de la información personal contenida en los sistemas de almacenamiento. Consulta el capitulo "**Cytomic Data Watch (Supervisión de información sensible)**" en la página **255**.
- **Cifrado**: define las plantillas de configuración que permiten cifrar el contenido de los dispositivos de almacenamiento interno. Consulta el capítulo "**Cytomic Encryption (Cifrado de dispositivos)**" en la página **349**.

Menú superior Tareas

Permite la gestión de tareas de seguridad programadas para su ejecución en los intervalos de tiempo designados por el administrador. Consulta el capítulo "**Tareas**" en la página **503**.

Menú superior Configuración General 

Muestra un menú desplegable que permite el acceso a la documentación del producto, cambio de idioma de la consola y otras herramientas.

Entrada	Descripción
Ayuda Online	Acceso a las ayudas web del producto.
Guía de administración de Cytomic Insights	Acceso a la guía para el administrador del módulo Cytomic Insights si está contratado.

Tabla 4.1: menú Configuración general

Entrada	Descripción
Guía de administración de Cytomic EPDR	Acceso a la Guía de administración del producto Cytomic EPDR.
Guía de administración de Cytomic Data Watch	Acceso a la guía para el administrador del módulo Cytomic Data Watch si está contratado.
Soporte técnico	Carga la dirección web correspondiente al soporte técnico de Cytomic EPDR.
Buzón de sugerencias	Lanza la herramienta de correo local instalada en equipo para mandar un mensaje de correo al departamento de soporte técnico de Cytomic.
Acuerdo de licencia	Muestra el EULA (End User License Agreement).
Novedades de Cytomic EPDR	Enlace a la página web de soporte que muestra los cambios y nuevas funcionalidades incluidas en la versión.
Idioma	Permite seleccionar el idioma en que se mostrará la consola de administración.
Acerca de...	Muestra la versión de los diferentes elementos de Cytomic EPDR. • **Versión**: versión del producto. • **Versión de la protección**: versión interna del módulo de protección instalado en los equipos. • **Versión del agente**: versión interna del módulo de comunicaciones instalado en los equipos.

Tabla 4.1: menú Configuración general

Menú superior Cuenta de usuario

Muestra un menú desplegable con las siguientes entradas de configuración:

Entrada	Descripción
Configurar mi perfil	Modifica la información de la cuenta principal del producto.
Cambiar de cuenta	Lista las cuentas accesibles por el administrador y permite seleccionar una para operar con la consola.
Cerrar sesión	Hace logout de la consola y devuelve el control a la pantalla de IdP.

Tabla 4.2: menú Cuenta de usuario

Menú lateral (2)

Muestra las diferentes subzonas dentro de la zona seleccionada, actuando como un selector de segundo nivel con respecto al menú superior.

El menú lateral varía en función de la zona presentada, adaptándose al tipo de información que se muestra.

Panel central (3)

Recoge toda la información relevante de la zona y subzona elegidas por el administrador. En la figura 4.1 se muestra la zona **Estado** subzona **Seguridad**, formada por los widgets que permiten interpretar la información de seguridad recogida. Para obtener más detalle acerca de los widgets consulta el apartado "**Paneles / Widgets de seguridad**" en la página **380**.

Acceso a Advanced Visualization Tool (4)

Advanced Visualization Tool es el punto de entrada para la consola de gestión de los módulos Cytomic Data Watch y Cytomic Insights. Ambos comparten una consola especialmente diseñada para mostrar gráficas avanzadas y tablas con información relevante sobre la actividad de los todos procesos ejecutados en los puestos de usuario y servidores.

Elementos básicos de la consola web

Menú de pestañas superior

En las zonas de la consola más complejas se muestra un selector de tercer nivel en forma de pestañas que mantiene la información ordenada por categorías.

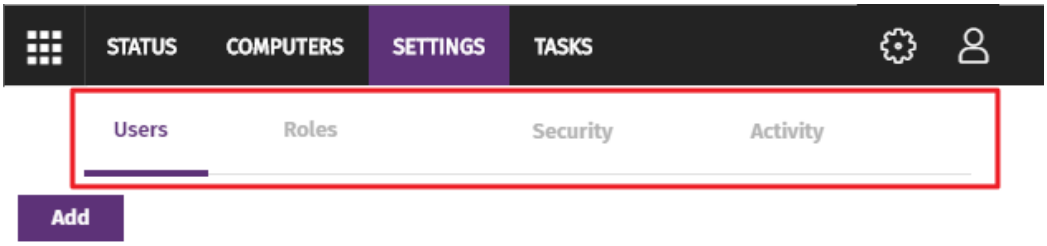


Figura 4.2: menú de pestañas

Barra de acciones

Figura 4.3: barra de acciones

Para facilitar la navegación de la consola y el acceso a algunas operaciones comunes sobre los puestos de usuario y servidores administrados, se incorpora una barra de acciones en la parte superior de la pantalla. El número de botones mostrados se adapta al tamaño de la ventana. Los botones que quedan fuera se añaden al icono ▪▪▪ situado a la derecha de la barra de acciones.

En la esquina derecha de la barra de acciones se muestra el número total de equipos seleccionados. Haz clic en el icono del aspa para deshacer la selección.

Herramientas de filtrado y búsqueda

Las herramientas de filtrado y búsqueda muestran los subconjuntos de información de interés para el administrador. Algunas herramientas de filtrado son generales y aplican a toda la zona de la consola mostrada, como por ejemplo en el menú superior **Estado** o menú superior **Equipos**.

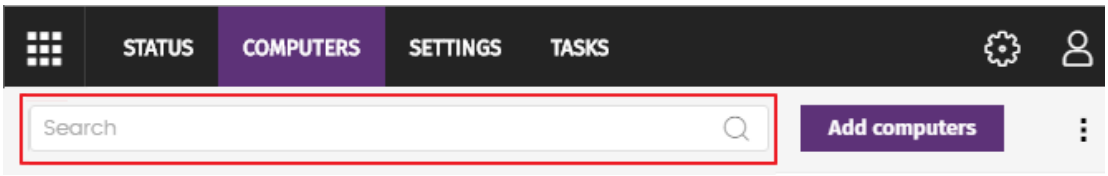


Figura 4.4: herramienta de búsqueda

Parte de las herramientas de filtrado se ocultan por defecto bajo el desplegable **Filtros**, y permiten definir búsquedas por categorías, rangos y otros parámetros dependientes del tipo de información mostrada.

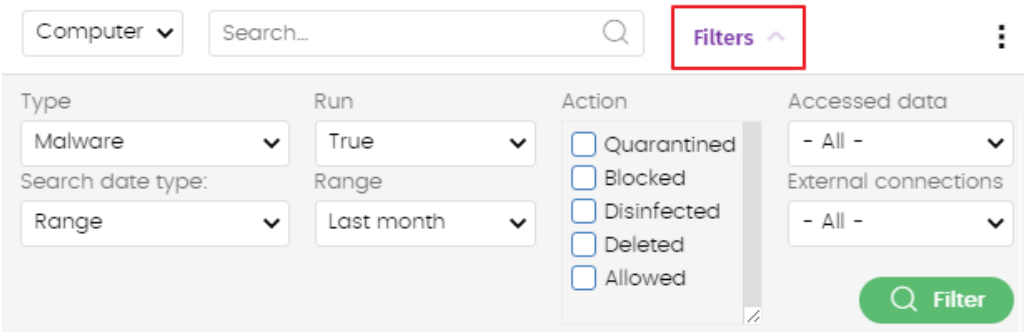


Figura 4.5: sistema de filtrado de información en listados

Elementos de configuración

La consola web Cytomic EPDR utiliza controles estándar para introducir configuraciones, como son:

- Botones. **(1)**
- Links. **(2)**
- Casillas de activación y desactivación. **(3)**
- Desplegables de selección. **(4)**
- Combos de selección. **(5)**

- Cuadros de texto. **(6)**

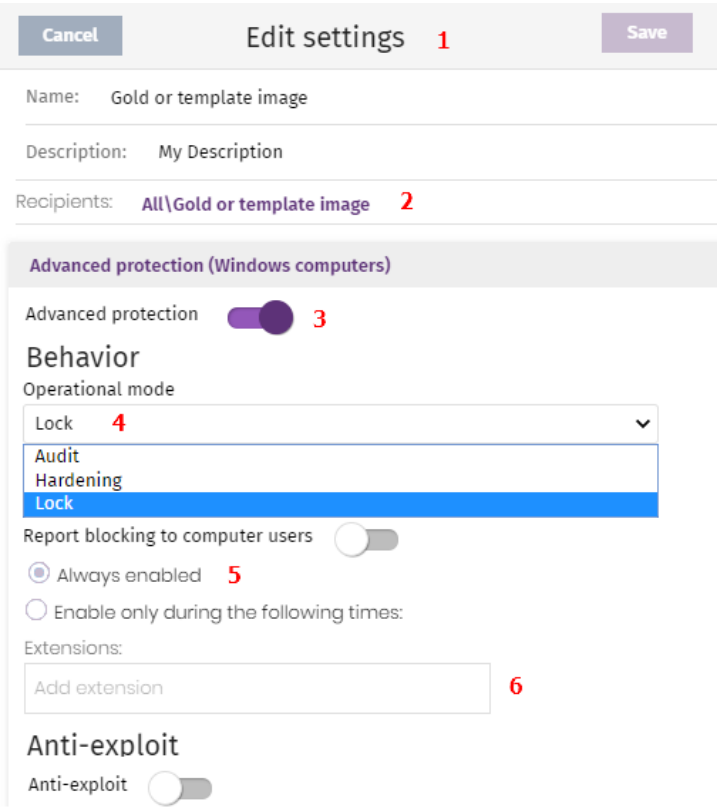


Figura 4.6: controles para el manejo de la consola de administración

Botón de ordenación

En algunos listados de elementos, como por ejemplo en la zona **Tareas** (menú superior **Tareas**) o en la zona **Configuración** (menú superior **Configuración**) se muestra el botón en la esquina superior derecha o en algunos casos en la esquina inferior derecha. Este botón permite establecer el criterio de ordenación del listado:

- **Ordenado por fecha de creación**: los elementos se ordenan según su fecha de incorporación al listado.
- **Ordenado por nombre**: los elementos se ordenan por su nombre.
- **Ascendente**
- **Descendente**

Menús de contexto

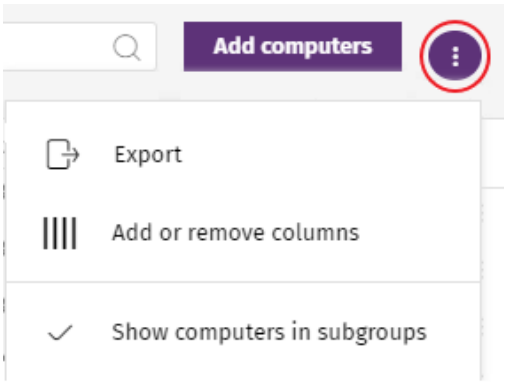


Figura 4.7: menús de contexto

Son menús desplegables que se muestran al hacer clic en el icono ⋮, con opciones que afectan al ámbito al que pertenecen según su posición.

Esquema general de la zona Estado

El menú **Estado** reúne las principales herramientas de visibilidad, y está distribuido en varias secciones:

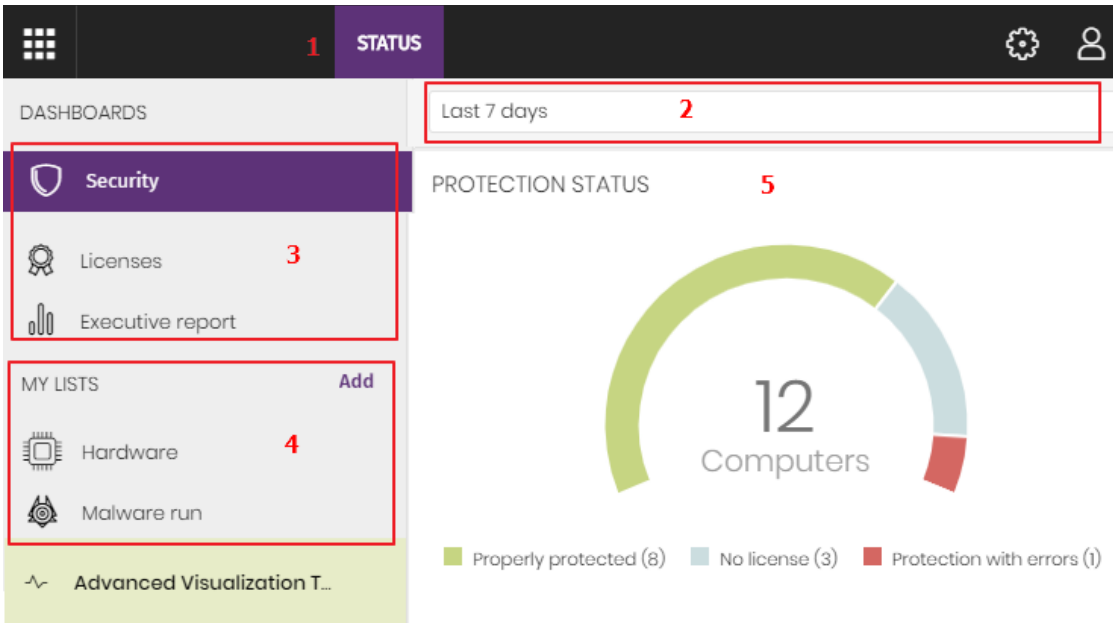


Figura 4.8: ventana de Estado con el panel de control y acceso a los listados

- **Acceso al panel de control (1)**

El acceso al panel de control se realiza mediante el menú superior **Estado**. Desde aquí se acceden a los diferentes widgets, así como a los listados.

Los widgets o paneles gráficos representan aspectos concretos del parque de equipos gestionado, dejando a los listados la entrega de datos más detallados.

- **Selector del intervalo de tiempo (2)**

El panel de control muestra la información relevante en el intervalo de tiempo fijado por el administrador mediante la herramienta situada en la parte superior de la ventana **Estado**. Los intervalos disponibles son:

- Últimas 24 h.
- Últimos 7 días.
- Último mes.
- Último año.

> *No todos los paneles soportan el filtrado de datos por el último año. Los paneles que no soporten este intervalo de tiempo mostrarán una leyenda en la parte superior indicándolo.*

- **Selector de panel (3)**
  - **Seguridad**: estado de la seguridad del parque informático. Para más información sobre los widgets incluidos consulta el apartado "**Paneles / Widgets de seguridad**" en la página **380**.
  - **Accesos web y spam**: filtrado de la navegación y del correo no solicitado en servidores Microsoft Exchange. Para más información sobre los widgets incluidos consulta el apartado "**Paneles / Widgets de seguridad**" en la página **380**.
  - **Gestión de parches**: actualización del sistema operativo y del software instalado en los equipos. Para más información sobre los widgets incluidos consulta el apartado "**Paneles / widgets en Cytomic Patch**" en la página **321**.
  - **Data control**: seguimiento de la información personal almacenada en los equipos de la red. Para más información sobre los widgets incluidos consulta el apartado "**Paneles / widgets en Cytomic Data Watch**" en la página **277**.
  - **Cifrado**: estado del cifrado de los dispositivos de almacenamiento internos en los equipos. Para más información sobre los widgets incluidos consulta el apartado "**Paneles / widgets en Cytomic Encryption**" en la página **360**.
  - **Licencias**: estado de las licencias de Cytomic EPDR asignadas a los equipos de la red. Consulta el capítulo "**Licencias**" en la página **131** para obtener más información acerca de la gestión de licencias.
  - **Envíos programados**: consulta el capítulo "**Envío programado de informes y listados**" en la página **479** para obtener más información acerca de la configuración y generación de informes.

- **Mis listados (4)**

Son tablas de datos con la información presentada en los paneles. Esta información se presenta con gran nivel de detalle e implementa herramientas de búsqueda y distribución que ayudan a localizar los datos requeridos.

- **Paneles informativos / Widgets (5)**

Está formado por widgets o paneles informativos centrados en un único aspecto de la seguridad de la red.

Los paneles se generan en tiempo real y son interactivos: pasando el ratón por encima de los elementos se muestran tooltips con información extendida.

Todas las gráficas incluyen una leyenda que permite determinar el significado de cada serie representada, e incorporan zonas activas que al ser seleccionadas abren distintos listados asociados al widget con filtros predefinidos.

Cytomic EPDR utiliza varios tipos de gráficas para mostrar la información de la forma más conveniente según el tipo de dato representado:

- Gráficos de tarta.
- Histogramas.
- Gráficas de líneas.

Gestión de listados

Cytomic EPDR estructura la información recogida en dos niveles: un primer nivel que representa de forma gráfica los datos mediante paneles o widgets y un segundo nivel más detallado, donde la información se representa mediante listados compuestos por tablas. La mayor parte de los paneles tienen un listado asociado para que el administrador pueda acceder de forma rápida a un resumen gráfico de la información y después profundizar mediante los listados en caso de requerir mayor nivel de detalle.

Cytomic EPDR soporta el envío programado de listados por correo electrónico. De esta forma, el administrador no necesita acceder a la consola Web para conocer el detalle de los eventos que se producen en la red. Además, esta funcionalidad facilita la compartición de información entre departamentos y permite habilitar la construcción de un repositorio externo con el histórico de todos los eventos que se han producido, mas allá de los límites de la consola Web. Con este repositorio, el equipo directivo podrá realizar un seguimiento de la información generada libre de interferencias de terceros.

Plantillas, configuraciones y vistas

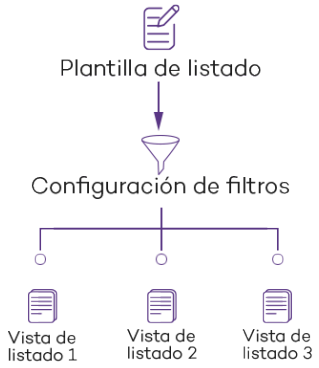


Figura 4.9: generación de tres listados a partir de una misma plantilla / fuente de datos

Un listado es la suma de dos elementos: una plantilla y una configuración de un filtro.

Una plantilla representa una fuente de datos sobre un apartado específico tratado por Cytomic EPDR.

Un filtro es una configuración específica de las herramientas de filtrado asociadas a cada plantilla.

Un filtro aplicado sobre una plantilla da como resultado una "vista de listado", también llamado simplemente "listado". El administrador puede crear y almacenar nuevos listados modificando los filtros asociados a una plantilla para su consulta posterior. De esta forma se evita reconfigurar los filtros de las plantillas más frecuentemente utilizadas, lo que lleva a un ahorro del tiempo de administración.

Plantillas de listado

En el menú superior **Estado**, panel lateral **Mis listados** se encuentra el enlace **Añadir** que muestra una ventana con las plantillas disponibles agrupadas por su tipo:

Grupo	Listado	Descripción
General	Licencias	Muestra en detalle el estado de las licencias de los equipos de la red. Consulta "**Listado de Licencias**" en la página **137**.
	Equipos no administrados descubiertos	Muestra los equipos Windows de la red que no tienen el software Cytomic EPDR instalado. Consulta "**Visualizar equipos descubiertos**" en la página **112**.
	Equipos con nombre duplicado	Muestra los equipos con el mismo nombre y pertenecen al mismo dominio. Consulta "**Listado Equipos con nombre duplicado**" en la página **174**.
	Software	Muestra el software instalado en los equipos del parque informático. Consulta "**Listado de software**" en la página **173**.
	Hardware	Muestra el hardware instalado en los equipos del parque informático. Consulta "**Listado de hardware**" en la página **171**.

Tabla 4.3: listado de plantillas disponibles en Cytomic EPDR

Grupo	Listado	Descripción
Seguridad	Estado de protección de los equipos	Muestra en detalle el estado del módulo de la protección instalada en los equipos. Consulta "**Listado de Estado de protección de los equipos**" en la página **400**.
	Actividad del malware y PUPS	Muestra el listado de las amenazas encontradas en los equipos protegidos con Cytomic EPDR. Consulta "**Listado de Actividad de malware / PUP**" en la página **414**.
	Actividad de exploits	Muestra el número de ataques por explotación de vulnerabilidades recibidos en los equipos Windows de la red. Consulta "**Listado de Actividad de exploits**" en la página **417**.
	Programas actualmente bloqueados en clasificación	Muestra una tabla con aquellos ficheros que, sin haber sido completada su clasificación, Cytomic EPDR ha detectado de forma preliminar algún riesgo en su ejecución. Consulta "**Listado de Programas actualmente bloqueados en clasificación**" en la página **404**.
	Amenazas detectadas por el antivirus	Ofrece información consolidada y completa de todas las detecciones realizadas en todas las plataformas soportadas y desde todos los vectores de infección analizados. Consulta "**Listado de Amenazas detectadas por el antivirus**" en la página **419**.
	Intentos de intrusión bloqueados	Muestra los ataques de red bloqueados por el cortafuegos del equipo. Consulta "**Listado de Intentos de intrusión bloqueados**" en la página **430**.
	Dispositivos bloqueados	Muestra en detalle todos los equipos de la red que tienen establecida alguna limitación en el acceso a sus periféricos. Consulta "**Listado de Dispositivos bloqueados**" en la página **424**.
	Conexiones bloqueadas	Muestra las conexiones que fueron bloqueadas por el cortafuegos local. Consulta "**Listado de Conexiones bloqueadas**" en la página **427**.

Tabla 4.3: listado de plantillas disponibles en Cytomic EPDR

Grupo	Listado	Descripción
Gestión de parches	Estado de gestión de parches	Muestra en detalle todos los equipos de la red compatibles con Cytomic Patch Consulta "**Listado Estado de gestión de parches**" en la página **328**.
	Parches disponibles	Muestra el detalle de todos los parches sin instalar en los equipos de la red y publicados por Cytomic. Consulta "**Parches disponibles**" en la página **326**.
	Historial de instalaciones	Muestra los parches que Cytomic EPDR intentó instalar y los equipos que los recibieron en un intervalo determinado. Consulta "**Listado Historial de instalaciones**" en la página **338**.
	Programas "End of Life"	Muestra la información relativa al "end of life" de los programas instalados en los equipos de la red, agrupados según el plazo restante. Consulta"**Listado Programas End of Life**" en la página **336**.
	Parches excluidos	Muestra los pares equipo - parche que son excluidos de su instalación. Consulta "**Listado Parches excluidos**" en la página **342**.
Control de actividad	Accesos a páginas web por categoría	Muestra las visitas de los usuarios de la red a las páginas web agrupadas por su categoría. Consulta "**Categorías más accedidas (top 10)**" en la página **396**.
	Accesos a páginas web por equipo	Muestra las visitas de los usuarios de la red a las páginas web agrupadas por dispositivo. Consulta "**Categorías más accedidas por equipo (top 10)**" en la página **397**.
	Programas bloqueados por el administrador	Muestra los intentos de ejecución de programas bloqueados por el administrador en los equipos de la red. Consulta "**Listados de bloqueo de programas**" en la página **375**.

Tabla 4.3: listado de plantillas disponibles en Cytomic EPDR

Grupo	Listado	Descripción
Protección de datos	Estado del cifrado	Muestra toda la información referente a los equipos de la red compatibles con la funcionalidad de cifrado. Consulta "**Listado Estado del cifrado**" en la página **366**.
	Estado de Data Control	Muestra el estado del módulo Cytomic Data Watch de Cytomic EPDR. Consulta "**Listado Estado de Data Control**" en la página **288**.
	Archivos con información personal	Muestra todos los ficheros PII encontrados, así como su tipo, localización y otra información relevante. Consulta "**Listado Archivos con información personal**" en la página **293**.
	Equipos con información personal	Muestra el número de ficheros PII encontrados en cada uno de los equipos de la red. Consulta "**Listado Equipos con información personal**" en la página **296**.
	Archivos eliminados por el administrador	Muestra el estado de los ficheros eliminados por el administrador mediante el módulo Cytomic Data Watch. Consulta "**Listado Archivos eliminados por el administrador**" en la página **300**.

Tabla 4.3: listado de plantillas disponibles en Cytomic EPDR

Adicionalmente, existen otras plantillas accesibles directamente desde el menú de contexto de ciertos listados o desde algunos widgets del panel de control. Consulta el capítulo correspondiente al widget en cuestión.

Secciones de los listados

Los listados incorporan un conjunto de herramientas comunes que facilitan su interpretación. A continuación se muestran las partes principales de un listado de ejemplo.

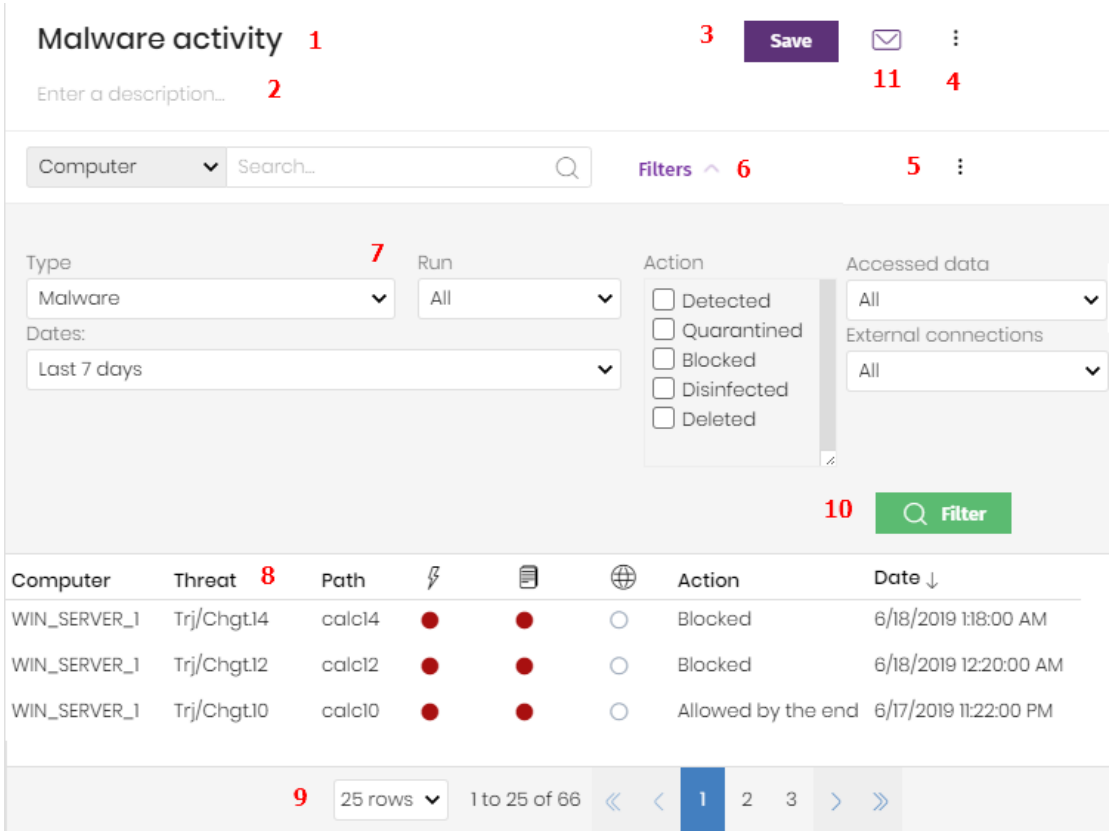


Figura 4.10: elementos de las pantallas de listados

- **Nombre del listado (1)**: identifica el tipo de datos que se muestran en el listado.
- **Descripción (2):** caja de texto libre donde el administrador puede indicar el objetivo del listado.
- **Salvar (3):** botón que salva la vista actual y crea un nuevo listado en el árbol Mis listados
- **Menú de contexto (4):** menú desplegable con las operaciones disponibles sobre el listado (copiar y eliminar. Consulta el apartado "**Operaciones con listados**".
- **Menú de contexto (5)**: menú desplegable con las opciones de exportación del listado.
- **Enlace de herramientas de filtrado y búsqueda (6)**: al hacer clic se despliega un panel con las herramientas de filtrado. Una vez configuradas haz clic en el botón **Filtrar (10)** para aplicarlas.
- **Bloque de controles de filtrado y búsqueda (7)**: filtra los datos mostrados en el listado.
- **Criterio de ordenación (8)**: al hacer clic en el nombre de las columnas el listado se ordena tomando como referente esa columna. Haz clic varias veces en el nombre de la columna para cambiar el sentido de la ordenación (ascendente o descendente). El sentido de ordenación se muestra mediante una fecha ascendente ↑ o descendente ↓. Si accedes a la consola de administración desde un dispositivo móvil de menor tamaño, haz clic en el icono situado en la esquina inferior

derecha para desplegar un menú con el nombre de las columnas.

- **Paginación (9)**: en el pie de la página se incluyen una serie de controles para navegar la información mostrada.

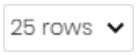
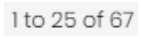
Icono	Descripción
	Selector del número de filas mostradas por página.
	Intervalo de registros mostrados del total disponible.
	Retroceso a la primera página.
	Retroceso a la página anterior a la actual.
	Acceso directo por número de páginas.
	Avance a la siguiente página.
	Avance a la última página.

Tabla 4.4: herramientas de paginación

- **Envío programado del listado (11)**: Cytomic EPDR permite el envío de correos electrónicos con el contenido del listado, adjuntando una exportación de los datos en formato csv. Consulta el capítulo "**Envío programado de informes y listados**" en la página **479** para obtener más información.

Operaciones con listados

En el menú superior **Estado**, panel lateral **Mis listados** se muestran todos los listados que el administrador a creado previamente y los listados que Cytomic EPDR incorpora por defecto. Consulta "**Listados incluidos por defecto**".

Crear un listado personalizado

Hay varias formas de añadir un nuevo listado personalizado / vista:

- **Desde el panel lateral Mis listados**
  - Al hacer clic sobre el link **Añadir** del panel **Mis listados** se muestra una ventana con un desplegable que contiene las plantillas disponibles.
  - Elige una plantilla, configura las herramientas de filtrado, modifica el nombre y la descripción y pulsa el botón **Guardar (3)**.
- **Desde un panel del dashboard**
  - Haz clic en un widget en el panel de control para abrir su plantilla asociada.
  - Haz clic en el menú de contexto **(4)** y selecciona **Copiar**. Se creará un nuevo listado.
  - Modifica los filtros, el nombre y la descripción del listado y haz clic en el botón **Guardar (3)**.

- **Desde un listado ya creado**
  - Haz una copia de un listado ya generado mediante el menú contextual **(4)** y haz clic en **Copiar**. Se generará un nuevo listado con el nombre "copia de...".
  - Modifica los filtros, el nombre y la descripción del listado y haz clic en el botón **Guardar (3)**.
- **Desde el menú de contexto del panel Mis listados**

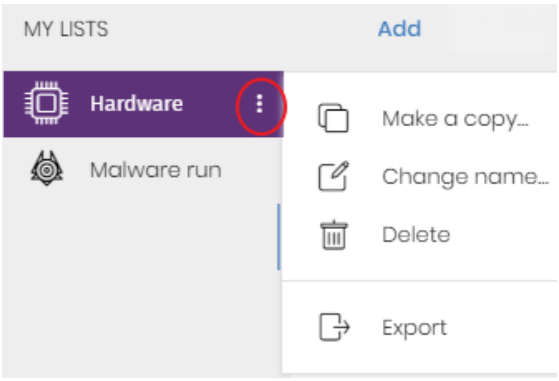


Figura 4.11: menú de contexto de los listados accesibles desde el Panel de listados

- Haz clic en el menú de contexto asociado al listado a copiar.
- Haz clic en **Hacer una copia**. Se creará una nueva vista de la plantilla con el nombre "copia de...".
- Modifica los filtros, el nombre y la descripción del listado y haz clic en el botón **Guardar (3)**.

Borrar un listado

Puedes borrar un listado de varias maneras:

- **Desde el panel Mis listados**
  - Haz clic el menú de contexto asociado al nombre del listado en el panel **Mis Listados**.
  - Haz clic en el icono .
- **Desde el propio listado**
  - Haz clic en el menú de contexto **(4)**.
  - Haz clic en el icono del menú desplegable.

Copiar un listado

Puedes copiar un listado de varias maneras:

- Desde el panel **Mis listados:**
  - Haz clic en el menú de contexto asociado al nombre del listado en el panel **Mis listados**.
  - Haz clic en el icono .
- Desde el propio listado:
  - Haz clic en el menú de contexto **(4)**.

- Haz clic en el icono del menú desplegado.

Exportar un listado

El botón de menú **(5)** incluye la opción de exportar el listado en formato csv. La exportación de listados en formato csv amplía la información mostrada en los listados de la consola Web. Estos campos están documentados más adelante en esta guía.

Personalizar un listado

- Asigna un nuevo nombre al listado **(1)**. Por defecto la consola forma un nuevo nombre para el listado añadiendo la cadena "Nuevo" al tipo de listado o "Copia" si el listado es la copia de uno anterior.
- Asigna una descripción **(2)**: este paso es opcional.
- Haz clic en el enlace **Filtros (6)** para desplegar las herramientas de búsqueda y filtrado.
- Haz clic en **Filtrar (10)** para aplicar el filtro configurado con el objetivo de comprobar si el filtrado configurado se ajusta a las necesidades. En el cuerpo del listado se mostrará la búsqueda resultado.
- Haz clic en el botón **Guardar (3)**. El listado se añadirá en el panel de la izquierda bajo **Mis listados**, y será accesible a partir de ese momento haciendo clic en su nombre.

Programar el envío de un listado

- **Desde el menú de contexto del panel Listados:**
  - Haz clic en el menú de contexto del listado que quieres enviar y elige la opción **Programar envío**.
  - Se mostrará una ventana con la información necesaria para enviar de forma automática la información.
- **Desde el propio listado:**
  - Haz clic en el icono **(11)** . Se mostrará una ventana con la información necesaria para enviar de forma automática la información.

*Consulta el capítulo "**Envío programado de informes y listados**" en la página **479** para obtener más información*

Acciones sobre equipos en los listados

En algunos listados como **Licencias** y **Estado de protección de los equipos** se incorporan casillas de selección por cada equipo. Al marcar uno o más equipos, se muestra la barra de acciones en la parte superior de la ventana, para facilitar la administración de los puestos de usuario y servidores seleccionados.

Listados incluidos por defecto

La consola de administración incluye varios listados pre generados:

- Estaciones y portátiles desprotegidos.
- Malware ejecutado.
- PUPs ejecutados.
- Servidores desprotegidos.
- Hardware
- Software

Estaciones y portátiles desprotegidos

Localiza todos los equipos de escritorio y portátiles, sin importar el sistema operativo instalado, considerados vulnerables a las amenazas debido a un problema en el funcionamiento de la protección:

- Equipos en proceso de instalación del software Cytomic EPDR o con error en la instalación.
- Equipos con la protección desactivada o en estado de error.
- Equipos sin licencia asignada o con licencia caducada.
- Consulta el apartado "**Listado de Estado de protección de los equipos**" en la página **400**.

Malware ejecutado

Localiza los equipos de la red que han ejecutado una amenaza en este último mes. Estos equipos son susceptibles de estar infectados por una de estas razones:

- El administrador desbloqueó un elemento desconocido antes de su clasificación y resulto ser malware.
- El administrador excluyó del análisis una amenaza conocida para habilitar su ejecución.
- El equipo se encuentra en modo **Audit** o en modo **Hardening** y la amenaza ya existía previamente a la instalación de Cytomic EPDR. Consulta el apartado "**Actividad de malware / PUP**" en la página **388**.

PUPs ejecutados

Localiza los equipos de la red que han ejecutado un programa no deseado en este último mes. Estos equipos son susceptibles de estar infectados por una de estas razones:

- El administrador desbloqueó un elemento desconocido antes de su clasificación y resultó ser un programa no deseado.
- El administrador excluyó del análisis un programa no deseado para habilitar su ejecución.
- El equipo se encuentra en modo **Audit** o en modo **Hardening** y el programa no deseado ya existían previamente a la instalación de Cytomic EPDR. Consulta el apartado "**Actividad de malware / PUP**" en

la página 388.

Servidores desprotegidos

Localiza todos los equipos de tipo servidor, sin importar el sistema operativo instalado, considerados vulnerables a las amenazas debido a un problema en el funcionamiento de la protección:

- Servidores en proceso de instalación del software Cytomic EPDR o con error en la instalación.
- Servidores con la protección desactivada o en estado de error.
- Servidores sin licencia asignada o con licencia caducada. Consulta el apartado "**Listado de Estado de protección de los equipos**" en la página 400.

Software

Muestra una relación de los programas instalados en el parque informático. Consulta el apartado "**Listado de software**" en la página 173.

Hardware

Muestra una relación de los componentes hardware instalados en el parque informático. Consulta el apartado "**Listado de hardware**" en la página 171.

Capítulo 5

Control y supervisión de la consola de administración

En este capítulo se detallan los recursos implementados en Cytomic EPDR para controlar y supervisar las acciones realizadas por los administradores de red que acceden a la consola web de gestión.

Esta supervisión y control se implementa en forma de tres recursos:

- Cuenta de usuario.
- Roles asignados a las cuentas de usuario.
- Registro de la actividad de las cuentas de usuario.

CONTENIDO DEL CAPÍTULO

Concepto de cuenta de usuario

Es un recurso gestionado por Cytomic EPDR, formado por un conjunto de información que el sistema utiliza para regular el acceso de los administradores a la consola web, y establecer las acciones que éstos podrán realizar sobre los equipos de los usuarios.

Las cuentas de usuario son utilizadas únicamente por los administradores de IT que acceden a la consola web de Cytomic EPDR. Cada administrador de IT tiene una o mas cuentas de usuario personales.

A diferencia del resto del documento, donde la palabra "usuario" se refiere a la persona que utiliza un equipo o dispositivo, en este capítulo "usuario" se asocia a la cuenta de usuario que el administrador utiliza para acceder a la consola web.

Estructura de una cuenta de usuario

Una cuenta de usuario está formada por los siguientes elementos:

- **Login de la cuenta**: asignada en el momento de la creación de la cuenta, su objetivo es identificar

al administrador que accede a la consola.

- **Contraseña de la cuenta**: asignada una vez creada la cuenta, regula el acceso a la consola de administración.
- **Rol asignado**: asignado una vez creada la cuenta de usuario, establece los equipos sobre los cuales la cuenta tiene capacidad de administración, y las acciones que puede ejecutar sobre los mismos.

Verificación en dos pasos

Cytomic EPDR soporta el estándar 2FA (Two Factor Authentication) para añadir una capa de seguridad adicional a la establecida en el esquema básico "usuario - contraseña". De esta manera, cuando el administrador de la red accede a la consola web se introduce un nuevo elemento en el sistema de autenticación básico: un código que solo posee el propietario de la cuenta. Este código es aleatorio y únicamente puede generase en un dispositivo concreto, normalmente el teléfono móvil o tablet personal del administrador del Cytomic EPDR.

Requisitos para activar 2FA

- Acceso a un teléfono móvil o tablet personal con cámara de fotos integrada.
- Aplicación Google Authenticator instalada, o una equivalente. Descarga la aplicación gratuita en el enlace **https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl**

Activar 2FA

- En el menú superior haz clic en la cuenta de usuario y en la opción **Configurar mi perfil**. Se abrirá la ventana de la **Cuenta Cytomic**.

Figura 5.1: acceso a la Cuenta Cytomic

- Haz clic en el menú lateral **Inicio de sesión** y en el enlace **Activar** de la sección **Verificación en dos pasos**. Se mostrará la ventana de configuración de la aplicación Google Authenticator o equivalente instalada en el dispositivo móvil.
- Escanea el código QR mostrado en la ventana con la aplicación Google Authenticator o equivalente, introduce el código generado en el apartado **Introduce el código que te muestra la app** y haz clic en el botón **Verificar**. Desde este momento el dispositivo quedará enlazado al servicio Cytomic EPDR y generará códigos de acceso aleatorios que caducarán cada poco tiempo.

Acceder a la consola mediante una cuenta con 2FA activado

Para acceder a la consola con una cuenta de usuario que tiene la funcionalidad 2FA activada introduce el usuario, contraseña y un código generado por el dispositivo vinculado a la cuenta.

Forzar la activación de 2FA a todos los usuarios de la consola

Para forzar la activación de 2FA a todos los usuarios de la consola es necesario que la cuenta de usuario que forzará la activación tenga permisos de **Gestionar usuarios y roles** y que además tenga visibilidad completa sobre el parque. Consulta el apartado "**Gestionar usuarios y roles**" para una descripción de este permiso, y el apartado "**Estructura de un rol**" para configurar los grupos sobre los que tiene permisos el rol.

- En el menú superior **Configuración** haz clic en la pestaña **Seguridad**.
- Activa la opción **Exigir tener activada la verificación en dos pasos para acceder a esta cuenta**.
- Si la cuenta de usuario que activa la funcionalidad 2FA para todos los usuarios de la consola no tiene activada la verificación en dos pasos para su propia cuenta se mostrará una ventana de aviso que le permitirá acceder a la **Cuenta Cytomic** para activarlo. Consulta el apartado "**Activar 2FA**".

Concepto de rol

Es una configuración específica de permisos de acceso a la consola, que se aplica a una o más cuentas de usuario. De esta forma, un administrador concreto esta autorizado a ver o modificar determinados recursos de la consola, dependiendo del rol asignado a la cuenta de usuario con la que accedió a Cytomic EPDR.

Una cuenta de usuario tiene un único rol asignado aunque un rol puede estar asignado a una o más cuentas de usuario.

Estructura de un rol

Un rol está formado por los siguientes elementos:

- **Nombre del rol**: designado en el momento de la creación del rol, su objetivo es meramente identificativo.
- **Grupos sobre los que tiene permisos**: restringe el acceso a determinados equipos de la red. Para configurar esta restricción es necesario especificar las carpetas del árbol de grupos a las cuales la cuenta de usuario tiene acceso.
- **Juego de permisos**: determina las acciones concretas que las cuentas de usuario pueden ejecutar sobre los equipos que pertenecen a los grupos definidos con accesibles.

¿Por qué son necesarios los roles?

En un departamento de IT de tamaño pequeño, todos los técnicos van a acceder a la consola como administradores sin ningún tipo de límite; sin embargo, en departamentos medianos o grandes con un parque informático amplio para administrar, es muy posible que sea necesario organizar o segmentar el acceso a los equipos, aplicando tres criterios:

- **Según la cantidad de equipos a administrar.**

Redes de tamaño medio/grande o redes pertenecientes a delegaciones de una misma empresa pueden requerir distribuir y asignar equipos a técnicos concretos. De esta forma, los dispositivos de una delegación administrados por un técnico en particular serán invisibles para los técnicos que administran los dispositivos de otras delegaciones.

También pueden existir restricciones de acceso a datos delicados de ciertos usuarios. En estos casos se suele requerir una asignación muy precisa de los técnicos que van a poder manipular los dispositivos que los contienen.

- **Según el cometido del equipo a administrar.**

Según la función que desempeñe, un equipo o servicio se puede asignar a un técnico experto en ese campo: por ejemplo, los servidores de correo Exchange se asignan a un grupo de técnicos especialistas, y de la misma forma, otros equipos como los dispositivos Android no serán visibles para este grupo.

- **Según los conocimientos o perfil del técnico.**

Según las capacidades del técnico o de su función dentro del departamento de IT, se puede asignar únicamente un acceso de monitorización/validación solo lectura o, por el contrario, uno más avanzado, como el de modificación de las configuraciones de seguridad de los equipos. Por ejemplo, es frecuente encontrar en compañías grandes un determinado grupo de técnicos dedicados únicamente a desplegar software en los equipos de la red.

Estos tres criterios se pueden solapar, dando lugar a una matriz de configuraciones muy flexible y fácil de establecer y mantener, que permite delimitar perfectamente las funciones de la consola para cada técnico, en función de la cuenta de usuario con la que acceden al sistema.

El rol Control total

Una licencia de uso de Cytomic EPDR incluye un rol de **Control total** predefinido. A este rol pertenece la cuenta de administración creada por defecto, y con ella es posible ejecutar todas las acciones disponibles en la consola sobre todos los equipos integrados en Cytomic EPDR.

El rol **Control total** no se puede borrar, modificar ni visualizar, y cualquier cuenta de usuario puede pertenecer a este rol previa asignación en la consola Web.

El rol Solo lectura

Está especialmente indicado para aquellos administradores de red encargados de la vigilancia del parque informático, pero que no poseen los permisos suficientes para realizar modificaciones, como por ejemplo editar configuraciones o lanzar análisis bajo demanda.

Los permisos activados son los siguientes:

- Ver configuraciones de seguridad para estaciones y servidores.
- Ver configuraciones de seguridad para dispositivos Android.
- Ver configuraciones de Data Control.
- Ver configuraciones de cifrado.
- Ver configuraciones de gestión de parches.
- Visualizar detecciones de amenazas.
- Visualizar accesos a páginas web y spam.
- Acceso a informes.

El rol Solo lectura tiene permisos de lectura sobre todos los grupos de equipos integrados en Cytomic EPDR.

Concepto de permiso

Un permiso regula el acceso a un aspecto concreto de la consola de administración. Existen varios permisos que establecen el acceso a otros tantos aspectos de la consola de Cytomic EPDR. Una configuración particular de todos los permisos disponibles forma un rol, que puede ser asignado a una o más cuentas de usuario.

Los permisos implementados en Cytomic EPDR son:

- **Usuarios**
  - Gestionar usuarios y roles.
- **Licencias**
  - Asignar licencias.
- **Equipos**
  - Modificar el árbol de equipos.
  - Añadir, descubrir y eliminar equipos.
  - Modificar configuración de red proxys y caché.
  - Configurar ajustes por equipo actualizaciones, contraseñas etc.
  - Reiniciar equipos y reinstalar la protección.
  - Aislar equipos.
- **Seguridad**
  - Configurar seguridad para estaciones y servidores.
  - Ver configuraciones de seguridad para estaciones y servidores.
  - Configurar seguridad para dispositivos Android.

- Ver configuraciones de seguridad para dispositivos Android.
- Utilizar la protección antirrobo para dispositivos Android localizar, borrar, bloquear, etc.
- Visualizar detecciones y amenazas.
- Visualizar accesos a páginas web y spam.
- Lanzar análisis y desinfectar.
- Excluir temporalmente amenazas Malware, PUP y Bloqueados.
- Configurar gestión de parches.
- Instalar y desinstalar parches.
- Visualizar parches disponibles.

- **Protección de datos**
  - Configurar Data Control.
  - Ver configuraciones de Data Control.
  - Buscar información en los equipos.
  - Visualizar inventario de información personal.
  - Eliminar y restaurar archivos.
  - Configurar cifrado de equipos.
  - Acceder a las claves de recuperación de unidades cifradas.

- **ADVANCED VISUALIZATION TOOL**
  - Acceder a información avanzada de seguridad Advanced Reporting Tool excepto Data Access Control.
  - Acceder a información de acceso a archivos Data Access Control en Advanced Reporting Tool.
  - Acceder a información avanzada de Data Control.

Descripción de los permisos implementados

Gestionar usuarios y roles

- **Al activar**: el usuario de la cuenta puede crear, borrar y editar cuentas de usuario y roles.
- **Al desactivar**: el usuario de la cuenta deja de poder crear, borrar y editar cuentas de usuario y roles. Se permite ver el listado de usuarios dados de alta y los detalles de las cuentas, pero no el listado de roles creados.

Asignar licencias

- **Al activar**: el usuario de la cuenta puede asignar y retirar licencias de los equipos gestionados.
- **Al desactivar**: el usuario de la cuenta no puede asignar y retirar licencias, pero puede ver si los

equipos tienen licencias asignadas.

Modificar el árbol de equipos

- **Al activar**: el usuario de la cuenta tiene pleno acceso al árbol de grupos y puede crear y eliminar grupos, y mover equipos a grupos ya creados.
- **Al activar con conflicto de permisos**: debido a herencia, modificar el árbol de equipos puede implicar un cambio de configuración para los dispositivos. Si alguno de los permisos que permiten al administrador cambiar las configuraciones están desactivados, solo se permitirá crear grupos, eliminar grupos vacíos y cambiar el nombre de un grupo. Los permisos que permiten cambiar las configuraciones son:
  - Modificar configuración de red proxys y caché.
  - Modificar ajustes por equipo actualizaciones, contraseñas, etc.
  - Configurar seguridad para estaciones y servidores.
  - Configurar seguridad para dispositivos Android.
  - Lanzar análisis y desinfectar.
  - Configurar gestión de parches.
  - Instalar y desinstalar parches.
  - Configurar inventario, seguimiento y búsqueda de información sensible.
- **Al desactivar**: el usuario de la cuenta puede visualizar el árbol de carpetas y las configuraciones asignadas a cada grupo, pero no puede crear nuevos grupos ni mover equipos. Puede cambiar la configuración de un grupo, ya que esta acción queda regulada con el permiso **Configurar seguridad para estaciones y servidores**, **Configurar seguridad para dispositivos Android**, **Configurar gestión de parches, Configurar cifrado de equipos**, **Configurar Data Control.**

Añadir, descubrir y eliminar equipos

- **Al activar**: el usuario de la cuenta puede distribuir el instalador entre los equipos de la red e integrarlos en la consola, eliminarlos y configurar toda la funcionalidad relativa al descubrimiento de puestos no gestionados: asignar y retirar el rol de descubridor a los equipos, editar las opciones de descubrimiento, lanzar descubrimientos inmediatos e instalar el agente de Cytomic de forma remota desde los listados de equipos descubiertos.
- **Al desactivar**: el usuario de la cuenta no puede descargar el instalador, ni por lo tanto distribuirlo entre los equipos de la red. Tampoco puede eliminar equipos previamente integrados ni gestionar la funcionalidad relativa al descubrimiento de equipos no gestionados.

Modificar configuración de red proxys caché

- **Al activar**: el usuario de la cuenta puede crear nuevas configuraciones de tipo **Configuración de red**, editar o borrar las existentes y asignarlas a los equipos integrados en la consola.
- **Al desactivar**: el usuario de la cuenta deja de poder crear nuevas configuraciones de tipo **Configuración de red**, borrar las existentes o cambiar la asignación de los equipos integrados a la

consola.

Puesto que un cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de la configuración de red asignada, al desactivar Modificar configuración de red proxys caché se obliga también a desactivar el permiso Modificar el árbol de equipos,

Configurar ajustes por equipo actualizaciones, contraseñas etc.

- **Al activar**: el usuario de la cuenta puede crear nuevas configuraciones de tipo **Ajustes por equipo**, editar y borrar las ya creadas y asignar a los equipos integrados en la consola.
- **Al desactivar**: el usuario de la cuenta deja de poder crear nuevas configuraciones de tipo **Ajustes por equipo**, borrar las existentes o cambiar la asignación de los equipos integrados a la consola.

Puesto que un cambio de carpeta de un equipo en el árbol de carpetas puede provocar un cambio de configuración de Ajustes por equipo asignado, al desactivar Ajustes por equipo se obliga también a desactivar el permiso Modificar el árbol de equipos.

Reiniciar y reparar equipos

- **Al activar**: el usuario de la cuenta puede reiniciar equipos desde los listados de equipos en estaciones y servidores Windows, Linux y macOS. También puede iniciar la reinstalación remota del software Cytomic EPDR en equipos Windows.
- **Al desactivar**: el usuario de la cuenta deja de poder reiniciar equipos y de reinstalar remotamente el software Cytomic EPDR.

Aislar equipos

- **Al activar**: el usuario de la cuenta puede aislar y dejar de aislar equipos desde el menú superior **Equipos** y desde los listados **Licencias** y **Equipos protegidos** seleccionando en el menú de contexto o en barra de acciones **Aislar equipos**, para estaciones y servidores Windows.
- **Al desactivar**: el usuario de la cuenta deja de poder aislar equipos.

Configurar seguridad para estaciones y servidores

Puesto que el cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de Estaciones y servidores, al desactivar Configurar seguridad para estaciones y servidores se obliga también a desactivar el permiso Modificar el árbol de equipos,

- **Al activar**: el usuario de la cuenta puede crear, editar, borrar y asignar configuraciones de seguridad para estaciones y servidores Windows, Linux y macOS.

- **Al desactivar**: el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de seguridad para estaciones y servidores Windows, Linux y macOS.

Al desactivar este permiso se mostrará el permiso **Ver configuraciones de seguridad para estaciones y servidores**.

Ver configuraciones de seguridad para estaciones y servidores

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar la seguridad para estaciones y servidores.

- **Al activar**: el usuario de la cuenta puede únicamente visualizar las configuraciones de seguridad creadas, así como ver la configuración de un equipo o de un grupo.
- **Al desactivar**: el usuario de la cuenta deja de poder ver las configuraciones de seguridad creadas, y tampoco podrá acceder a las configuraciones asignadas de cada equipo.

Configurar seguridad para dispositivos Android

- **Al activar**: el usuario de la cuenta puede crear, editar, borrar y asignar configuraciones de dispositivos Android.
- **Al desactivar**: el usuario de la cuenta deja de poder crear, editar, borrar y asignar configuraciones de dispositivos Android.

Puesto que el cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de dispositivos Android, al desactivar Configurar seguridad para dispositivos Android se obliga también a desactivar el permiso Modificar el árbol de equipos.

Al desactivar este permiso se mostrará el permiso **Ver configuraciones de seguridad para dispositivos Android**, explicado a continuación.

Ver configuraciones de seguridad para dispositivos Android

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar la seguridad para dispositivos Android.

- **Al activar**: el usuario de la cuenta puede únicamente visualizar las configuraciones dispositivos Android creadas, así como ver la configuración de un dispositivo Android equipo o de un grupo.
- **Al desactivar**: el usuario de la cuenta deja de poder ver las configuraciones de dispositivos Android creadas, y tampoco podrá acceder a las configuraciones asignadas de cada dispositivo Android.

Utilizar la protección antirrobo para dispositivos Android localizar, borrar, bloquear, etc.

- **Al activar**: el usuario de la cuenta puede visualizar el mapa de geolocalización y operar con el panel de acciones que permite enviar tareas antirrobo a los dispositivos Android.
- **Al desactivar**: el usuario de la cuenta no puede visualizar el mapa de geolocalización ni operar con el panel de acciones que permite enviar tareas antirrobo a los dispositivos Android.

Visualizar detecciones y amenazas

- **Al activar**: el usuario de la cuenta puede acceder a los paneles y listados de la sección **Seguridad** en el menú superior **Estado,** y crear nuevos listados con filtros personalizados.
- **Al desactivar**: el usuario de la cuenta no puede visualizar ni acceder a los paneles y listados de la sección **Seguridad** en el menú superior **Estado,** ni crear nuevos listados con filtros personalizados.

El acceso a la funcionalidad relativa a la exclusión y desbloqueo de amenazas y elementos desconocidos se establece mediante el permiso Excluir temporalmente amenazas Malware, PUP y Bloqueados.

Visualizar accesos a páginas web y spam

- **Al activar**: el usuario de la cuenta puede acceder a los paneles y listados de la sección **Accesos web y spam** en el menú superior **Estado.**
- **Al desactivar**: el usuario de la cuenta ya no puede acceder a los paneles y listados de la sección **Accesos web y spam** en el menú superior **Estado**.

Lanzar análisis y desinfectar

- **Al activar**: el usuario de la cuenta puede crear editar, modificar y borrar tareas de tipo análisis y desinfección.
- **Al desactivar**: el usuario de la cuenta no puede crear, editar, modificar ni borrar las tareas ya creadas de tipo análisis. Únicamente podrá listar las tareas y visualizar su configuración.

Excluir temporalmente amenazas Malware, PUP y Bloqueados

- **Al activar**: el usuario de la cuenta puede desbloquear, no volver a detectar, bloquear, dejar de permitir y cambiar el comportamiento ante reclasificaciones de malware, PUP y desconocidos en clasificación.
- **Al desactivar**: el usuario de la cuenta no podrá desbloquear, no volver a detectar, bloquear, dejar de permitir y cambiar el comportamiento ante reclasificaciones de malware, PUP y desconocidos

en clasificación.

> *Es necesario activar Visualizar detecciones y amenazas para poder ejercer completamente Excluir temporalmente amenazas Malware, PUP y Bloqueados.*

Configurar gestión de parches

- **Al activar**: el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de gestión de parches para estaciones y servidores Windows.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de gestión de parches para estaciones y servidores Windows.

> *Puesto que el cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de Gestión de parches, al desactivar Configurar gestión de parches se obliga también a desactivar el permiso Modificar el árbol de equipos.*

Al desactivar este permiso se mostrará el permiso **Visualizar configuraciones de gestión de parches**.

Visualizar configuraciones de gestión de parches

> *Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar gestión de parches.*

- **Al activar**: el usuario de la cuenta podrá únicamente visualizar las configuraciones de gestión de parches creadas, así como ver la configuración asignadas a un equipo o a un grupo.
- **Al desactivar**: el usuario de la cuenta dejará de poder ver las configuraciones Gestión de parches creadas, y tampoco podrá acceder a las configuraciones asignadas a cada equipo.

Instalar / desinstalar y excluir parches

> *Puesto que el cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de Instalar / desinstalar parches, al desactivar Instalar / desinstalar parches se obliga también a desactivar el permiso Modificar el árbol de equipos.*

- **Al activar**: el usuario de la cuenta podrá crear tareas de parcheo, desinstalación y exclusión de parches, así como acceder a los listados **Parches disponibles**, **Programas "End of life"**, **Historial de instalaciones** y **Parches excluidos**.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear tareas de parcheo, desinstalación y exclusión de parches.

Visualizar parches disponibles

Este permiso solo es accesible cuando se ha deshabilitado el permiso Instalar / desinstalar y excluir parches.

- **Al activar**: el usuario de la cuenta podrá acceder a los listados **Estado de gestión de parches**, **Parches disponibles**, **Programas "End of life"** e **Historial de instalaciones**.
- **Al desactivar**: el usuario de la cuenta dejará de poder acceder a los listados **Parches disponibles**, **Programas "End of life"** e **Historial de instalaciones**.

Configurar bloqueo de programas

Puesto que el cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de Bloqueo de programas, al desactivar Configurar bloqueo de programas se obliga también a desactivar el permiso Modificar el árbol de equipos.

- **Al activar**: el usuario de la cuenta puede crear, editar, borrar y asignar configuraciones de bloqueo de programas para estaciones y servidores Windows.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de bloqueo de programas para estaciones y servidores Windows.

Al desactivar este permiso se mostrará el permiso **Ver configuraciones de bloqueo de programas**.

Ver configuraciones de bloqueo de programas

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar bloqueo de programas.

- **Al activar**: el usuario de la cuenta puede únicamente visualizar las configuraciones de bloqueo de programas, así como ver la configuración de un equipo o de un grupo.
- **Al desactivar**: el usuario de la cuenta deja de poder ver las configuraciones de bloqueo de programas creadas, y tampoco podrá acceder a las configuraciones asignadas de cada equipo.

Configurar Data Control

- **Al activar**: el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de Data Control en equipos Windows.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de Data Control en equipos Windows.

Ver configuraciones de Data Control

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar inventario, seguimiento y búsqueda de información sensible.

- **Al activar**: el usuario de la cuenta podrá únicamente visualizar las configuraciones de Data Control, así como ver la configuración de un equipo o de un grupo.
- **Al desactivar**: el usuario de la cuenta dejará de poder ver las configuraciones de Data Control creadas, y tampoco podrá acceder a las configuraciones asignadas de cada equipo.

Buscar información en los equipos

- **Al activar**: el usuario de la cuenta podrá acceder al widget de **Búsquedas** para localizar ficheros por nombre y contenido almacenados en los equipos de los usuarios.
- **Al desactivar**: el usuario de la cuenta dejará de poder acceder al widget Búsquedas.

Visualizar inventario de información personal

- **Al activar**: el usuario de la cuenta podrá acceder a los listados **Archivos con información personal** y **Equipos con información personal**, así como a los widgets **Archivos con información personal**, **Equipos con información personal** y **Archivos por tipo de información personal**.
- **Al desactivar**: el usuario de la cuenta dejará de tener acceso a los listados **Archivos con información personal** y **Equipos con información personal**, así como a los widgets **Archivos con información personal**, **Equipos con información personal** y **Archivos por tipo de información personal**.

Eliminar y restaurar archivos

- **Al activar**: el usuario de la cuenta puede acceder a la opción **Eliminar** del menú de contexto en el listado **Archivos con información personal** para borrar y restaurar ficheros.
- **Al desactivar**: el usuario de la cuenta no puede acceder a la opción **Eliminar** del menú de contexto en el listado **Archivos con información personal** y por lo tanto no puede borrar ni restaurar ficheros.

Configurar cifrado de equipos

- **Al activar**: el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de cifrado para equipos Windows.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear, editar, borrar y asignar

configuraciones de cifrado para equipos Windows.

> *Puesto que el cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de Cifrado, al desactivar Configurar cifrado de equipos se obliga también a desactivar el permiso Modificar el árbol de equipos,*

Ver configuraciones de cifrado de equipos

> *Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar cifrado de equipos.*

- **Al activar**: el usuario de la cuenta podrá únicamente visualizar las configuraciones de cifrado de equipos, así como ver la configuración asignadas a un equipo o a un grupo.
- **Al desactivar**: el usuario de la cuenta dejará de poder ver las configuraciones de cifrado creadas, y tampoco podrá acceder a las configuraciones asignadas a cada equipo.

Acceder a las claves de recuperación de unidades cifradas

- **Al activar**: el usuario de la cuenta podrá visualizar las claves de recuperación para los equipos con dispositivos de almacenamiento cifrados y administrados por Cytomic EPDR.
- **Al desactiva**: el usuario de la cuenta no podrá visualizar las claves de recuperación para los equipos con dispositivos de almacenamiento cifrados.

Acceder a información avanzada de seguridad

- **Al activar**: el usuario de la cuenta podrá acceder a la herramienta Advanced Reporting Tool desde el menú superior **Estado**, panel izquierdo **Advanced Visualization Tools** pero la aplicación Data Access Control de Advanced Reporting Tool no es visible con este permiso.
- **Al desactivar**: se impide el acceso a la herramienta Advanced Reporting Tool.

Acceder a información de acceso a archivos

- **Al activar**: el usuario de la cuenta podrá acceder a la herramienta Advanced Reporting Tool desde el menú superior **Estado**, panel izquierdo **Advanced Visualization Tools**. La aplicación Data Access Control de Advanced Reporting Tool es accesible con este permiso.
- **Al desactivar**: se impide el acceso a la herramienta Advanced Reporting Tool.

Acceder a información avanzada de Data Control

- **Al activar**: el usuario de la cuenta podrá acceder a la consola extendida de Data Control desde el menú superior **Estado**, panel izquierdo **Advanced Visualization Tools**.
- **Al desactivar**: el usuario de la cuenta no podrá acceder a la consola extendida de Data Control desde el menú superior **Estado**, panel izquierdo **Advanced Visualization Tools**.

Acceso a la configuración de cuentas de usuarios y roles

En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios.** Aparecerán dos entradas asociadas a la gestión de roles y cuentas de usuario:

- **Usuarios**: crea nuevas cuentas de usuario y definir su pertenencia a uno o varios roles.
- **Roles**: crea y modifica una nueva configuración de acceso a los recursos de Cytomic EPDR.

Solo se puede acceder a las pestañas de **Usuarios y roles** si el usuario tiene asignado el permiso **Gestionar usuarios y roles.**

Crear y configurar cuentas de usuario

Crear, modificar y borrar usuarios

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios.**
- Haz clic en la pestaña **Usuarios** desde donde puedes realizar todas las acciones necesarias relativas a la creación y modificación de cuentas de usuario:
  - **Añadir nueva cuenta de usuario**: haz clic en el botón **Añadir** para añadir un nuevo usuario, establecer la cuenta de correo para el acceso, el rol al que pertenece y una descripción de la cuenta. Al terminar el sistema enviará un correo a la cuenta para generar la contraseña de acceso.
  - **Editar una cuenta de usuario**: haz clic en el nombre del usuario para mostrar una ventana con todos los datos de la cuenta editables.
  - **Borrar o desactivar cuentas de usuarios**: haz clic sobre el icono de una cuenta de usuario para borrarla. Haz clic en una cuenta de usuario y selecciona el interruptor **Bloquear este usuario** para inhabilitar temporalmente el acceso de la cuenta a la consola web. De esta manera, esa cuenta tendrá denegado el acceso a la consola de administración, y si ya está conectado será expulsada de forma inmediata. También dejará de recibir alertas por correo en las direcciones de correo especificadas en su configuración.

Listar los usuarios creados

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios.**
- Haz clic en la pestaña **Usuarios.** Se mostrará un listado con todas las cuentas de usuario creadas en Cytomic EPDR con la información mostrada a continuación:

Campo	Descripción
Nombre de la cuenta	Nombre de la cuenta de usuario.

Tabla 5.1: listado de usuarios

Campo	Descripción
Rol	Rol asignado a la cuenta de usuario.
Cuenta de correo	Cuenta de correo asignado al usuario.
Candado	Indica si la cuenta tiene activada la funcionalidad de 2FA (Verificación en dos pasos / factores, Two Factor Authentication).
Estado	Indica si la cuenta de usuario esta activada o bloqueada.

Tabla 5.1: listado de usuarios

Crear y configurar roles

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios.**
- Haz clic en la pestaña **Roles** para realizar todas las acciones necesarias relativas a la creación y modificación de roles:
  - **Añadir nuevo rol**: haz clic en el botón **Añadir** e introduce el nombre del rol, una descripción opcional, una selección sobre los equipos accesibles y una configuración concreta de los permisos.
  - **Editar un rol**: haz clic en el nombre del rol para mostrar una ventana con todas sus configuraciones editables.
  - **Copiar un rol:** haz clic en el icono para mostrar una ventana con un nuevo rol configurado de la misma forma que el original.
  - **Borrar rol**: haz clic sobre el icono de un rol para borrarlo. Si al borrar un rol éste ya tiene cuentas de usuario asignadas, se cancela el proceso de borrado.

Limitaciones en la creación de usuarios y roles

Para evitar una situación de escalado de permisos, los usuarios con el permiso Gestionar usuarios y roles activo tienen las siguientes limitaciones a la hora de crear roles o asignarlos a otros usuarios ya creados:

- Una cuenta de usuario solo puede crear nuevos roles con los mismos permisos o menos de los que tiene asignada.
- Una cuenta de usuario sólo puede editar los permisos que tenga activos en los roles ya existentes. El resto permanecerán desactivados.
- Una cuenta de usuario no puede asignar un rol a un usuario si ese rol tiene más permisos asignados que la cuenta de usuario.
- Una cuenta de usuario no puede copiar un rol si ese rol tiene más permisos asignados que la cuenta de usuario.

Registro de la actividad de las cuentas de usuario

Cytomic EPDR registra todas las acciones efectuadas por los administradores de red en la consola web de gestión para determinar quién realizó un cambio, en que momento y sobre qué objeto.

Para acceder a la sección de actividad haz clic en el menú superior **Configuración** y después en la pestaña **Actividad.**

Registro de sesiones

La sección de sesiones lista todos los accesos a la consola de administración, los exporta a formato csv y filtra la información.

- **Campos mostrados en el listado de sesiones**

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se produce el acceso.	Fecha
Usuario	Cuenta de usuario que accede.	Cadena de caracteres
Actividad	Acción que ejecuta la cuenta.	• Iniciar sesión • Cerrar sesión
Dirección IP	Dirección IP desde donde se produce el acceso.	Cadena de caracteres

Tabla 5.2: campos del listado sesiones

- **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se produce el acceso.	Fecha
Usuario	Cuenta de usuario que accede.	Cadena de caracteres
Actividad	Acción que ejecuta la cuenta.	• Iniciar sesión • Cerrar sesión
Dirección IP	Dirección IP desde donde se produce el acceso.	Cadena de caracteres

Tabla 5.3: campos del fichero exportado sesiones

- **Herramienta de búsqueda**

Campo	Descripción	Valores
Desde	Establece el limite inferior del intervalo de búsqueda.	Fecha

Tabla 5.4: campos de filtrado para el listado de sesiones

Campo	Descripción	Valores
Hasta	Establece el limite superior del intervalo de búsqueda.	Fecha
Usuarios	Nombre del usuario.	Listado de cuentas de usuario creados en la consola de administración.

Tabla 5.4: campos de filtrado para el listado de sesiones

Registro de acciones de usuario

La sección de **Acciones de usuario** lista todas las acciones ejecutadas por las cuentas de usuario, exporta las acciones a formato csv y filtra la información.

- **Campos mostrados en el listado de acciones**

Campo	Descripción	Valores
Fecha	Fecha y hora en la que ha producido la acción.	Fecha
Acción	Tipo de operación ejecutada.	Consulta la tabla **5.8**
Tipo de elemento	Tipo del objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla **5.8**
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla **5.8**

Tabla 5.5: campos del Registro de acciones

- **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se ha producido la acción.	Fecha
Usuario	Cuenta de usuario que ejecutó la acción.	Cadena de caracteres
Acciones	Tipo de operación realizada.	Consulta la tabla **5.8**
Tipo de elemento	Tipo del objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla **5.8**
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla **5.8**

Tabla 5.6: campos del fichero exportado Registro de acciones

- **Herramienta de búsqueda**

Campo	Descripción	Valores
Desde	Establece el límite inferior del intervalo de búsqueda.	Fecha
Hasta	Establece el límite superior del intervalo de búsqueda.	Fecha
Usuarios	Nombre del usuario encontrado.	Listado de cuentas de usuario creados en la consola de administración.

Tabla 5.7: campos de filtrado para el Registro de acciones

- **Tipos de elementos y acciones**

Tipo de elemento	Acción	Elemento
Acuerdo de licencia	Aceptar	Número de versión del EULA aceptado.
Cuenta	Actualizar consola	De Versión origen a Versión destino.
	Cancelar actualización de consola	De Versión origen a Versión destino.
Amenaza	Permitir	Nombre de la amenaza sobre la que el usuario realizó la acción.
	Dejar de permitir	Nombre de la amenaza sobre la que el usuario realizó la acción.
Búsqueda de información'	Lanzar	Nombre de la búsqueda sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la búsqueda sobre el que el usuario realizó la acción.
	Cancelar	Nombre de la búsqueda sobre el que el usuario realizó la acción.
Configuración - 'Configuración de red'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Ajustes por equipo'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la Configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.

Tabla 5.8: tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
Configuración - 'Bloqueo de programas'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Estaciones y servidores'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Dispositivos Android'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Información personal'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Gestión de parches'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Cifrado'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Entornos VDI'	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.

Tabla 5.8: tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
Configuración - 'Criterios para red de confianza'	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
Envío programado	Crear	Nombre del envío programado sobre el que el usuario realizó la acción.
	Editar	Nombre del envío programado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del envío programado sobre el que el usuario realizó la acción.
Equipo	Eliminar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Editar nombre	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Editar descripción	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Cambiar Grupo	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Configuración de red'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Configuración de red'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Proxy e idioma'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Proxy e idioma'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Ajustes por equipo'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Ajustes por equipo'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Estaciones y servidores'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Estaciones y servidores'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'dispositivos Android'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'dispositivos Android'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Información sensible'	Nombre del dispositivo sobre el que el usuario realizó la acción.

Tabla 5.8: tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
	Heredar configuración de 'Información sensible'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar licencia	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Desasignar licencia	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reiniciar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Bloquear	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Borrar datos	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Foto al ladrón	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Alarma remota	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Localizar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Designar Proxy Cytomic	Nombre del equipo sobre el que el usuario realizó la acción.
	Revocar Proxy Cytomic	Nombre del equipo sobre el que el usuario realizó la acción.
	Designar equipo caché	Nombre del equipo sobre el que el usuario realizó la acción.
	Configurar equipo caché	Nombre del equipo sobre el que el usuario realizó la acción.
	Revocar equipo caché	Nombre del equipo sobre el que el usuario realizó la acción.
	Designar equipo descubridor	Nombre del equipo sobre el que el usuario realizó la acción.
	Configurar descubrimiento	Nombre del equipo sobre el que el usuario realizó la acción.
	Revocar equipo descubridor	Nombre del equipo sobre el que el usuario realizó la acción.
	Descubrir ahora	Nombre del equipo sobre el que el usuario realizó la acción.
	Mover a su ruta de Active Directory	Nombre del equipo sobre el que el usuario realizó la acción.
	Aislar	Nombre del dispositivo sobre el que el usuario realizó la acción.

Tabla 5.8: tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
	Dejar de aislar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Desinstalar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reinstalar agente	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reinstalar protección	Nombre del dispositivo sobre el que el usuario realizó la acción
Equipo no administrado	Ocultar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Visibilizar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Editar descripción	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Instalar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
Filtro	Crear	Nombre del filtro sobre el que el usuario realizó la acción.
	Editar	Nombre del filtro sobre el que el usuario realizó la acción.
	Eliminar	Nombre del filtro sobre el que el usuario realizó la acción.
Grupo	Crear	Nombre del grupo sobre el que el usuario realizó la acción.
	Editar	Nombre del grupo sobre el que el usuario realizó la acción.
	Eliminar	Nombre del grupo sobre el que el usuario realizó la acción.
	Cambiar Grupo-Padre	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Configuración de red'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Configuración de red'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Ajustes por Equipo'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Ajustes por Equipo'	Nombre del grupo sobre el que el usuario realizó la acción.

Tabla 5.8: tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
	Asignar configuración de 'Estaciones y servidores'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Estaciones y servidores'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'dispositivos Android'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'dispositivos Android'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Información sensible'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Información sensible'	Nombre del grupo sobre el que el usuario realizó la acción.
	Sincronizar grupo	Nombre del grupo sobre el que el usuario realizó la acción.
	Mover equipos a su ruta de Active Directory	Nombre del grupo sobre el que el usuario realizó la acción.
Informes avanzados	Acceder	
Listado	Crear	Nombre del listado sobre el que el usuario realizó la acción.
	Editar	Nombre del listado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del listado sobre el que el usuario realizó la acción.
Parche	Excluir para un equipo	Nombre del parche sobre el que el usuario realizó la acción.
	Excluir para todos los equipos	Nombre del parche sobre el que el usuario realizó la acción.
	Dejar de excluir para un equipo	Nombre del parche sobre el que el usuario realizó la acción.
	Dejar de excluir para todos los equipos	Nombre del parche sobre el que el usuario realizó la acción.
	Marcar como "Descargado manualmente"	Nombre del parche sobre el que el usuario realizó la acción.
	Marcar como "Requiere descarga manual"	Nombre del parche sobre el que el usuario realizó la acción.
Preferencia ante reclasificación de amenaza	Editar	
Preferencia para envío emails	Editar	

Tabla 5.8: tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
Preferencia de acceso de equipo de Cytomic S.L.	Editar	
Preferencia de acceso del distribuidor	Editar	
Preferencia para envío emails distribuidor	Editar	
Preferencia de verificación en dos pasos	Editar	
Rol	Crear	Nombre del rol sobre el que el usuario realizó la acción.
	Editar	Nombre del rol sobre el que el usuario realizó la acción.
	Eliminar	Nombre del rol sobre el que el usuario realizó la acción.
Tarea - Análisis de seguridad	Crear	Nombre de la tarea sobre el que el usuario realizó la acción.
	Editar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Cancelar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Publicar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Crear y publicar	Nombre de la tarea sobre el que el usuario realizó la acción.
Tarea - Instalación de parches	Crear	Nombre de la tarea sobre el que el usuario realizó la acción.
	Editar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Cancelar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Publicar	Nombre de la tarea sobre el que el usuario realizó la acción.

Tabla 5.8: tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
	Crear y publicar	Nombre de la tarea sobre el que el usuario realizó la acción.
Usuario	Crear	Nombre del usuario sobre el que el usuario realizó la acción.
	Editar	Nombre del usuario sobre el que el usuario realizó la acción.
	Eliminar	Nombre del usuario sobre el que el usuario realizó la acción.
	Bloquear	Nombre del usuario sobre el que el usuario realizó la acción.
	Desbloquear	Nombre del usuario sobre el que el usuario realizó la acción.
Tarea - Desinstalación de parches	Crear	Nombre de la tarea sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Cancelar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Publicar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Crear y publicar	Nombre de la tarea sobre el que el usuario realizó la acción.

Tabla 5.8: tipos de elemento y acciones

Eventos del sistema

Lista los eventos que se producen en Cytomic EPDR y que no tienen una cuenta de usuario como origen, sino que son desencadenados por el propio sistema como respuesta las situaciones mostradas en la tabla **5.12**.

- **Campos mostrados en el listado de eventos del sistema**

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se ha producido el acceso.	Fecha
Evento	Acción que ejecutó Cytomic EPDR.	Consulta la tabla **5.12**
Tipo	Tipo del objeto sobre el cual se ejecutó la acción.	Consulta la tabla **5.12**
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla **5.12**

Tabla 5.9: campos del listado Eventos del sistema

- **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se ha producido el acceso.	Fecha
Evento	Acción que ejecutó Cytomic EPDR.	Consulta la tabla **5.12**
Tipo	Tipo del objeto sobre el cual se ejecutó la acción.	Consulta la tabla **5.12**
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla **5.12**

Tabla 5.10: campos del listado Eventos del sistema

- **Herramienta de búsqueda**

Campo	Descripción	Valores
Desde	Establece el límite inferior del intervalo de búsqueda.	Fecha
Hasta	Establece el límite superior del intervalo de búsqueda.	Fecha

Tabla 5.11: campos del listado Eventos del sistema

- **Tipos de elementos y acciones**

Tipo de elemento	Acción	Elemento
Equipo no-persistente	Eliminar automáticamente	Nombre del equipo sobre el que se realizó la acción.
Equipo	Registrar en servidor por primera vez.	Nombre del equipo sobre el que se realizó la acción.
Equipo	Registrar en servidor tras eliminación de equipo.	Nombre del equipo sobre el que se realizó la acción.
Equipo	Registrar en servidor tras reinstalación de agente.	Nombre del equipo sobre el que se realizó la acción.
Equipo	Desinstalar el agente	Nombre del equipo sobre el que se realizó la acción.

Tabla 5.12: tipos de elementos y acciones

Parte 3

Despliegue y puesta en marcha

Capítulo 6: Instalación del software cliente

Capítulo 7: Licencias

Capítulo 8: Actualización del software cliente

Capítulo 6

Instalación del software cliente

La instalación es el proceso que distribuye Cytomic EPDR en los equipos de la red de la organización. El paquete de instalación contiene todo el software necesario para activar el servicio de protección avanzado, la monitorización y la visibilidad del estado de la seguridad de los equipos, y no es necesaria la instalación de ningún otro programa.

Cytomic EPDR ofrece varias herramientas que facilitan la instalación de la protección, que se mostrarán a lo largo de este capítulo.

CONTENIDO DEL CAPÍTULO

Visión general del despliegue de la protección

El proceso de instalación comprende varios pasos, dependiendo del estado de la red en el momento del despliegue y del número de equipos a proteger. Para desarrollar un despliegue con garantías de éxito es necesario elaborar una planificación que comprenda los puntos enumerados a continuación:

Localiza los equipos desprotegidos en la red

Localiza los equipos que no tienen instalada protección en la red del cliente o que tienen un producto de terceros que sea necesario sustituir o complementar con Cytomic EPDR y comprueba que el número de licencias contratadas es suficiente.

Cytomic EPDR permite la instalación del software sin tener contratadas licencias suficientes. Estos equipos serán visibles en la consola de administración y mostrarán el software instalado, hardware y otras características, pero no estarán protegidos frente al malware de nueva generación.

Requisitos mínimos de la plataforma destino

Los requisitos mínimos de cada plataforma se describen en el apartado "**Requisitos de red y sistema operativo**".

Procedimiento de instalación

Dependiendo del número total de equipos Windows a proteger, los puestos y servidores con un agente Cytomic ya instalado y la arquitectura de red de la empresa, será preferible utilizar un procedimiento u otro de los cuatro disponibles:

- Herramienta de despliegue centralizado.
- Instalación manual utilizando la herramienta **Enviar URL por mail**.
- Programa de instalación compartido en una carpeta accesible por los usuarios de la red.
- Instalación remota desde la consola de administración.

Desinstalación de otros productos de seguridad y reinicio de equipos

Todos los servicios de protección de Cytomic EPDR comenzarán a funcionar sin necesidad de reiniciar los equipos en el caso de equipos sin antivirus previamente instalado.

Algunas versiones anteriores de Citrix pueden requerir un reinicio del equipo o producirse un pequeño micro corte en las conexiones.

Si deseas instalar Cytomic EPDR en un equipo en el que ya se encuentra instalada otra solución de seguridad ajena a Cytomic, puedes elegir entre instalarlo sin retirar la otra protección, de tal manera que ambas soluciones de seguridad convivan en el mismo equipo o, por el contrario, desinstalar la otra solución de seguridad y funcionar exclusivamente con Cytomic EPDR. Consulta el recurso web

https://www.pandasecurity.com/es/support/card?id=50021 para obtener un listado de los productos de seguridad de terceros que Cytomic EPDR desinstala de forma automática.

> *Para completar la desinstalación del antivirus de terceros es posible que se requiera un reinicio de la máquina.*

En función del tipo de versión de Cytomic EPDR que quieras instalar, el comportamiento por defecto varía tal y como se muestra a continuación.

- **Versiones Trials**

No se desinstalarán por defecto las soluciones de seguridad de terceros para evaluar Cytomic EPDR.

- **Versiones comerciales**

Por defecto Cytomic EPDR no se instala en un equipo que ya dispone de otra solución ajena a Cytomic. Si está disponible un desinstalador del producto, el antivirus de terceros se eliminará del equipo y se lanzará la instalación de Cytomic EPDR. En caso contrario, la instalación se detiene.

El comportamiento por defecto es configurable tanto en versiones trial como en versiones comerciales asignando una configuración de **Estaciones y servidores** donde esté habilitada la opción Desinstalar otros productos de seguridad.

> *Consulta el capítulo "**Configuración de estaciones y servidores**" en la página **225** si quieres diseñar una configuración de seguridad. Consulta el apartado "**Asignación manual y automática de configuraciones**" en la página **203** para asignar configuraciones a los equipos de la red.*

Instalación en horario no laboral

Adicionalmente a la necesidad de reinicio del equipo de usuario descrita en el punto anterior, la instalación de Cytomic EPDR provoca un micro corte de menos de 4 segundos de duración sobre las conexiones establecidas por los programas en funcionamiento. Las aplicaciones que no implementen mecanismos para detectar cortes de conexión requerirán un reinicio. Si no es posible este reinicio y además la aplicación no se comporta adecuadamente tras el micro corte, se recomienda la instalación fuera del horario laboral.

Configuración por defecto de los equipos

Con el objeto de proteger a los equipos de la red desde el primer momento, Cytomic EPDR obliga a seleccionar el grupo de destino donde el equipo se integrará dentro del árbol de grupos, y la configuración de red de forma independiente. Esta selección se realiza al generar el instalador, consulta más adelante en la sección "**Instalación local del software cliente**".

Una vez instalado el software en el equipo, Cytomic EPDR aplicará las configuraciones establecidas en el grupo al que pertenezca el equipo y, posteriormente, si la configuración de red del grupo seleccionado difiere de la indicada al generar el instalador, se generará una asignación manual. De esta forma será la configuración de red seleccionada en la instalación la que prevalece por encima de la asignada en el árbol de grupos.

Requisitos de instalación

*Para una descripción completa de los requisitos por plataforma consulta el capítulo "***Requisitos de hardware, software y red***" en la página* **515**.

Requisitos por plataforma

- **Windows**
  - **Estaciones de trabajo**: Windows XP SP3 y superiores, Windows Vista, Windows 7, Windows 8 y superiores, y Windows 10.
  - **Servidores**: Windows 2003 SP2 y superiores, Windows 2008, Windows Small Business Server 2011 y superiores, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server Core 2008 y superiores.
  - **Servidores Exchange**: 2003 al 2019.**Espacio para la instalación**: 650 Mbytes.
  - **Certificados raíz actualizados** para utilizar el módulo Cytomic Patch y las comunicaciones en tiempo real con la consola de administración.
- **macOS**
  - **Sistemas operativos**: macOS 10.10 Yosemite y superiores.
  - **Espacio para la instalación**: 400 Mbytes.
  - **Puertos**: se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento del filtrado web y la detección web de malware.
- **Linux**
  - **Sistemas operativos 64 bits**: Ubuntu 14.04 LTS y superiores, Fedora 23 y superiores, Debian 8 y superiores, RedHat 7 y superiores, CentOS 7 y superiores, LinuxMint 18 y superiores. No requiere sistema de ventanas instalado. Utiliza la herramienta `/usr/local/protection-agent/bin/pa_cmd` desde la linea de comandos.
  - **Kernel soportado**: hasta la versión 5.4.1 64 bits. Consulta la web de soporte en **https://www.pandasecurity.com/spain/support/card?id=700009** para comprobar la última versión del kernel de Linux soportada por Cytomic EPDR. Versiones superiores del kernel no funcionarán.
  - **Espacio para la instalación**: 100 Mbytes.

- **Puertos**: se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento del filtrado web y la detección web de malware. En equipos sin entorno gráfico la detección web y el filtrado web están deshabilitados.

Para instalar Cytomic EPDR en plataformas Linux es necesario que el equipo tenga conexión a Internet durante todo el proceso. El script de instalación conectará con los repositorios apropiados dependiendo del sistema (rpm o deb) y se descargarán todos los paquetes necesarios para finalizar la instalación con éxito.

- **Android**
  - **Sistemas operativos**: Android 4.0 y superiores.
  - **Espacio para la instalación**: 10 Mbytes (dependiendo del modelo de dispositivo se requerirá espacio adicional).

Requisitos de red

En su funcionamiento normal Cytomic EPDR accede a varios recursos alojados en Internet. De forma general se requiere acceso a los puertos 80 y 443. Para un listado completo de las URLs que se acceden desde los equipos con el software Cytomic EPDR instalado consulta el apartado "**Acceso a URLs del servicio**" en la página **521**.

Instalación local del software cliente

Para descargar e instalar el software cliente en los equipos de la red sigue las tareas mostradas a continuación:

- Descarga del paquete de instalación desde la consola Web.
- Generar de URL de descarga.
- Instalar manualmente el software cliente.

Descarga del paquete de instalación desde la consola Web

*Para más información sobre asignar configuraciones consulta el apartado "***Asignación manual y automática de configuraciones**" *en la página* **203**.

Consiste en descargar el paquete de instalación directamente desde la consola de administración. Para ello sigue los pasos mostrados a continuación y consulta la figura **6.2**:

- En la zona **Equipos** haz clic en el botón **Añadir equipo** y elige la plataforma a proteger: Windows,

Linux, Android o macOS.

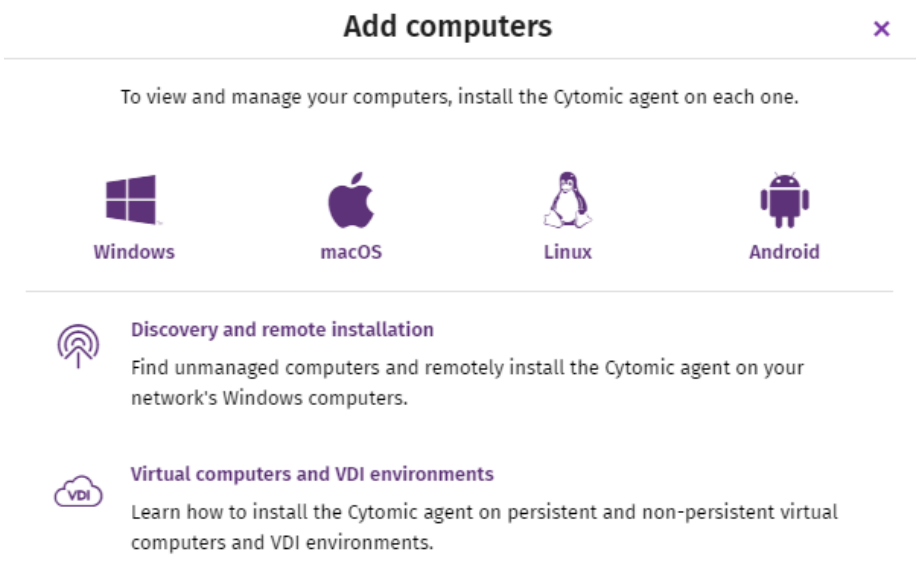


Figura 6.1: ventana de selección de plataforma compatible con Cytomic EPDR

- Selecciona el grupo donde se integra el equipo en el árbol de carpetas:
  - Para integrar el equipo en un grupo nativo haz clic en **Añadir los equipos al siguiente grupo (1)** y selecciona el destino en el árbol de carpetas mostrado.
  - Para integrar el equipo en un grupo Directorio Activo haz clic en **Añadir los equipos en su ruta de Directorio Activo (2)**. Para más información sobre los diferentes tipos de grupos consulta el apartado "**Tipos de grupos**" en la página **158**.
  - Para integrar el equipo en un grupo u otro en función de su dirección IP haz clic en la opción **Seleccionar el grupo en función de la IP del equipo** y elige el grupo a partir del cual se buscará un destino que coincida con la IP del equipo. Consulta el apartado "**Integración de equipos según su dirección IP**".

Selecciona la **Configuración de red (3)** que se aplicará al equipo a instalar. Para más información sobre crear nuevas configuraciones de red consulta el apartado "**Crear y gestionar configuraciones**" en la página **202**.

- Si quieres integrar el puesto en un grupo nativo, se seleccionará de forma automática la configuración asignada a la carpeta donde residirá.
- Si has elegido integrarlo en un grupo Directorio Activo selecciona de forma manual la configuración de red de entre las mostradas en el desplegable. Si la elección automática no se

ajusta a tus necesidades haz clic en el desplegable y elige otra de entre las disponibles.

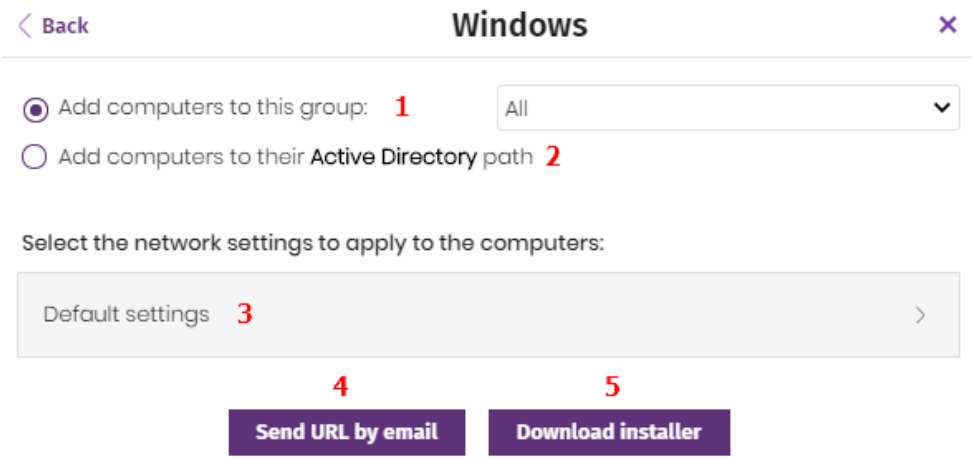


Figura 6.2: configuración del paquete de descarga

- Haz clic en el botón **Descargar instalador (5)** para iniciar la descarga del paquete apropiado. El instalador contiene un asistente que guiará al usuario en los pasos necesarios para completar la instalación del software.

Integración de equipos según su dirección IP

Al crear un grupo de equipos, Cytomic EPDR permite la asignación de rangos de direcciones IPs e IPs individuales que determinan los equipos que formarán parte del grupo en el momento de su instalación. Consulta el apartado "**Crear y organizar grupos**" en la página **160** para obtener más información sobre la creación de grupos.

El objetivo de esta funcionalidad consiste en ahorrar tiempo al administrador organizando de forma automática los equipos recién integrados en el producto. Cuando un nuevo equipo se integra en Cytomic EPDR se siguen los pasos mostrados a continuación:

- Si la opción elegida en la integración es **Seleccionar el grupo en función de la IP del equipo** Cytomic EPDR ejecutará una búsqueda en profundidad para recuperar las IPs asociadas al grupo indicado en el campo **Seleccionar a partir de qué grupo se añadirán los equipos** y las de todos sus hijos.
- Si se encuentra una única IP coincidente el equipo se moverá al grupo pertinente.
- Si hay varios grupos de IPs que coinciden con la IP del equipo se tomará siempre el grupo de mayor profundidad. Si existen varios grupos que coinciden con la IP con un mismo nivel de profundidad se elegirá el último de ellos.
- Si no existe ninguna coincidencia, el equipo se moverá al grupo indicado en el campo **Seleccionar a partir de qué grupo se añadirán los equipos**, y si este grupo no existe en el momento de la integración el equipo se moverá al grupo Todos.

Una vez movido el equipo al grupo correspondiente, el equipo no se volverá a mover automáticamente al cambiar su IP, ni tampoco se reorganizaran los equipos ya integrados al cambiar las IPs asignadas a los grupos de IPs.

Generar la URL de descarga

Este método permite la creación de una URL de descarga para enviar por correo a los usuarios que quieran iniciar una instalación manual en su equipo.

Para generar la URL de descargar sigue los pasos del apartado "**Descarga del paquete de instalación desde la consola Web**" y haz clic en el botón **Enviar por email (4)**.

Los usuarios recibirán un correo electrónico con el enlace de descarga correspondiente a su sistema operativo. Al hacer clic en el enlace, se iniciará la descarga del instalador.

Instalar manualmente el software cliente

Para la instalación del software Cytomic EPDR en el equipo de usuario se requieren permisos de administrador.

Instalación en plataformas Windows y macOS

Para ejecutar el instalador descargado haz doble clic sobre su icono y sigue el asistente. Durante el proceso de instalación se mostrará una ventana con el progreso de la tarea. En los equipos Windows se le indicará al administrador de la red si el número de licencias libres no es suficiente como para asignar una al equipo en proceso de instalación. Independientemente de este hecho el equipo se integrará en el servicio aunque el equipo no estará protegido si no hay licencias disponibles.

Una vez completado, el producto comprobará que tiene la última versión del fichero de firmas y del motor de protección. Si no es así, iniciará una actualización automática.

Instalación en plataformas Linux

Para ejecutar el script descargado abre una sesión de terminal en la carpeta donde reside el paquete y ejecuta el siguiente comando:

```
sudo sh "nombre_del_paquete"
```

El script de instalación se conectará a los repositorios rpm o deb dependiendo del sistema operativo y descargará todos los paquetes necesarios para su instalación.

Instalación en plataformas Android

- Al hacer clic en el botón **Añadir equipo** del menú superior **Equipos** y seleccionar el icono de

Android, se mostrará una ventana con la información mostrada a continuación:**Añadir los equipos**

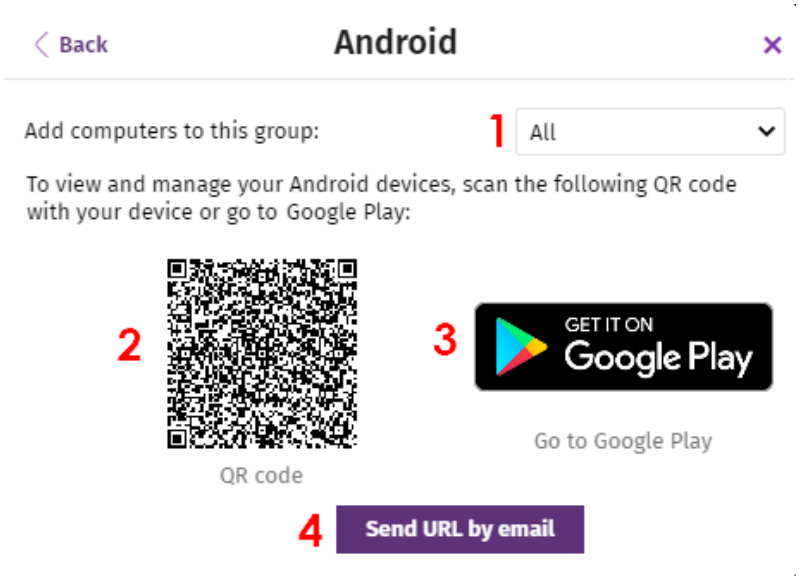


Figura 6.3: instalación en dispositivos Android

al siguiente grupo (1): especifica el grupo dentro del árbol de carpetas en el que se integrará el dispositivo una vez se haya instalado el software Cytomic EPDR.

- **Código QR (2)**: código QR que contiene el link para descargar el software de la Google Play.
- **Acceso a la Google Play (3)**: link directo de descarga del software Cytomic EPDR de la Google Play.
- **Enviar URL por mail (4)**: mensaje de correo con el link de descarga listo para enviar al usuario del dispositivo a proteger con Cytomic EPDR.

Para instalar el software en el dispositivo del usuario sigue los pasos mostrados a continuación:

- Selecciona el grupo dentro del árbol de carpetas donde se integrará el dispositivo. El código QR se actualizará de forma automática con la nueva selección.
- Sigue uno de los tres procedimientos descritos a continuación para descargar la aplicación Android:
  - **Mediante código QR**: haz clic en el código QR para agrandarlo, enfoca la cámara del dispositivo a la pantalla y, mediante una aplicación de lectura de códigos QR, escanéalo. En la pantalla del terminal aparecerá una URL de la Google Play que mostrará la ficha de la aplicación lista para su descarga. Pulsando la URL se mostrará la ficha de la aplicación lista para su descarga.

> *QR Barcode Scanner y Barcode Scanner son dos aplicaciones para la lectura de códigos QR gratuitas y disponibles en la Google Play.*

  - **Mediante correo electrónico**: haz clic en el link **Enviar URL por email** para enviar al usuario un mail con el link que le llevará a la ficha de la aplicación en Google Play, lista para su descarga.
  - **Mediante la consola de administración**: si has accedido a la consola de administración desde el propio dispositivo, haz clic en el link **Acceso a la Google Play**. Se mostrará la ficha de la aplicación

lista para su descarga.

- Una vez instalada la aplicación se le pedirá al usuario que acepte conceder ciertos permisos de acceso a recursos del dispositivo movil. Dependiendo de la versión de Android (6.0 en adelante), estos permisos se presentarán de forma progresiva según se necesiten, o por el contrario se mostrará una ventana la primera vez que se ejecute la aplicación, solicitando todos los permisos necesarios de una sola vez.

Una vez terminado el procedimiento, el dispositivo aparecerá en el grupo seleccionado dentro del árbol de carpetas.

Instalación remota del software cliente

Los productos basados en Cytomic Platform incorporan las herramientas necesarias para localizar los puestos de usuario y servidores sin proteger, e iniciar una instalación remota desatendida desde la consola de administración.

La instalación remota es compatible con plataformas Windows.

Requisitos de red y sistema operativo

Para poder instalar Cytomic EPDR de forma remota, es necesario que los equipos cumplan con los requisitos indicados a continuación:

- Abrir los puertos UDP 21226 y 137 para el proceso `System`.
- Abrir el puerto TCP 445 para el proceso `System`.
- Hablitar el protocolo NetBIOS sobre TCP.
- Permitir las resoluciones DNS.
- Acceso al recurso de administración `Admin$`. En las ediciones "Home" de Windows es necesario habilitar este recurso de forma explícita.
- Credenciales de administrador de dominio o de la cuenta de administrador local generada por defecto en la instalación del sistema operativo.
- Credenciales de administrador de dominio o de administrador local.
- Activar la Administración remota.

Para cumplir con estos requisitos de forma rápida sin necesidad de añadir reglas de forma manual en el firewall de Windows, selecciona Activar la detección de redes red y Activar el uso compartido de archivos e impresoras en Centro de redes y recursos compartidos, Configuración de uso compartido avanzado.

Adicionalmente, para que un equipo de la red con Cytomic EPDR instalado pueda descubrir a otros equipos es necesario que:

- No estén ocultos por el administrador.
- No estén siendo ya administrados por Cytomic EPDR sobre Cytomic Platform.
- Se encuentren en el mismo segmento de subred al que pertenece el equipo descubridor.

Equipos ocultos

Para evitar generar listados de equipos no administrados descubiertos muy extensos que incluyan dispositivos sin interés para la instalación de Cytomic EPDR, es posible ocultarlos de forma selectiva siguiendo los pasos mostrados a continuación:

- En el listado **Equipos no administrados descubiertos** selecciona **Descubierto** en el combo.
- Haz clic en las casillas correspondientes a los equipos a ocultar.
- Para ocultar varios equipos haz clic en el menú de contexto general y en **Ocultar y no volver a descubrir**.
- Para ocultar un único equipo haz clic en el menú de contexto del equipo y en **Ocultar y no volver a descubrir**.

Descubrir equipos

El descubrimiento de equipos se efectúa a través de un equipo con el rol de Descubridor asignado. Todos los equipos que cumplan los requisitos se mostrarán en el listado **Equipos no administrados descubiertos**, independientemente de si el sistema operativo o el tipo de dispositivo admite la instalación de Cytomic EPDR.

El primer equipo Windows que se integre en Cytomic EPDR tendrá asignado el rol descubridor de forma automática.

Asignar el rol de descubridor a un equipo de la red

- Comprueba que el equipo descubridor tiene instalado Cytomic EPDR.
- Haz clic en el menú superior **Configuración**, panel lateral **Servicios de red** y pestaña **Descubrimiento**.
- Haz clic en el botón **Añadir equipo descubridor** y selecciona en el listado los equipos que lanzarán procesos de descubrimiento en la red.

Una vez asignado el rol de descubridor a un equipo, éste se mostrará en la lista de equipos descubridores (menú superior **Configuración**, panel lateral **Configuración de red**, pestaña **Descubrimiento**). Para cada equipo descubridor se muestra la siguiente información:

Campo	Descripción
Nombre del equipo	Nombre del equipo descubridor.
Dirección IP	Dirección IP del equipo descubridor.
Configuración de la tarea de descubrimiento	Configuración de la tarea automática que se lanza para descubrir equipos en la red, si está configurada.
Última comprobación	Fecha y hora de la última vez que se lanzó una tarea de descubrimiento.
"El equipo está apagado o sin conexión"	Cytomic EPDR no es capaz de conectar con el equipo descubridor.
Configurar	Establece el alcance y tipo de descubrimiento (automático o manual). Si es automático, la tarea de descubrimiento se ejecutará una vez al día.

Tabla 6.1: campos del detalle de un equipo con el rol descubridor asignado

Establecer el alcance del descubrimiento

Todas las configuraciones de alcance de descubrimiento están limitadas al segmento de red donde está conectado el equipo descubridor. Para buscar dispositivos en todos los segmentos de red asigna el rol de descubridor a por lo menos un equipo en cada segmento de red.

Para limitar el alcance del descubrimiento de equipos en la red sigue los pasos mostrados a continuación:

- En el menú superior **Configuración**, panel lateral **Configuración de red**, pestaña **Descubrimiento**, haz clic en el botón **Configurar** del equipo descubridor cuyo alcance de descubrimiento quieres modificar.
- En la sección **Limitar el alcance del descubrimiento** selecciona un criterio:
  - **Buscar en toda la red**: el equipo descubridor utiliza la máscara configurada en la interface para efectuar un barrido completo de la subred a la que pertenece.
  - **Buscar solo en los siguientes rangos de direcciones IPs**: define varios rangos de búsqueda en la red separados por comas. Separa el inicio y el final del rango mediante el carácter guion '-'.
  - **Buscar sólo equipos de los siguientes dominios**: la búsqueda queda limitada a los dominios Windows indicados separados por comas.

Programar las tareas de descubrimiento

Las tareas de descubrimiento de equipos se pueden lanzar de forma programada cada cierto tiempo por los equipos descubridores.

- En el menú superior **Configuración**, panel lateral **Configuración de red**, pestaña **Descubrimiento**, haz clic en el enlace **Configurar** del equipo descubridor a configurar.
- En el desplegable **Ejecutar** automáticamente elige **Todos los días**.
- Elige la hora a la que se ejecutará la tarea.
- Marca en la casilla para tomar la hora local del equipo o la hora del servidor Cytomic EPDR.
- Haz clic en **Aceptar**. El equipo configurado mostrará en su descripción la programación configurada.

Lanzar las tareas de descubrimiento manuales

- En el menú superior **Configuración**, panel lateral **Configuración** de red, pestaña **Descubrimiento**, haz clic en el enlace **Configurar** del equipo descubridor a configurar.
- En el desplegable **Ejecutar** automáticamente elige **No**.
- Haz clic en **Aceptar**. El equipo mostrará un enlace **Comprobar ahora** que el administrador podrá utilizar para lanzar una tarea de descubrimiento bajo demanda.

Visualizar equipos descubiertos

Existen dos formas de acceder al listado de **Equipos no administrados descubiertos**:

- **Widget Estado de protección**: desde el menú superior **Estado** accede al panel de control de Cytomic EPDR donde se encuentra el widget **Estado de la protección**. En su parte inferior se mostrará el enlace **Se han descubierto x equipos que no están siendo administrados desde Cytomic EPDR**.
- **Panel Mis listados**: accede a la sección **Mis listados** desde el panel lateral y haz clic en el enlace **Agregar**. Selecciona en el desplegable el listado **Equipos no administrados descubiertos.**
- **Listado Equipos no administrados descubiertos**

Este listado contiene los equipos descubiertos en la red del cliente que no tienen instalado Cytomic EPDR o que, habiéndose instalado correctamente su funcionamiento no es el correcto.

Campo	Descripción	Valores
Equipo	Nombre del equipo descubierto.	Cadena de caracteres

Tabla 6.2: campos del listado de equipos no administrados descubiertos

Campo	Descripción	Valores
Estado	Estado en el que se encuentra el equipo con respecto al proceso de instalación.	• — **No administrado**: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado. • **Instalando**: el proceso de instalación se ha iniciado. • **Error instalando:** mensaje con el tipo de error producido en la instalación. Consulta el apartado "**Sección alertas de equipo (2)**" en la página **178** para una relación de mensajes de error y la explicación de cada uno de ellos. Si el error es de origen desconocido se mostrará su código de error asociado.
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Fabricante NIC	Marca de la tarjeta de red del equipo descubridor.	Cadena de caracteres
Último descubridor	Nombre del dispositivo que descubrió más recientemente el puesto de trabajo o servidor.	Cadena de caracteres
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha

Tabla 6.2: campos del listado de equipos no administrados descubiertos

Cuando el campo **Estado** muestra **Error instalando** y es un error de origen conocido, se añade una cadena de texto que lo describe. Consulta el apartado "**Sección alertas de equipo (2)**" en la página **178** para obtener un listado de los errores de instalación reportados por Cytomic EPDR.

- **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Nombre	Nombre del equipo descubierto.	Cadena de caracteres
IP	Dirección IP principal del equipo.	Cadena de caracteres
Dirección MAC	Dirección física del equipo.	Cadena de caracteres

Tabla 6.3: campos del fichero exportado Listado de Equipos no administrados descubiertos

Campo	Descripción	Valores
Fabricante NIC	Marca de la tarjeta de red del equipo descubridor.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Primera vez visto	Fecha en la que el equipo fue descubierto por primera vez.	Cadena de caracteres
Primera vez visto por	Nombre del equipo descubridor que vio por primera vez al puesto de usuario.	Cadena de caracteres
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha
Última vez visto por	Nombre del equipo descubridor que vio por última vez al puesto.	Cadena de caracteres
Descripción	Descripción del equipo descubierto.	Cadena de caracteres
Estado	Estado en el que se encuentra el equipo con respecto al proceso de instalación.	• **No administrado**: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado. • **Instalando**: el proceso de instalación se ha iniciado. • **Error instalando:** mensaje con el tipo de error producido en la instalación. Consulta el apartado "**Sección alertas de equipo (2)**" en la página **178** para una relación de mensajes de error y la explicación de cada uno de ellos.
Error	Descripción del error encontrado.	Consulta el apartado "**Sección alertas de equipo (2)**" en la página **178**.
Fecha error instalación	Fecha y hora en la que se produjo el error.	Fecha

Tabla 6.3: campos del fichero exportado Listado de Equipos no administrados descubiertos

- **Herramienta de búsqueda**

Campo	Descripción	Valores
Buscar	Búsqueda por el nombre del equipo, IP, fabricante de la tarjeta de red o equipo descubridor.	Cadena de caracteres

Tabla 6.4: campos de filtrado para el listado Listado de Equipos no administrados descubiertos

Campo	Descripción	Valores
Estado	Estado de la instalación de Cytomic EPDR.	• **No administrado**: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado. • **Instalando**: el proceso de instalación se ha iniciado. • **Error instalando**: mensaje con el tipo de error producido en la instalación.
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	• Últimas 24 horas • Últimos 7 días • Último mes

Tabla 6.4: campos de filtrado para el listado Listado de Equipos no administrados descubiertos

- **Ventana detalle del equipo**

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta el apartado "**Información de equipo**" en la página **177** para obtener más información.

Equipos borrados

Cytomic EPDR no elimina de la lista **Equipos no administrados descubiertos** los dispositivos que una vez fueron detectados, pero ya no están accesibles por haberse retirado (avería, robo o cualquier otra razón).

Para eliminar de forma manual estos equipos nunca más accesibles sigue los pasos mostrados a continuación:

- En el listado de **Equipos no administrados descubiertos** selecciona **Descubiertos** u **Ocultos** en el combo dependiendo del estado del dispositivo.
- Haz clic en las casillas correspondientes a los equipos a borrar.
  - Para borrar varios equipos haz clic en el menú de contexto general y en **Borrar**.
  - Para borrar un único equipo haz clic en el menú de contexto del equipo y en **Borrar**.

Un equipo que se elimina de la consola sin desinstalar el software Cytomic EPDR, y sin retirarse físicamente de la red volverá a aparecer en la siguiente tarea de descubrimiento. Borra únicamente los equipos que nunca más vayan a ser accesibles.

Detalle de los equipos descubiertos

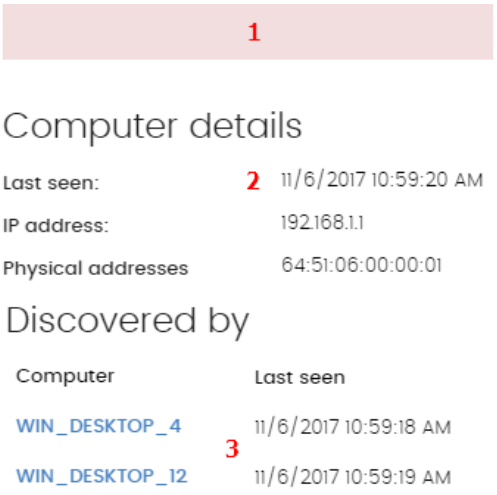


Figura 6.4: distribución de la información en un equipo descubierto

En el listado de **Equipos no administrados descubiertos**, haz clic en un equipo descubierto para ver su ventana de detalle dividida en 3 secciones:

- **Alertas de equipo (1)**: muestra potenciales problemas asociados a la instalación del equipo.
- **Detalles del equipo (2)**: muestra un resumen ampliado del hardware, software y seguridad configurada en el equipo.
- **Descubierto por (3)**: muestra los equipos descubridores que vieron el equipo no administrado.

Alertas de equipo

Estado	Tipo	Resolución
Error instalando el agente de Cytomic	Indica el motivo del error en la instalación del agente.	
	Credenciales incorrectas	Lanza de nuevo la instalación con unas credenciales que tengan suficientes privilegios para realizar la instalación.
	No es posible conectar con el equipo	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible descargar el instalador del agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible copiar el instalador del agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible instalar el agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible registrar el agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
Error instalando la protección de Cytomic EPDR	Indica el motivo del error en la instalación de la protección.	

Tabla 6.5: campos del listado Equipos protegidos

Estado	Tipo	Resolución
	No hay suficiente espacio libre en el disco para realizar la instalación	Consulta el apartado "**Requisitos hardware**" en la página **516** para ver los requisitos de espacio necesarios para instalar Cytomic EPDR.
	El servicio de Windows Installer no está operativo	Comprueba que el servicio Windows Installer se esté ejecutando. Para y arranca el servicio.
	El usuario canceló la desinstalación de la protección de otro fabricante	Acepta la desinstalación del antivirus de terceros.
	Hay otra instalación en curso	Espera a que finalice la instalación previa.
	Error desinstalando automáticamente protecciones de otros fabricantes	Consulta el capítulo "**Desinstaladores soportados**" en la página **379** para ver una lista de fabricantes con desinstalador soportado por Cytomic.
	Desinstalador no disponible para protección de otro fabricante	Contacta con el departamento de soporte para pedir un desinstalador.
Instalando agente de Cytomic	Una vez terminado el proceso de instalación el equipo dejará de aparecer en el listado de Equipos no administrados descubiertos.	
Equipo no administrado	El equipo no tiene el agente Cytomic instalado. Comprueba que se trata de un equipo compatible con Cytomic EPDR y que cumple con los requisitos indicados en el capítulo "**Requisitos de hardware, software y red**" en la página **515**.	

Tabla 6.5: campos del listado Equipos protegidos

Detalles del equipo

Campo	Descripción
Nombre del equipo	Nombre del equipo descubierto.
Descripción	Permite asignar una descripción al equipo, aunque no esté administrado todavía.
Primera vez visto	Fecha y hora de la primera vez que el equipo fue descubierto.
Última vez visto	Fecha y hora de la ultima vez que el equipo fue descubierto.
Dirección IP	Dirección IP de la tarjeta de red del equipo descubierto.
Direcciones físicas (MAC)	Dirección física de la tarjeta de red del equipo descubierto.
Dominio	Dominio Windows al que pertenece el equipo.
Fabricante NIC	Fabricante de la tarjeta de red instalada en el equipo.

Tabla 6.6: filtros del listado de licencias

Descubierto por

Campo	Descripción
Equipo	Nombre del equipo descubridor que vio al equipo no administrado.
Última vez visto	Fecha y hora de la primera vez que el equipo fue visto por el equipo descubridor.

Tabla 6.7: filtros del listado de licencias

Instalación remota de equipos descubiertos

Para instalar de forma remota el software Cytomic EPDR en uno o varios equipos distribuidos sigue los pasos mostrados a continuación:

Desde el listado de Equipos no administrados descubiertos

- Accede al listado de **Equipos no administrados descubiertos**.
  - Desde el panel lateral **Mis listados, Añadir**, selecciona el listado **Equipos no administrados descubiertos**.
  - Desde el menú superior **Estado** en el widget **Estado de la protección**, haz clic en el link **Se han descubierto x equipos que no están siendo administrados desde Cytomic EPDR**.
  - Desde el menú superior **Equipos** haz clic en **Añadir equipos** y selecciona **Descubrimiento e instalación remota**. Se mostrará una ventana con un asistente. Haz clic en el link **Ver equipos no administrados descubiertos**.
- En el listado de **Equipos no administrados descubiertos** selecciona **Descubiertos u Ocultos** en el combo, dependiendo del estado del dispositivo.
- Haz clic en las casillas correspondientes a los equipos a instalar.
  - Para instalar varios equipos haz clic en el menú de contexto general y en **Instalar agente de Cytomic**.
  - Para instalar un único equipo haz clic en el menú de contexto del equipo y en **Instalar agente de Cytomic**.
- Configura la instalación según los pasos descritos en el apartado "**Descarga del paquete de instalación desde la consola Web**" en la página **104**.
- Introduce una o varias credenciales de instalación. Es necesario utilizar una cuenta de administración local del equipo o del dominio al que pertenece para completar la instalación con éxito.

Desde la pantalla de detalles de equipo

Al hacer clic en un equipo descubierto se mostrará su detalle y en la parte superior el botón **Instalar agente de Cytomic**. Sigue los pasos descritos en el apartado "**Descarga del paquete de instalación desde la consola Web**" en la página **104**.

Instalar con herramientas centralizadas

En redes de tamaño medio o grande es conveniente instalar el software cliente para equipos Windows de forma centralizada con la ayuda de herramientas de terceros.

Línea de comandos del paquete de instalación

Para automatizar la instalación e integración del agente Cytomic en la consola de administración se implementan los parámetros siguientes de línea de comandos:

- **GROUPPATH="grupo1\grupo2"**: ruta dentro del árbol de grupos y sin indicar el nodo raíz Todos donde se integrará el equipo. Si el grupo no existe el equipo se integra en el nodo raíz Todos.
- **PRX_SERVER**: dirección IP o nombre del servidor proxy corporativo.
- **PRX_PORT**: puerto del servidor proxy corporativo.
- **PRX_USER**: usuario del servidor proxy corporativo.
- **PRX_PASS**: contraseña del servidor proxy corporativo.

A continuación, se muestra un ejemplo de instalación con parámetros

```
Msiexec /i "PandaAetherAgent.msi" GROUPPATH="Madrid\Contabilidad"
PRX_SERVER="ProxyCorporative" PRX_PORT="3128" PRX_USER="admin" PRX_PASS="panda"
```

Despliegue con Microsoft Active Directory

A continuación, se detallan los pasos para el despliegue del software Cytomic EPDR en los equipos de una red Windows con Directorio Activo mediante GPO (Group Policy Object).

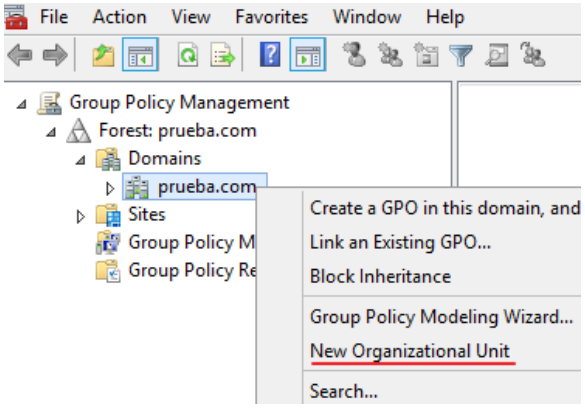


Figura 6.5: nueva unidad organizativa

1. Descarga del paquete Cytomic EPDR y comparte el instalador en la red.

• Coloca el instalador Cytomic EPDR en una carpeta compartida que sea accesible por todos los equipos que vayan a recibir el software.

2. Crea un nueva UO (Unidad Organizativa) de nombre "Despliegue Cytomic".

• Abre la `mmc` y agrega el snap-in Administrador de políticas de grupo.

- Con el botón de la derecha en el nodo del dominio, haz clic en Nuevo y Unidad Organizativa para crear una unidad organizativa de nombre "Despliegue Cytomic".
- Haz clic con el botón de la derecha del ratón en la unidad organizativa recién creada y selecciona

en el menú Bloquear herencia.

3. Crea una nueva GPO con el paquete de instalación

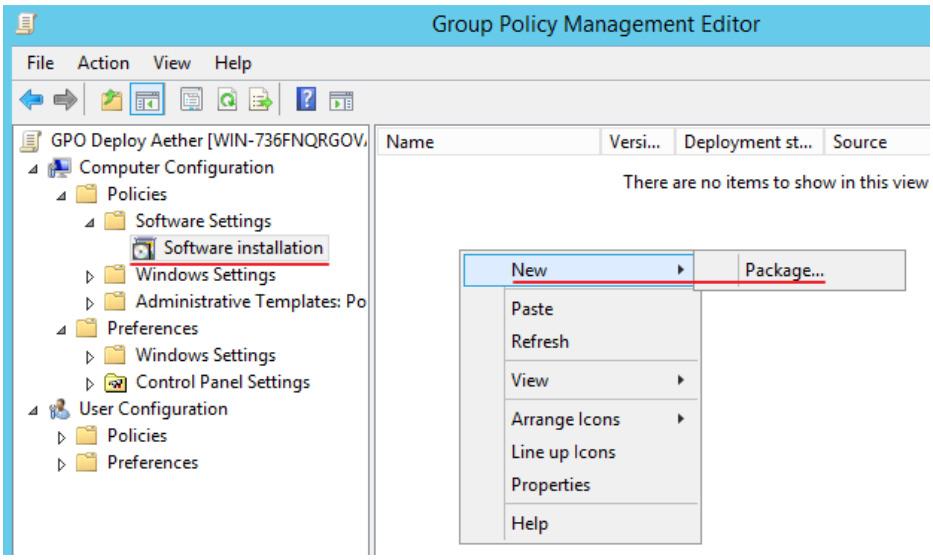


Figura 6.6: nuevo paquete de instalación

- Haz clic con el botón de la derecha del ratón en la Unidad Organizativa recién creada y selecciona Crear una GPO en este, de nombre "GPO Despliegue Cytomic".
- Edita la GPO recién creada y añade el paquete de instalación que contiene el software Cytomic EPDR en la rama Configuración del equipo, Políticas, Configuración de software, Instalación del software.
  - Con el botón de la derecha en el panel de la derecha, haz clic en Nuevo, Paquete.
  - Añade el fichero de instalación `.msi` de Cytomic EPDR.

4. Edita las propiedades del paquete

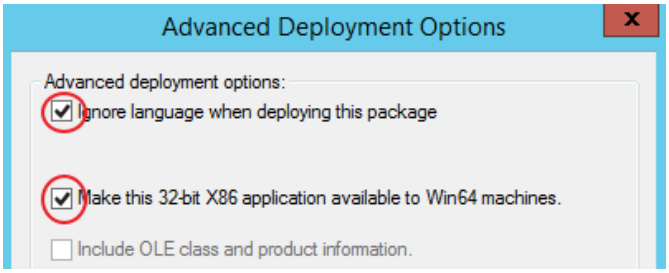


Figura 6.7: configuración del despliegue

- Haz clic con el botón derecho sobre el paquete agregado y selecciona Propiedades, pestaña Despliegue y Avanzado. Selecciona las casillas que evitan las comprobaciones de idioma y de plataforma entre el sistema operativo de destino y el definido en el instalador.
- Añade a la OU "Despliegue Cytomic" todos los equipos de la red que recibirán el agente.

Instalar mediante generación de imágenes gold

En redes grandes formadas por muchos equipos homogéneos, el procedimiento de instalación del sistema operativo y del software que lo acompaña puede automatizarse generando una imagen gold (también conocida como imagen "master", "base" o imagen "plataforma"). Posteriormente esta imagen se distribuye a todos los equipos de la red evitando una gran parte del proceso manual que supone instalar desde cero un equipo.

Para generar esta imagen es necesario instalar en un equipo de la red el sistema operativo ya actualizado junto a todo el software que el usuario vaya a necesitar, incluyendo las herramientas de seguridad.

Imágenes gold y Cytomic EPDR

La instalación del software Cytomic EPDR lleva asociada la asignación automática de un identificador único que Cytomic utiliza para referenciar el equipo en la consola de administración. Si se genera una imagen gold con el software Cytomic EPDR ya instalado y se copia en otros equipos, todos los equipos heredarán el mismo identificador, de forma que la consola mostrará un único equipo. Para evitar esta situación es necesario borrar este identificador con el programa `Panda Aether tool` accesible desde la página web de soporte de Cytomic en la siguiente URL:

https://www.pandasecurity.com/spain/support/card?id=700050

> *En esta URL además encontrarás el procedimiento detallado para preparar e instalar una imagen gold en entornos VDI persistentes y no persistentes.*

Entornos no persistentes y Cytomic EPDR

En los entornos VDI no persistentes algunos parámetros del hardware virtual como por ejemplo la MAC de las tarjetas de red pueden cambiar en cada reinicio. Por esta razón la identificación de estos equipos y su posterior asignación de una licencia no pueden realizarse mediante el hardware ya que el sistema consideraría a un equipo como nuevo en cada reinicio y consumiendo una licencia adicional. Además, el sistema de almacenamiento de un equipo VDI no persistente se limpia en cada reinicio, perdiéndose el identificador de Cytomic EPDR asignado.

Creación de una imagen gold para entornos VDI persistentes

En un entorno VDI persistente los equipos conservan entre reinicios la información que han salvado en el disco duro y por esta razón el proceso de creación de imagen gold solo requiere configuración de actualización de Cytomic EPDR.

Una vez instalado el sistema operativo actualizado e instalados todos los programas que los usuarios necesitarán sigue los pasos mostrados a continuación:

- Instala el software cliente Cytomic EPDR en el equipo según los pasos mostrados en el apartado "**Instalación local del software cliente**".
- Comprueba que el equipo tiene conexión a Internet y asígnale una configuración con la actualización de la protección y el conocimiento de Cytomic EPDR activada. Consulta el capítulo "**Gestión de configuraciones**" en la página **195** y el capítulo "**Actualización del software cliente**" en la página **143** para crear y asignar una configuración al equipo respectivamente.
- Ejecuta la herramienta `Panda Aether tool` y haz clic en el botón **Start cache scan** para analizar el equipo y precargar la caché de goodware de Cytomic EPDR.
- Haz clic en el botón **Unregister device** para borrar el identificador del equipo y asegúrate de que la casilla de selección **Is a gold image** NO está marcada.
- Apaga el equipo y genera la imagen con el software de administración de entornos virtuales que utilices.

Creación de una imagen gold para entornos VDI no persistentes

En un entorno VDI no persistente son necesarias dos configuraciones de actualización de Cytomic EPDR: una para actualizar la imagen gold en el momento de su preparación y mantenimiento, y otra para desactivar las actualizaciones en su ejecución ya que no tiene sentido consumir ancho de banda para actualizar Cytomic EPDR si el sistema de almacenamiento del equipo se va a revertir a su estado original en cada reinicio.

Preparación de la imagen gold

Una vez instalado el sistema operativo actualizado y todos los programas que los usuarios necesitarán sigue los pasos mostrados a continuación:

- Instala el software cliente Cytomic EPDR según los pasos mostrados en el apartado "**Instalación local del software cliente**".
- Comprueba que el equipo tiene conexión a Internet y asígnale una configuración con la actualización de la protección y el conocimiento de Cytomic EPDR activada. Consulta el capítulo "**Gestión de configuraciones**" en la página **195** y el capítulo "**Actualización del software cliente**" en la página **143** para crear y asignar una configuración al equipo respectivamente.
- Ejecuta la herramienta `Panda Aether tool` y haz clic en el botón **Start cache scan** para analizar el equipo y precargar la caché de goodware de Cytomic EPDR.
- Haz clic en el botón **Unregister device** para borrar el identificador del equipo y asegúrate de que la casilla de selección **Is a gold image** SI está marcada.
- Asigna al equipo una configuración que deshabilite la actualización de la protección y del conocimiento de Cytomic EPDR.
- Deshabilita el servicio Panda Endpoint Agent desde el panel de servicios de Windows para que no arranque automáticamente al usar esta imagen gold en las instancias virtuales.
- Apaga el equipo para generar la imagen con el software de administración de entornos virtuales que utilices.

- En el menú superior **Configuración**, panel lateral **Entornos VDI** define el máximo número de equipos que estarán activos simultáneamente. Esto permitirá una gestión automática de las licencias que consumen estas máquinas.

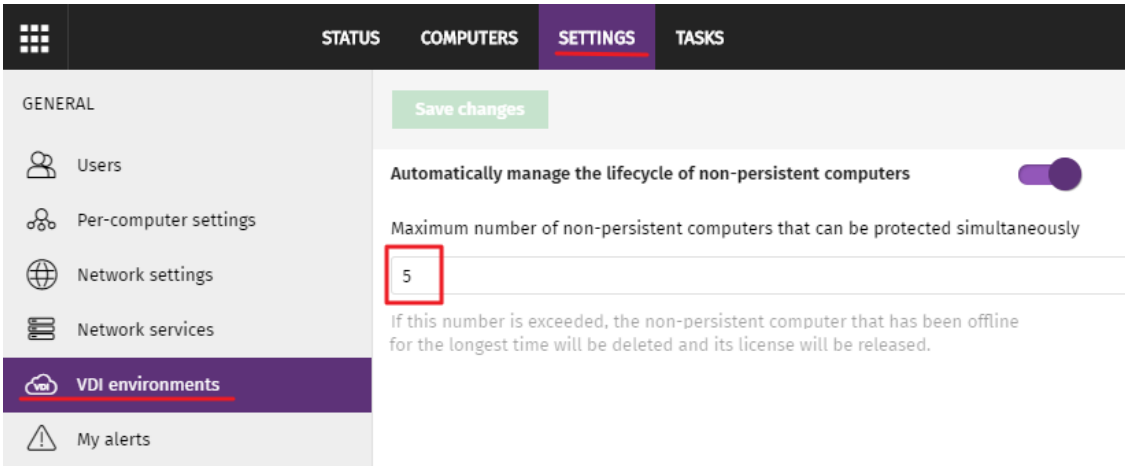


Figura 6.8: configuración del numero de licencias asignadas a equipos VDI no persistentes

Ejecución del entorno VDI no persistente

Para que Cytomic EPDR se ejecute con normalidad es necesario cambiar el tipo de inicio del servicio del agente de Cytomic, que previamente hemos deshabilitado en la imagen gold. Para ello sigue los pasos mostrados a continuación:

- Utiliza las herramientas de administración de GPO en un equipo físico conectada al dominio y crea una GPO para cambiar el tipo de inicio del servicio Panda Endpoint Agent.

> *Consulta la URL* **https://www.microsoft.com/es-ES/download/details.aspx?id=21895** *para conocer más detalles.*

- Dentro de la configuración de GPO, navega a la siguiente ruta: Computer Configuration, Policies, Windows Settings, Security Settings, System Services, Panda Endpoint Agent.
- Cambia la configuración del servicio a automática para que se modifique en el siguiente arranque y así pueda integrarse con la consola.

Mantenimiento de la imagen gold para entornos VDI no persistentes

Dado que los equipos VDI tienen asignada una configuración de actualización deshabilitada, es necesario actualizar la imagen gold de forma manual una vez al mes por lo menos para que reciba la ultima versión de la protección y del fichero de firmas. Para ello accede al equipo que tiene instalada la imagen gold y sigue los pasos mostrados a continuación:

- Habilita el servicio Panda Endpoint Agent.
- Comprueba que el equipo tiene conexión a Internet y asígnale una configuración con la actualización de la protección y el conocimiento de Cytomic EPDR activada.

- Ejecuta la herramienta `Panda Aether tool` y haz clic en el botón **Start cache scan** para analizar el equipo y precargar la caché de goodware de Cytomic EPDR.
- Haz clic en el botón **Unregister device** para borrar el identificador del equipo y asegúrate de que la casilla de selección **Is a gold image** SI está marcada.
- Asigna al equipo una configuración que deshabilite la actualización de la protección y del conocimiento de Cytomic EPDR.
- Deshabilita el servicio Panda Endpoint Agent para que no arranque automáticamente al usar esta imagen gold en las instancias virtuales.
- Apaga el equipo para generar la imagen con el software de administración de entornos virtuales que utilices.
- Sustituye en el entorno VDI la imagen anterior por la nueva obtenida.
- Repite este proceso de mantenimiento una vez al mes por lo menos.

Mostrar los equipos no persistentes

Cytomic EPDR identifica por el FQDN (Fully Qualifiend Domain Name) aquellos equipos cuyo identificador ha sido borrado mediante el programa `Panda Aether tool` y están marcados como imagen gold. Para obtener un listado de los equipos VDI no persistentes sigue los pasos mostrados a continuación:

- En el menú superior **Configuración**, panel lateral **Entornos DVI** haz clic en el link **Mostrar los equipos no persistentes**.
- Se mostrará el listado de equipos con el filtro **Equipos no persistentes** configurado.

Comprobar el despliegue

El administrador de la red dispone de tres formas complementarias para determinar el resultado del despliegue del software Cytomic EPDR en la red gestionada:

- Mediante el widget **Estado de protección**. Consulta el apartado "**Estado de protección**" en la página **380**.
- Mediante el listado **Estado de la seguridad de los equipos**. Consulta el apartado "**Listado de Estado de protección de los equipos**" en la página **400**.
- Mediante el registro Aplicación del visor de sucesos en los equipos Windows.

Visor de sucesos Windows

El registro Aplicación del visor de sucesos recoge información extendida sobre el resultado de la instalación del agente en el equipo del usuario y sobre su funcionamiento una vez instalado. A

continuación se muestra una tabla con la información suministrada por Cytomic EPDR en cada campo del visor de sucesos.

Mensaje	Nivel	Categoría	Id
The device %deviceId% was unregistered	Advertencia	Registro (1)	101
The device %deviceId% was registered	Información	Registro (1)	101
A new SiteId %SiteId% was set	Advertencia	Registro (1)	102
Error %error%: Cannot change SiteId	Error	Registro (1)	102
Error %error%: Calling %method%	Error	Registro (1)	103
Error %code%: Registering device, %description%	Error	Registro (1)	103
Installation success of %fullPath% with parameters %parameters%	Información	Instalación (2)	201
A reboot is required after installing %fullPath% with parameters %parameters%	Advertencia	Instalación (2)	201
Error %error%: executing %fullPath% with parameters %parameters%	Error	Instalación (2)	201
Message: %Module% installer error with next data: (optional) Extended code: %code% (optional) Extended subcode: %subCode% (optional) Error description: %description% (optional) The generic uninstaller should be launched (optional) Detected AV: Name = %name%, Version = %version%	Error	Instalación (2)	202
Uninstallation success of product with code %productCode% and parameters %parameters%	Información	Desinstalación (4)	401
A reboot is required after uninstalling product with code %productCode% and parameters %parameters%	Advertencia	Desinstalación (4)	401
Error %error%: Uninstalling product with code %productCode% and parameters %parameters%	Error	Desinstalación (4)	401
Uninstallation of product with code %productCode% and command line %commandLine% was executed	Información	Desinstalación (4)	401
Error %error%: Uninstalling product with code %productCode% and command line %commandLine%	Error	Desinstalación (4)	401
Error %error%: Uninstalling product with code %productCode% and command line %commandLine%	Error	Desinstalación (4)	401
Generic uninstaller executed: %commandLine%	Información	Desinstalación (4)	402
Error %error%: executed generic uninstaller %commandLine%	Error	Desinstalación (4)	402

Tabla 6.8: códigos de resultado del procesos de instalación del agente en el visor de sucesos

Mensaje	Nivel	Categoría	Id
Configuration success of product with code %productCode% and command line %commandLine%	Información	Reparación (3)	301
A reboot is required after configuring product with code %productCode% and command line %commandLine%	Advertencia	Reparación (3)	301
Error %error%: Configuring product with code %productCode% and command line %commandLine%	Error	Reparación (3)	301

Tabla 6.8: códigos de resultado del procesos de instalación del agente en el visor de sucesos

Desinstalar el software

Puedes desinstalar el software Cytomic EPDR de forma manual desde el panel de control del sistema operativo, o de forma remota desde la zona **Equipos** o desde los listados **Estado de la protección de los equipos** y **Licencias**.

Desinstalación manual

El propio usuario podrá ejecutar una desinstalación manual siempre y cuando el administrador de la protección no haya establecido una contraseña de desinstalación al configurar el perfil de la protección para su PC. Si lo ha hecho, se necesitará autorización o disponer de las credenciales necesarias para poder desinstalar la protección.

*Consulta el apartado "**Protección del agente mediante contraseña**" en la página **221** para establecer o eliminar la password de desinstalación del agente.*

La instalación de Cytomic EPDR incluye varios programas independientes, según sea la plataforma de destino:

- **Equipos Windows y macOS**: agente y protección.
- **Equipos Linux**: agente, protección y módulo del kernel.
- **Dispositivos Android**: protección.

Para desinstalar completamente Cytomic EPDR es necesario quitar todos los módulos. Si se desinstala únicamente el módulo de la protección, transcurrido un tiempo el agente la reinstalará de forma automática.

- **Windows 8 o superior:**
  - Panel de Control > Programas > Desinstalar un programa.

- También puedes desinstalar tecleando, en el menú Metro: "desinstalar un programa".

- **Windows Vista, Windows 7, Windows Server 2003 y superiores:**
  - Panel de Control > Programas y características > Desinstalar o cambiar.
- **En Windows XP:**
  - Panel de Control > Agregar o quitar programas.
- **macOS:**
  - Finder > Aplicaciones > Arrastra el icono de la protección que deseas desinstalar a la papelera o ejecuta el comando `sudo sh /Applications/Protection-Agent.app/Contents/uninstall.sh`
  - El agente no se desinstala arrastrando el icono a la papelera, en su lugar es necesario ejecutar el comando `sudo sh /Applications/Management-Agent.app/Contents/uninstall.sh`
- **Dispositivos Android:**
  - Accede a Configuración de Android. Seguridad > Administradores de dispositivos.
  - Desactiva la casilla correspondiente a Cytomic EPDR. A continuación, Desactivar > Aceptar.
  - De nuevo en la pantalla de Configuración de Android selecciona Aplicaciones instaladas. Haz clic en Cytomic EPDR > Desinstalar > Aceptar.
- **En Linux:**

En Linux se utiliza el entorno gráfico para gestionar paquetes incluido en la distribución.

- **Fedora**: Actividades > Software > Instalado
- **Ubuntu**: Software de Ubuntu > Instaladas

Se recomienda utilizar la línea de comandos para desinstalar el producto:

- **Ubuntu**
  - **Agente**: `sudo dpkg -r management-agent`
  - **Kernel**: `sudo dpkg -r protection-agent-dkms`
  - **Protección**: `sudo dpkg -r protection-agent-corporate`
- **Fedora** (sustituye "version" por la build del maquete pulsando la tecla de tabulación)
  - **Agente**: `sudo dnf remove management-agent-"version"`
  - **Kernel**: `sudo dnf remove protection-agent-dkms-"version"`
  - **Protección**: `sudo dnf remove protection-agent-corporate-"version"`

Resultado de la desinstalación manual

Al desinstalar el software Cytomic EPDR (agente Cytomic y Protección) el equipo desaparecerá completamente de la consola de administración. Todos los contadores, entradas en informes e información de la actividad del equipo y de sus procesos se borrarán.

Si, posteriormente, el mismo equipo vuelve a ser integrado en la consola de administración mediante la reinstalación del software Cytomic EPDR, se recuperará toda la información previamente eliminada.

Desinstalación remota

Para desinstalar de forma remota un equipo Windows protegido con Cytomic EPDR sigue los pasos mostrados a continuación:

- En la zona **Equipos**, o en los listados **Licencias** y **Estado de la protección de equipos** marca los equipos a desinstalar con las casillas de selección.
- En la barra de acciones haz clic en el botón **Eliminar**. Se mostrará una ventana de confirmación.
- En la ventana de confirmación haz clic en la casilla **Desinstalar el agente de Cytomic de los equipos seleccionados** para retirar por completo el software Cytomic EPDR.

Reinstalación remota

Para resolver algunos situaciones donde el software Cytomic EPDR presente una mal funcionamiento, se permite su reinstalación remota desde la consola de administración, tanto para equipos de usuario como para servidores.

La reinstalación del software se realiza por separado para el agente y para el módulo de la protección.

Requisitos de la funcionalidad de reinstalación remota

- Equipo de usuario o servidor con sistema operativo Windows instalado.
- Un equipo con el rol de descubridor asignado en el mismo segmento de red que el equipo a reinstalar y que comunique con la nube de Cytomic.
- Tener las credenciales de una cuenta de administrador local o de dominio.

Acceso a la funcionalidad

Desde los listados mostrados a continuación accesibles en el menú superior **Estado**, haciendo clic en el enlace **Añadir** del panel lateral:

- "**Listado de Estado de protección de los equipos**" en la página **400**.
- "**Listado Estado de gestión de parches**" en la página **328**.
- "**Listado Estado del cifrado**" en la página **366**.
- "**Listado de Licencias**" en la página **137**.
- "**Listado de hardware**" en la página **171**.

La funcionalidad también es accesible desde el listado de Equipos en el menú superior Equipos, haciendo clic en una rama del árbol de carpetas o filtros situado en el panel lateral.

> *Las opciones **Reinstalar la protección (requiere reinicio)** y **reinstalar agente** solo se mostrarán en equipos compatibles con esta funcionalidad.*

Descubrimiento de equipos a reinstalar

Utiliza el listado **Equipos no administrados descubiertos** para localizar los dispositivos en los que es necesario realizar la reinstalación. Consulta el apartado "**Visualizar equipos descubiertos**".

Reinstalación en un equipo

- Localiza en el listado el equipo a reinstalar.
- En el menú de contexto asociado al equipo selecciona la opción **Reinstalar la protección (requiere reinicio)** o **Reinstalar el agente**, se mostrará una ventana donde el administrador configurará el tipo de reinstalación. Consulta el apartado "**Ventana de selección Reinstalar la protección**" en la página **129** y "**Ventana de selección Reinstalar el agente**" en la página **130**.

Reinstalación en varios equipos

- Marca con las casillas de selección en el listado los equipos que reinstalarán su protección o agente.
- Selecciona en la barra de herramientas la opción **Reinstalar la protección (requiere reinicio)** o **Reinstalar el agente**. Se mostrará una ventana donde el administrador configurará el tipo de reinstalación. Consulta el apartado "**Ventana de selección Reinstalar la protección**" en la página **129** y "**Ventana de selección Reinstalar el agente**" en la página **130**.

Ventana de selección Reinstalar la protección

Al configurar la reinstalación de la protección se muestra una ventana flotante con dos opciones:

- **Reinstalar la protección inmediatamente (requiere reinicio)**: el reinicio se producirá en el plazo de 1 minuto. Si el equipo de destino no está accesible en ese momento por encontrarse apagado o fuera de red, la petición de reinicio se mantendrá en el servidor Cytomic EPDR durante 1 hora.
- **Ofrecer un margen de tiempo antes de forzar la reinstalación**: el reinicio se producirá en el plazo configurado por el administrador. Si el equipo de destino no está accesible por encontrarse apagado o fuera de red, la petición de reinicio se mantendrá en el servidor Cytomic EPDR durante 7 días.

En el momento en que el administrador inicia la reinstalación de la protección, el usuario del equipo recibe un mensaje emergente dándole la posibilidad de reiniciar el equipo en ese momento, o esperar a que finalice el tiempo definido por el administrador. Una vez que ha expirado el plazo, la protección se desinstalará y el equipo se reiniciará de forma automática para reinstalar la protección.

Si la desinstalación de la protección presenta algún tipo de problema, Cytomic EPDR iniciará de forma transparente al usuario un desinstalador genérico que tratará de desinstalar nuevamente la protección y limpiar cualquier rastro en el equipo. Para ello es posible que se requiera un reinicio adicional.

Ventana de selección Reinstalar el agente

Al configurar la reinstalación del agente se muestra una ventana flotante que solicita la información siguiente:

- **Seleccionar el equipo con el rol de descubridor desde el cual se reinstalará el agente**:
  - Asegúrate de que el equipo descubridor se encuentra en el mismo segmento de red que el equipo a reinstalar.
  - Si el equipo descubridor está apagado, la petición se encolará hasta que sea visible de nuevo. Las peticiones se encolan por un intervalo de 1 hora, transcurrido el cual se descartarán.
- **Credenciales para reinstalar los equipos**: introduce una o varias credenciales de instalación. Utiliza una cuenta de administración local del equipo o del dominio al que pertenece para completar la reinstalación con éxito.

Una vez introducida la información, el equipo con el rol de descubridor seguirá los pasos mostrados a continuación:

- Conectará con el equipo a reinstalar.
- Desinstalará el agente instalado en el equipo a reinstalar.
- Descargará un nuevo agente preconfigurado con el cliente, grupo y la configuración de red asignada al equipo, lo copiará y lo ejecutará remotamente en el equipo a reinstalar.
- Si hay algún problema en el transcurso de la operación se lanzará el desinstalador genérico y, si es necesario, se mostrará un mensaje al usuario con una cuenta atrás para el reinicio del equipo automático y un botón para reiniciar de forma manual e inmediata.

Códigos de error

Consulta el apartado "**Errores en el proceso de reinstalación del software de protección**" en la página **180** para obtener un listado de los mensajes de error y las acciones recomendadas para corregirlos.

Capítulo 7

Licencias

Para proteger los equipos de la red de las amenazas es necesario contratar licencias de Cytomic EPDR en un número igual al número de puestos de usuario y servidores a proteger. Una licencia de Cytomic EPDR solo se puede asignar a un único equipo en un momento concreto (estación de trabajo, dispositivo móvil o servidor).

Este capítulo trata la gestión de licencias de Cytomic EPDR: su asignación a los equipos de la red, liberación y comprobación de su estado.

CONTENIDO DEL CAPÍTULO

Definiciones y conceptos clave

Para interpretar correctamente la información y las gráficas suministradas por Cytomic EPDR que reflejan el estado de las licencias del producto es necesario conocer los términos mostrados en este apartado.

Para contratar y/o renovar licencias consulta con tu partner asignado.

Mantenimientos

Las licencias contratadas por el cliente se agrupan en mantenimientos. Un mantenimiento es un conjunto de licencias con características comunes:

- **Tipo de Producto**: Cytomic EPDR, Cytomic Encryption, Cytomic Patch, Cytomic EPDR con Cytomic Insights, Cytomic EPDR con Cytomic Data Watch, Cytomic EPDR con Cytomic Insights y Cytomic Data Watch.
- **Licencias contratadas**: número de licencias que pertenecen al mantenimiento.
- **Tipo de licencias**: NFR, Trial, Comercial, Suscripción.
- **Caducidad**: Fecha en la que las todas las licencias del mantenimiento caducan y los equipos dejarán de estar protegidos.

Estado de los equipos

Desde el punto de vista de las licencias, Cytomic EPDR distingue tres estados en los equipos de la red:

- **Equipos con licencia**: equipos con una licencia válida en uso asignada.
- **Equipos sin licencia**: equipos que no tienen una licencia en uso, pero que son candidatos a tenerla.
- **Excluidos**: equipos que no compiten por la obtención de una licencia. Estos equipos no están ni estarán protegidos por Cytomic EPDR aunque haya licencias sin asignar disponibles. Los equipos excluidos se seguirán mostrando en la consola y podrás utilizar algunas funcionalidades de gestión. Para excluir un equipo es necesario liberar su licencia de forma manual.

Es necesario distinguir entre el número de equipos sin licencia asignada (candidatos a tenerla en caso de existir licencias sin asignar) y el número de equipos excluidos (sin posibilidad de tener una licencia asignada, aunque haya licencias disponibles).

Estado de las licencias y grupos

Las licencias contratadas pueden tener dos estados:

- **Asignada**: licencia usada por un equipo de la red.

- **Sin asignar**: licencia que no está siendo usada por ningún equipo de la red.

Las licencias se agrupan por su estado en dos grupos:

- **Grupo de licencias usadas**: formado por todas las licencias asignadas a equipos.
- **Grupo de licencias sin usar**: formado por las licencias sin asignar.

Tipos de licencias

- **Licencias comerciales**: son las licencias estándar de Cytomic EPDR. Un equipo con una licencia comercial asignada tiene acceso a toda la funcionalidad del producto licenciado.
- **Licencias de prueba (Trial)**: son licencias gratuitas de prueba, válidas por un periodo limitado de 30 días. Un equipo con una licencia de prueba asignada tiene acceso completo a la funcionalidad del producto.
- **Licencias NFR**: licencias Not For Resale, destinadas a personal interno y partners de Cytomic. No está permitida su venta ni uso por personal o partners ajenos a Cytomic.
- **Licencias de tipo suscripción**: licencias que no tienen fecha de caducidad. El servicio es de tipo "pago por uso".

Asignar licencias

Puedes asignar licencias de forma manual o automática.

*Consulta el capítulo "**Gestión de equipos y dispositivos**" en la página **149** para obtener más información acerca de la herramienta de búsqueda y del árbol de carpetas y árbol de filtros.*

Asignación automática

Al instalar el software Cytomic EPDR en un equipo de la red, y siempre que existan licencias sin utilizar, el sistema le asignará de forma automática una licencia libre.

Asignación manual

Sigue los pasos mostrados a continuación.

- En el menú superior **Equipos** localiza el dispositivo a asignar la licencia mediante el árbol de carpetas, el árbol de filtros o la herramienta de búsqueda.
- Haz clic en el equipo para mostrar la ventana de detalle.
- En la pestaña **Detalles**, **Licencias** se mostrará el estado **Sin licencias**. Haz clic en el icono y se asignará de forma automática una licencia libre.

Liberar licencias

Liberar una licencia es un proceso equivalente a la asignación de licencias.

Liberación automática

- Al desinstalar el software Cytomic EPDR de un equipo de la red, el sistema recupera de forma automática una licencia y la devuelve al grupo de licencias sin usar.
- Al caducar un mantenimiento se liberan automáticamente licencias de los equipos siguiendo la lógica de licencias caducadas explicadas en el apartado "**Lógica de liberación de licencias caducadas**".

Liberación manual

La liberación manual de una licencia asignada previamente a un equipo lo convierte en un equipo excluido. Aunque existan licencias libres, estas no son asignadas al equipo de forma automática.

Para liberar manualmente una licencia de Cytomic EPDR de un equipo de la red sigue los pasos mostrados a continuación.

- En el menú superior **Equipos** localiza el dispositivo a liberar la licencia mediante el árbol de carpetas, el árbol de filtros o la herramienta de búsqueda.
- Haz clic en el equipo para mostrar su información.
- En la pestaña **Detalles, Licencias** se mostrará el estado del equipo. Haz clic en el icono  para liberar la licencia y devolverla al grupo de licencias sin utilizar.

Procesos asociados a la asignación de licencias

Caso I: Equipos con licencia asignada y equipos excluidos

Por defecto, a cada nuevo equipo integrado en la plataforma Cytomic se le asigna una licencia de producto Cytomic EPDR de forma automática, pasando a tomar el estado de **equipo con licencia asignada**. Este proceso se repite hasta que el grupo de licencias sin usar número quede reducido a 0.

Al retirar una licencia de un equipo de forma manual, éste toma el estado de **equipo excluido**. A partir de ese momento el equipo no competirá por la asignación de una licencia de forma automática, en el caso de existir licencias sin usar.

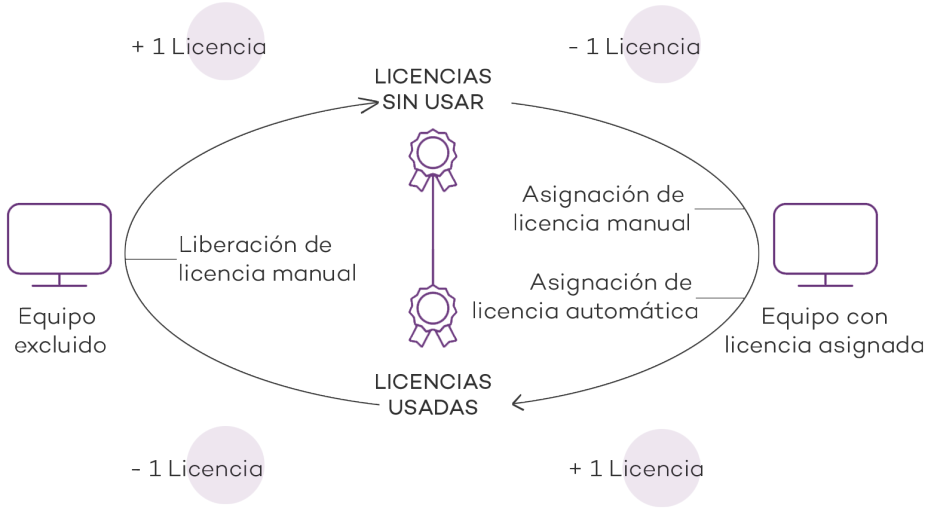


Figura 7.1: modificación de los grupos de licencias en equipos con licencia asignada y excluidos

Caso II: Equipos sin licencia asignada

En el momento en que nuevos equipos se incorporan a la plataforma Cytomic y el grupo de licencias sin usar está a 0, los equipos pasarán al estado **Equipos sin licencia**. Cuando estén disponibles nuevas licencias, estos equipos tomarán una licencia de forma automática.

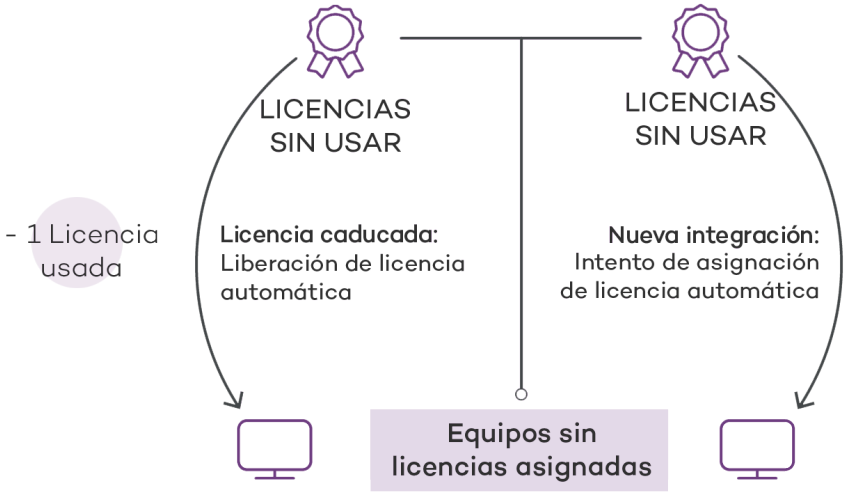


Figura 7.2: equipos sin licencia asignada por caducar su mantenimiento y estar vacío el grupo de licencias sin usar

De la misma forma, en el momento en que una licencia asignada caduque, un equipo de la red pasará al estado **Sin licencia asignada**, siguiendo la lógica de licencias caducadas explicadas el en apartado "**Lógica de liberación de licencias caducadas**".

Visualizar las licencias contratadas

Para visualizar el detalle de las licencias contratadas haz clic en el menú superior **Estado** y después en el menú lateral **Licencias**. Se mostrará una ventana con dos gráficas (widgets): **Licencias contratadas** y **Caducidad de licencias**.

Widget de Licencias

El panel representa cómo se distribuyen las licencias del producto contratado.

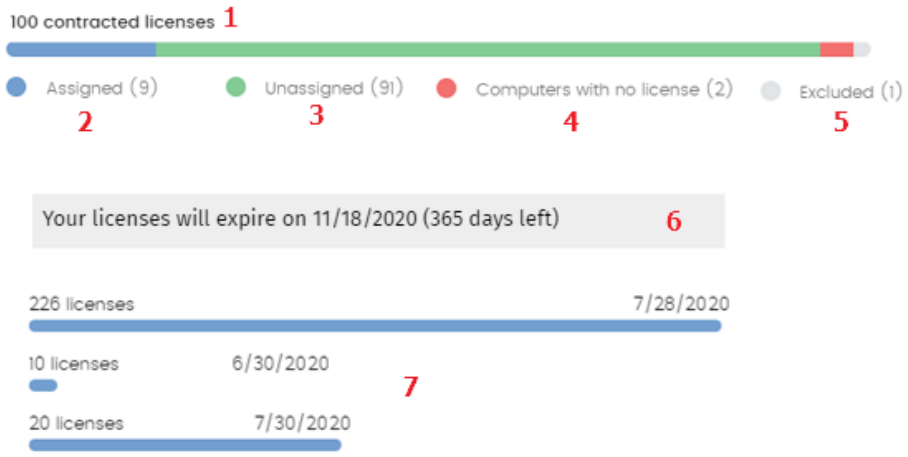


Figura 7.3: panel de licencias mostrando tres mantenimientos

Zona activa	Descripción
Número de licencias contratadas totales (1)	Número máximo de equipos que se pueden proteger, en el caso de que todas las licencias contratadas sean asignadas.
Número de licencias asignadas (2)	Número de equipos protegidos con una licencia asignada.
Número de licencias sin asignar (3)	Número de licencias contratadas pero que no se han asignado a ningún equipo y por lo tanto están sin utilizar.
Número de equipos sin licencia (4)	Equipos no protegidos por no disponer de licencias suficientes. El sistema les asignará licencia de forma automática si se adquieren nuevas licencias.
Número de equipos excluidos (5)	Equipos sin licencia asignada que no son candidatos a tenerla.
Caducidad de las licencias (6)	Si existe un único mantenimiento contratado, todas las licencias caducaran a la vez, en la fecha indicada.
Caducidad por mantenimiento (7)	Si un mismo producto ha sido contratado varias veces a lo largo del tiempo se mostrará una gráfica de barras horizontales con las licencias asociadas a cada contrato / mantenimiento y su fecha de caducidad independiente.

Tabla 7.1: campos del panel de licencias

Listado de Licencias

Muestra en detalle el estado de las licencias de los equipos de la red e incorpora filtros que ayudan a localizar los puestos de trabajo o dispositivos móviles en función de su estado.

Para acceder al listado de licencias haz clic en el botón **Añadir** del panel lateral **Mis listados,** o haz clic en el widget.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Estado de licencia	Estado en el que se encuentra el equipo con respecto al sistema de licencias.	• Licencia asignada • Equipo sin licencia • Equipo excluido
Última conexión	Fecha del último envío del estado del equipo a la nube de Cytomic.	Fecha.

Tabla 7.2: campos del listado Equipos protegidos

- **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el producto.	Cadena de caracteres
Tipo de equipo	Finalidad del equipo en la red de la organización.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS • Android
Directorio Activo	Ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo.	Cadena de caracteres
Servidor Exchange	Versión del servidor de correo instalada en el servidor.	Cadena de caracteres

Tabla 7.3: campos del fichero exportado Licencias

Campo	Descripción	Valores
Máquina virtual	Indica si el equipo es físico o esta virtualizado.	Booleano
Versión del agente	Versión interna del componente agente que forma parte del software de cliente Cytomic EPDR.	Cadena de caracteres
Versión de la protección	Versión interna del componente protección que forma parte del software de cliente Cytomic EPDR.	Cadena de caracteres
Fecha de arranque del sistema	Fecha en la que el equipo se inició por última vez.	Fecha
Fecha instalación	Fecha en la que el software Cytomic EPDR se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha del último envío del estado del equipo a la nube de Cytomic.	Fecha
Estado de licencia	Estado en el que se encuentra el equipo con respecto al sistema de licencias.	• Asignada • No asignada • Excluido
Grupo	Carpeta dentro del árbol de carpetas de Cytomic a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo.	Cadena de caracteres

Tabla 7.3: campos del fichero exportado Licencias

- **Herramienta de filtrado**

Campo	Descripción	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Tipo de equipo	Finalidad del equipo en la red de la organización.	• Estación • Portátil • Dispositivo móvil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS • Android

Tabla 7.4: campos de filtrado para el listado Licencias

Campo	Descripción	Valores
Última conexión	Fecha del último envío del estado de Cytomic EPDR a la nube de Cytomic.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días • Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Estado de licencia	Estado en el que se encuentra el equipo con respecto al sistema de licencias.	• Asignada • Sin licencia • Excluido

Tabla 7.4: campos de filtrado para el listado Licencias

- **Ventana detalle del equipo**

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta el apartado "**Información de equipo**" en la página **177** para obtener más información.

- **Filtros preestablecidos desde el panel**

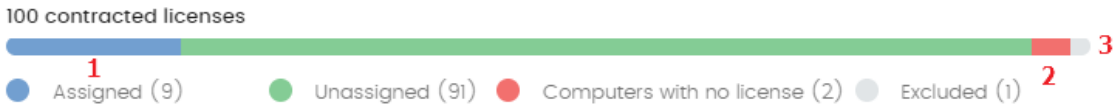


Figura 7.4: zonas activas del panel licencias contratadas

Se muestra el listado **Licencias** con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

Campo para filtrar	Valor
(1) Estado de licencia	Asignada
(2) Estado de licencia	Sin licencia
(3) Estado de licencia	Excluido

Tabla 7.5: filtros del listado de licencias

Licencias caducadas

Excepto los mantenimientos de tipo suscripción, todos los demás tienen asignada una fecha de caducidad, pasada la cual los equipos de la red dejarán de están protegidos.

Mensajes de caducidad próxima y vencida

A los 30 días de vencer el mantenimiento, el panel **Licencias** contratadas mostrará un mensaje con los días que quedan para finalizar el mantenimiento y el número de licencias que se verán afectadas.

Adicionalmente, se mostrará un mensaje por cada mantenimiento caducado, indicando el número de licencias que ya no son funcionales en el plazo de los 30 últimos días.

Si todos los productos y mantenimientos están caducados se denegará el acceso a la consola de administración.

Lógica de liberación de licencias caducadas

Cytomic EPDR no mantiene una relación de pertenencia estricta entre mantenimientos de licencias y equipos. Los equipos con licencias asignadas no pertenecen a un mantenimiento concreto u otro; en su lugar todas las licencias de todos los mantenimientos se suman en un único grupo de licencias disponibles, que posteriormente se reparten entre los equipos de la red.

En el momento en que un mantenimiento caduca, Cytomic EPDR determina el número de licencias asignadas a ese mantenimiento. Acto seguido, se ordenan los equipos de la red con licencias asignadas utilizando como criterio de ordenación el campo **Última conexión**, que contiene la fecha en la que el equipo se conectó por última vez a la nube de Cytomic.

Los equipos candidatos a retirar su licencia de protección son aquellos no vistos en el periodo de tiempo alejado. Así, se establece un sistema de prioridades donde la mayor probabilidad de retirar una licencia se asigna a los equipos que no han sido utilizados recientemente.

La lógica de liberación de licencias caducadas afecta a todos los dispositivos compatibles con Cytomic EPDR que tengan licencias asignadas.

Buscar equipos según su estado de licencia

Cytomic EPDR incluye la categoría **Licencia** para crear filtros que ayuden a localizar los equipos de la red que tengan un determinado estado de licencia.

*Consulta el capítulo "**Crear y organizar filtros**" en la página **154** para obtener más información acerca de cómo crear un filtro en Cytomic EPDR.*

A continuación, se muestran las propiedades de la categoría **Licencias** para crear filtros que generen listados de equipos con información relevante sobre licencias.

Categoría	Propiedad	Valor	Descripción
Licencia	**Estado**	Establece filtros según el estado de la licencia.	
		Asignada	Lista los equipos con una licencia Cytomic EPDR asignada.
		Sin asignar	Lista los equipos que no tiene una licencia Cytomic EPDR asignada.
		Desasignada manualmente	El administrador de la red liberó la licencia Cytomic EPDR previamente asignada al equipo.
		Desasignada automáticamente	El sistema liberó al equipo la licencia Cytomic EPDR asignada previamente.

Tabla 7.6: campos del listado Equipos protegidos

Capítulo 8

Actualización del software cliente

Cytomic EPDR es un servicio cloud gestionado, y por lo tanto el administrador de la red no necesita ejecutar tareas de actualización de la infraestructura de back-end encargada de soportar el servicio de protección. Sin embargo, sí es necesaria la actualización del software cliente instalado en los equipos de la red.

CONTENIDO DEL CAPÍTULO

Módulos actualizables en el software cliente

Los elementos instalados en el equipo del usuario son:

- Agente de comunicaciones Cytomic Platform.
- Motor de la protección Cytomic EPDR.
- Archivo de identificadores / fichero de firmas para la protección antivirus tradicional.

Dependiendo de la plataforma a actualizar, el procedimiento y las posibilidades de configuración varían tal y como se indica en la tabla **8.1**.

Módulo	Plataforma			
	Windows	**macOS**	**Linux**	**Android**
Agente Cytomic	Bajo demanda			
Protección Cytomic EPDR	Configurable	Configurable	Configurable	No
Archivo de identificadores	Habilitar / Deshabilitar	Habilitar / Deshabilitar	Habilitar / Deshabilitar	No

Tabla 8.1: formas de actualización según el componente del software cliente

- **Bajo demanda**: el administrador puede iniciar la actualización una vez que esté disponible, o retrasarla hasta el momento que considere oportuno.
- **Configurable**: el administrador podrá definir en la consola web ventanas de actualización recurrentes y en el futuro, siendo posible además desactivar la actualización.
- **Habilitar / Deshabilitar**: El administrador puede desactivar la actualización. Si la actualización está activada ésta se producirá automáticamente cuando esté disponible.
- **No**: El administrador no puede influir en el proceso de actualización. Las actualizaciones se efectuarán cuando estén disponibles y no es posible deshabilitarlas.

Actualización del motor de protección

Para configurar la actualización del motor de protección crea y asigna un perfil de configuración de tipo **Ajustes por equipo**, accesible desde el menú superior **Configuración**, en el panel de la izquierda de la consola de administración.

Actualizaciones

Para habilitar la actualización automática del módulo de protección Cytomic EPDR haz clic en el botón de activación **Actualizar automáticamente Cytomic EPDR en los dispositivos**. Esta acción habilitará el resto de configuraciones de la página. Si esta opción esta deshabilitada, el módulo de protección no se actualizará nunca.

Se desaconseja totalmente deshabilitar la actualización del motor de protección. Los equipos con la protección sin actualizar serán más vulnerables en el medio plazo frente a las amenazas avanzadas y el malware.

Aplicar actualizaciones en rangos de horas

Indica los siguientes parámetros para que los equipos apliquen las actualizaciones disponibles dentro de un rango de horas concreto:

- Hora de inicio
- Hora de fin

Para aplicar las actualizaciones en cualquier momento haz clic en la casilla de selección **A cualquier hora**.

Aplicar actualizaciones en fechas determinadas

Utiliza el desplegable para indicar las fechas en las que se aplicará la actualización:

- **En cualquier fecha**: las actualizaciones se aplicarán el día que estén disponibles. Esta opción no limita la actualización de Cytomic EPDR a fechas concretas.
- **Los siguientes días de la semana**: utiliza las casillas de selección para establecer los días de la semana en los que Cytomic EPDR se actualizará. La actualización se producirá el primer día de la semana que coincida con la selección del administrador en caso de haber una actualización disponible.
- **Los siguientes días del mes**: utiliza los desplegables para establecer un rango de días hábiles dentro del mes en los que Cytomic EPDR se actualizará. La actualización se producirá el primer día del mes que coincida con los seleccionados por el administrador en caso de haber una actualización disponible.
- **Los siguientes días**: utiliza los desplegables para establecer un rango de días hábiles dentro del calendario en los que Cytomic EPDR se actualizará. Los rangos definidos en esta opción se establecen de forma absoluta para casos en que el administrador quiera establecer rangos que no se repiten en el tiempo. De esta forma, se permite definir rangos de fechas concretas de actualización, pasadas las cuales dejan de tener efecto. Este método requiere redefinir los rangos de actualización de forma constante una vez hayan vencido.

Reinicio de equipos

Cytomic EPDR permite definir la lógica de reinicios en caso de que sea necesario, mediante el desplegable situado al final de la pantalla de configuración:

- **No reiniciar automáticamente**: se mostrará al usuario una ventana en intervalos de tiempo cada vez más cortos, aconsejando el reinicio de la máquina para aplicar la actualización.
- Reiniciar automáticamente sólo las estaciones de trabajo.
- Reiniciar automáticamente sólo los servidores.
- Reiniciar automáticamente tanto estaciones de trabajo como servidores.

Actualización del agente de comunicaciones

La actualización del agente Cytomic se ejecuta bajo demanda. Cytomic EPDR incluirá una notificación en la consola de administración indicando la existencia de una nueva versión del agente, y el administrador podrá lanzar la actualización cuando lo desee.

La actualización del agente Cytomic no requiere reinicio del equipo del usuario y suele implicar cambios y mejoras en la consola de administración que facilitan la gestión de la seguridad.

Actualización del conocimiento

La configuración de la actualización del fichero de firmas en Cytomic EPDR se realiza en el perfil de configuración de seguridad asignado al equipo, según sea su tipo.

Dispositivos Windows, Linux y macOS

La configuración se realiza en los perfiles de tipo **Estaciones y Servidores**, accesibles desde el panel de la izquierda en el menú superior **Configuración**.

En la pestaña **General** las opciones disponibles son:

- **Actualizaciones automáticas de conocimiento**: habilita o deshabilita la descarga del fichero de firmas. Si se deshabilita el fichero de firmas nunca será actualizado.

Se desaconseja totalmente deshabilitar la actualización del conocimiento. Los equipos con la protección sin actualizar serán más vulnerables en el corto plazo frente a las amenazas avanzadas y el malware.

- **Realizar un análisis en segundo plano cada vez que se actualice el conocimiento**: lanza de forma automática un análisis cada vez que un fichero de firmas se descarga en el equipo. El análisis tendrá prioridad mínima para no interferir en el trabajo del usuario.

Dispositivos Android

La configuración se realiza en los perfiles **Dispositivos Android**, accesibles desde el panel de la izquierda en el menú superior **Configuración**.

Cytomic EPDR permite limitar las actualizaciones del software de forma que no consuman datos de conexiones móviles sujetas a tarificación.

Haz clic en el botón de **Activación** para restringir las actualizaciones a aquellos momentos en que el smartphone o tablet tenga conexión wifi disponible.

Parte 4

Gestión de los dispositivos de la red

Capítulo 9: Gestión de equipos y dispositivos

Capítulo 10: Gestión de configuraciones

Capítulo 11: Configuración remota del agente

Capítulo 9

Gestión de equipos y dispositivos

La consola web muestra los dispositivos administrados de forma ordenada y flexible, aplicando distintas estrategias que permiten localizarlos rápidamente para facilitar su gestión.

Para que un equipo de la red sea gestionable por Cytomic EPDR se requiere como mínimo de la instalación del agente Cytomic en el equipo. Los equipos sin licencia pero con el agente Cytomic instalado, aparecerán en la consola de administración, aunque su protección estará desactualizada y no podrán ejecutar tareas, análisis ni otras acciones vinculadas con el servicio de protección.

CONTENIDO DEL CAPÍTULO

La zona equipos

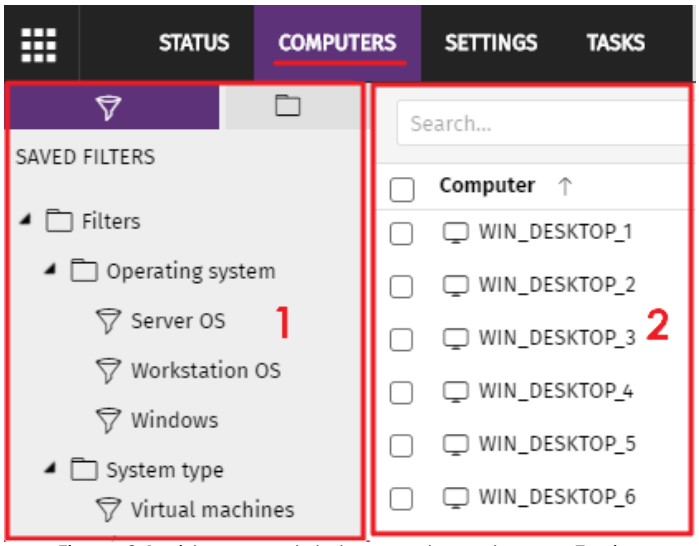


Figura 9.1: vista general de los paneles en la zona Equipos

La zona **Equipos** es el área de la consola web donde se gestionan los dispositivos integrados en Cytomic EPDR.

Para acceder a la ventana de administración de equipos, haz clic en el menú superior **Equipos**. Se mostrarán dos zonas diferenciados: el panel lateral con el **árbol de equipos (1)** y el panel central con el **listado de equipos (2)**. Ambos paneles trabajan de forma conjunta: al seleccionar una rama del árbol de equipos, el listado de equipos se actualiza con todos sus equipos asignados.

Mostrar equipos en subgrupos

Para ampliar o limitar el listado de los equipos activa o desactiva la opción **Mostrar equipos de los subgrupos** disponible en el menú de contexto general.

- Si la opción está activada, al seleccionar una rama del árbol se mostrarán todos los equipos que pertenecen a ella y a todas las ramas de orden inferior.
- Si la opción esta desactivada, al seleccionar una rama del árbol se mostrarán únicamente todos los equipos que pertenecen a ella.

El panel Árbol de equipos

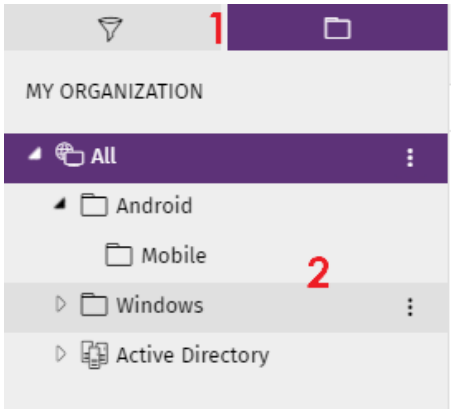


Figura 9.2: el panel Árbol de equipos

Cytomic EPDR representa la estructura de equipos mediante el **Árbol de equipos (1)**, que presenta dos vistas o árboles independientes **(2)**:

- **Árbol de filtros**: gestiona los equipos de la red mediante agrupaciones dinámicas. La pertenencia de un equipo a una agrupación de este tipo se establece de forma automática.
- **Árbol de grupos**: gestiona los equipos de la red mediante agrupaciones estáticas. La pertenencia de un equipo a una agrupación de este tipo se establece de forma manual.

Los dos árboles muestran el parque de equipos y dispositivos Android del cliente de distintas formas, con el objeto de favorecer la ejecución de tareas de diferentes tipos, tales como:

- Localizar los equipos que cumplan con características determinadas, relativas al hardware, software o a la seguridad.
- Asignar perfiles de configuración de seguridad de forma rápida.
- Ejecutar acciones de resolución sobre grupos de equipos.

*Para localizar equipos desprotegidos o de características determinadas relativas a la seguridad o al estado de la protección consulta el capítulo "***Visibilidad del malware y del parque informático***" en la página* **379**. *Para asignar perfiles de configuración de seguridad consulta el apartado "***Asignación manual y automática de configuraciones***" en la página* **203**. *Para ejecutar tareas de resolución de problemas consulta el capítulo "***Herramientas de resolución***" en la página* **493**.

Al pasar el puntero del ratón por las ramas del árbol de filtros y de grupos se muestra el icono de menú de contexto. Haz clic para desplegar un menú emergente con todas las operaciones disponibles sobre la rama del árbol seleccionada.

Árbol de filtros

Es una de las dos vistas del Árbol de equipos, y permite agrupar de forma dinámica los equipos en la red mediante reglas y condiciones que describen características de los dispositivos. Estas reglas se pueden combinar mediante operaciones lógicas para producir expresiones complejas.

Para acceder al Árbol de filtros haz clic en el icono del filtro  desde el panel de la izquierda. Al hacer clic en los diferentes elementos del árbol, el panel de la derecha se actualiza, presentando todos los equipos que cumplen con los criterios establecidos en el filtro seleccionado.

Definición de filtro

Son agrupaciones dinámicas de equipos. La pertenencia de un equipo a un filtro se determina de forma automática cuando el equipo en cuestión cumple con las condiciones de pertenencia al filtro que haya configurado el administrador.

Un equipo puede pertenecer a más de un filtro.

Un filtro está constituido por un conjunto de reglas o condiciones que los equipos tendrán que satisfacer para pertenecer a aquél. En la medida en que el equipo cumpla con las características descritas formará parte del filtro; de la misma forma, cuando un equipo cambie su estado y no

cumpla los criterios de pertenencia, automáticamente dejará de formar parte de la agrupación descrita por el filtro.

Los filtros se pueden ordenar de forma manual agrupándolos en carpetas, con el criterio que el administrador considere oportuno.

Filtros predefinidos

Cytomic EPDR incorpora filtros de uso muy común que el administrador puede utilizar desde el primer momento para ordenar y localizar equipos en la red. Los filtros predeterminamos se pueden modificar o borrar.

No es posible recuperar un filtro predeterminado que haya sido borrado.

Nombre	Grupo	Descripción
Estaciones y servidores	Tipo de sistema	Lista los equipos físicos de sobremesa o servidores.
Portátiles	Tipo de sistema	Lista los equipos físicos portátiles.
Móviles y tablets	Tipo de sistema	Lista los dispositivos de tipo smartphone y tablet.
Virtuales	Tipo de sistema	Lista los equipos virtualizados.
SO de servidores	Sistema operativo	Lista los equipos con un sistema operativo de tipo Servidor instalado.
SO de estaciones	Sistema operativo	Lista los equipos con un Sistema operativo de tipo estación de trabajo.
Windows	Sistema operativo	Lista todos los equipos con sistema operativo Windows instalado.
macOS	Sistema operativo	Lista todos los equipos con sistema operativo macOS instalado.
Linux	Sistema operativo	Lista todos los equipos con sistema operativo Linux instalado.
Android	Sistema operativo	Lista todos los dispositivos equipos con sistema operativo Android instalado.
Java	Software	Lista todos los equipos que tiene instalado el SDK JRE Java.
Adobe Acrobat Reader	Software	Lista todos los equipos que tiene instalado el software Acrobat Reader.
Adobe Flash Player	Software	Lista todos los equipos que tiene instalado el plugin de reproducción Flash.

Tabla 9.1: listado de filtros predefinidos

Nombre	Grupo	Descripción
Google Chrome	Software	Lista todos los equipos que tiene instalado el navegador Chrome.
Mozilla Firefox	Software	Lista todos los equipos que tiene instalado el navegador Firefox.
Servidores Exchange	Software	Lista los equipos que tienen instalado el servidor de correo Microsoft Exchange Server.

Tabla 9.1: listado de filtros predefinidos

Crear y organizar filtros

Para crear y organizar filtros haz clic en el icono de menú de contexto de las ramas del árbol de filtros. Se mostrará un menú emergente con las opciones permitidas en esa rama en particular.

Crear carpetas

- Haz clic en el menú de contexto de la rama donde quieres crear la carpeta y haz clic en **Añadir carpeta**.
- Introduce el nombre de la carpeta y haz clic en **Aceptar**.

Una carpeta no puede depender de un filtro. Si seleccionas un filtro antes de crear la carpeta, ésta se creará al mismo nivel que el filtro, compartiendo su carpeta padre.

Crear filtros

Para crear un filtro es necesario seguir los pasos mostrados a continuación:

- Selecciona el menú de contexto de la carpeta en el árbol donde será creado el filtro.
  - Si deseas crear una estructura jerárquica de filtros, crea carpetas contenedoras y mueve los filtros dentro de ellas. Una carpeta puede contender otras carpetas con filtros.
- Haz clic en **Añadir filtro**.
- Introduce el nombre del filtro. No es necesario que sea un nombre único. El resto de la configuración se detalla en el apartado "**Configurar filtros**".

Borrar filtros y carpetas

Para borrar un filtro o una carpeta haz clic en el menú de contexto de la rama a borrar y elige la opción **Eliminar**. La rama se borrará junto a todos sus descendientes.

No se permite borrar el nodo raíz Filtros.

Mover y copiar filtros y carpetas

- Haz clic en el menú de contexto de la rama a copiar o mover.
- Haz clic en **Mover** o **Hacer una copia**. Se mostrará una ventana emergente con el árbol de filtros de destino.
- Selecciona la carpeta de destino y pulsa **Aceptar**.

No es posible copiar carpetas de filtros. Únicamente se permite la copia de filtros.

Renombrar filtros y carpetas

- Haz clic en el menú de contexto de la rama a renombrar.
- Haz clic en **Renombrar**.
- Introduce el nuevo nombre.

No es posible renombrar la carpeta raíz. Para renombrar un filtro es necesario editarlo.

Configurar filtros

Haz clic en el menú de contexto del filtro y elige la entrada **Editar filtro** del menú. Se mostrará la ventana de configuración de filtros.

Un filtro está formado por una o más reglas, relacionados entre sí mediante operadores lógicos Y / O. Un equipo formará parte de un filtro si cumple con los valores especificados en las reglas del filtro.

El esquema general de un filtro se compone de cuatro bloques:

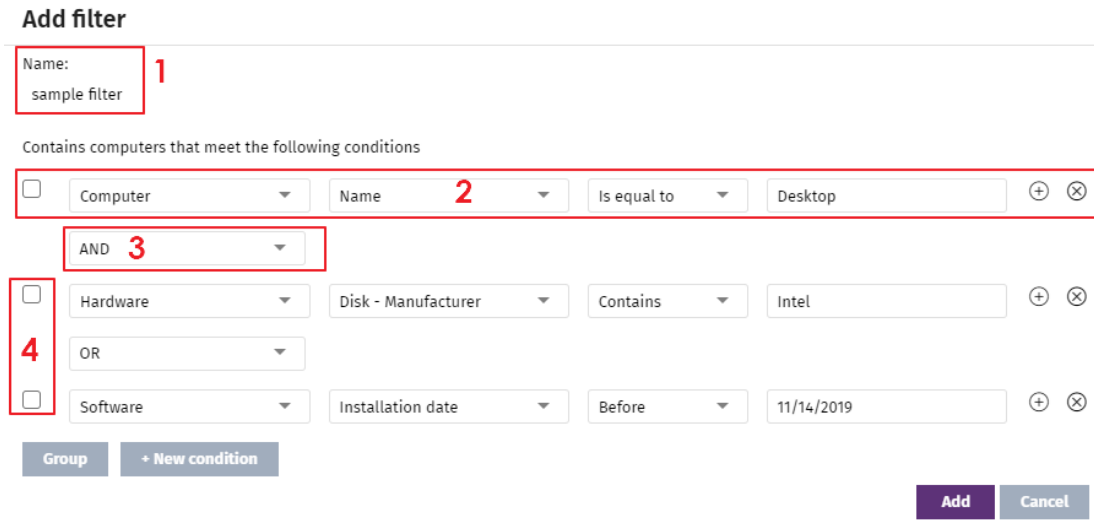


Figura 9.3: vista general de configuración de un filtro

- **Nombre del filtro (1)**: identifica al filtro.
- **Reglas de filtrado (2)**: construye condiciones indivisibles de pertenencia al filtro. Una regla de filtrado únicamente comprueba una característica concreta de los equipos de la red.
- **Operadores lógicos (3)**: combina dos reglas de filtrado mediante los operadores lógicos Y o O.
- **Agrupaciones (4)**: varían el orden de evaluación de las reglas de filtrado configuradas y relacionadas mediante operadores lógicos.

Reglas de filtrado

Una regla de filtrado se compone de los elementos mostrados a continuación:

- **Categoría**: agrupa las propiedades en secciones para facilitar su localización.
- **Propiedad**: característica del equipo que se evaluará para determinar su pertenencia al filtro.
- **Operador**: establece el modo de comparación del contenido de la propiedad del equipo con el valor de referencia que establezca el administrador para el filtro.
- **Valor**: contenido de la propiedad. Dependiendo del tipo de propiedad el campo valor cambiará para ajustarse a entradas de tipo fecha, literales etc.

Para añadir reglas de filtrado a un filtro haz clic en el icono y para borrarlas en el icono .

Operadores lógicos

Para combinar dos reglas en un mismo filtro se utilizan los operadores lógicos Y y O. Al añadir una segunda regla y sucesivas a un filtro se mostrará de forma automática un desplegable con los operadores lógicos disponibles, que se aplicarán a las reglas adyacentes.

Agrupaciones de reglas de filtrado

Los paréntesis en una expresión lógica se utilizan para variar el orden de evaluación de los operadores que relacionan las reglas de filtrado introducidas.

Para encerrar dos o más reglas en un paréntesis crea una agrupación marcando con las casillas de selección las reglas que formarán parte del grupo y haz clic en el botón **Agrupación**. Se mostrará una línea delgada que abarcará las reglas de filtrado que forman parte de la agrupación.

Mediante el uso de paréntesis se definen agrupaciones de varios niveles para poder anidar grupos de operandos en una expresión lógica.

Casos de uso comunes

A continuación se indican a modo de ejemplo algunos casos de uso de filtros muy utilizados por los administradores de redes:

Equipos sin parches instalados

Lista los equipos que no tienen un determinado parche instalado. Consulta el capítulo "**Cytomic Patch (Actualización de programas vulnerables)**" en la página **307** para obtener más información sobre Cytomic Patch.

- **Categoría**: Programas
- **Propiedad**: Nombre del software
- **Condición**: No contiene
- **Valor**: {Nombre del parche}

Equipos sin conectar con la nube de Cytomic en X días

Lista los equipos que no conectaron con la nube de Cytomic en el intervalo configurado:

- **Categoría**: Equipo
- **Propiedad**: Última conexión
- **Condición**: Antes de
- **Valor**: {Fecha en formato dd/mm/aa}

Equipos aislados

Lista los equipos que han sido aislados de la red. Consulta el apartado "**Aislar un equipo**" en la página **499**.

- **Categoría**: Equipo
- **Propiedad**: Estado de aislamiento
- **Condición**: Es igual

- **Valor**: Aislado

Integración con otras herramientas de gestión

Muestra los equipos que coinciden con alguno de los nombres de equipo especificados en un listado obtenido por una herramienta de terceros. Cada línea del listado deberá de terminar con un retorno de carro y será considerada como un nombre de equipo.

- **Categoría**: Equipo
- **Propiedad**: Nombre
- **Condición**: En
- **Valor**: listado de nombres de equipo

Árbol de grupos

El árbol de grupos reúne de forma estática los equipos en la red en las agrupaciones definidas por el administrador.

Para acceder al árbol de grupos:

- Haz clic en el icono de carpeta en el panel lateral.
- Al hacer clic en las diferentes ramas del árbol, el panel de la derecha se actualiza, presentando todos los equipos que contienen el grupo seleccionado y sus subgrupos.

Definición de grupo

Es un contenedor de equipos asignados de forma manual por el administrador. El árbol de grupos admite crear una estructura de n niveles compuesta por grupos, subgrupos y equipos.

El máximo nivel de profundidad del árbol es 10.

Tipos de grupos

Tipo de grupo	Descripción
Grupo raíz	Grupo padre del que cuelgan el resto de carpetas.
Grupos nativos	Grupos estándar de Cytomic EPDR que soportan todas las operaciones (movimiento, renombrado, borrado etc.) Pueden contener otros grupos nativos y equipos.

Tabla 9.2: tipos de grupos en Cytomic EPDR

Tipo de grupo	Descripción
Grupos IP	Grupo nativo con IPs o rangos de IPs asociados para acelerar la integración de nuevos equipos en el servicio de seguridad.
Grupos Directorio Activo	Replican la estructura del Directorio Activo instalado en la empresa, por esta razón tienen limitadas algunas operaciones. Pueden contener otros grupos de Directorio Activo y equipos.
Grupo raíz del directorio activo	Abarca todos los dominios del Directorio Activo configurados en la red de la organización. Contiene grupos de dominio Directorio Activo.
Grupo de dominio Active Directory	Ramas del Directorio Activo que representan dominios. Contienen otros grupos de dominio Directorio Activo, grupos Directorio Activo y equipos.

Tabla 9.2: tipos de grupos en Cytomic EPDR

El tamaño de la organización, lo homogéneos que sean los equipos gestionados y la presencia o no de un servidor de Directorio Activo en la red de la empresa determinará la estructura del árbol de grupos. La estructura de grupos podrá variar desde un árbol plano de un único nivel para los casos más sencillos, hasta una estructura compleja con varios niveles, para redes grandes formadas por equipos muy heterogéneos.

En un momento determinado un equipo solo puede pertenecer a un grupo, a diferencia de los filtros donde un equipo puede pertenecer a varios simultáneamente.

Grupos de Directorio Activo

Para las organizaciones que tienen instalado un servidor de Directorio Activo en la red, Cytomic EPDR puede obtener de forma automática la estructura configurada y replicarla en el árbol de grupos: los agentes Cytomic reportan a la consola Web el grupo del Directorio Activo al que pertenecen y, conforme se despliegan los agentes en los equipos, el árbol se completará con las distintas unidades organizativas. De esta manera, bajo la rama se presentará una distribución de los equipos familiar para el administrador, con el objeto de acelerar la localización de dispositivos y su gestión.

Para mantener la coherencia entre el Directorio activo de la empresa y el árbol representado en la consola de administración, los grupos de directorio activo no son modificables desde la consola de Cytomic EPDR: únicamente cambiarán cuando lo haga la estructura de Directorio Activo subyacente. Los cambios se replicarán en la consola Web de Cytomic EPDR transcurrido un máximo de 15 minutos.

Crear y organizar grupos

Para acceder a las operaciones disponibles sobre grupos haz clic en el icono de menú de contexto de las ramas del árbol de grupos. Se mostrará un menú emergente con las opciones permitidas para esa rama en particular.

Crear grupos

- Selecciona el menú de contexto del grupo padre del cual dependerá el grupo a crear, y haz clic en **Añadir grupo**.
- Introduce el nombre del grupo en la caja de texto **Nombre** y haz clic en el botón Añadir.

> *No es posible crear grupos de Directorio Activo en el árbol de grupos. Solo se replicarán los grupos y unidades organizativas creadas en el servidor de Directorio Activo de la empresa.*

Si deseas que los equipos sobre los cuales se va a instalar un agente Cytomic EPDR se muevan a un determinado grupo según su IP sigue los pasos mostrados a continuación:

- Haz clic en el enlace **Añadir reglas de asignación automática por IPs**, se mostrará una caja de texto donde añadir las IPs de los equipos que serán movidos al grupo.
- Especifica IPs individuales separadas por comas o rangos de IPs separados por un guion.

El movimiento del equipo se efectuará únicamente en el momento de la instalación del agente Cytomic EPDR. Si posteriormente el equipo cambia de IP éste permanecerá en el grupo asignado inicialmente.

Borrar grupos

Selecciona el menú de contexto del grupo a borrar. Si el grupo contiene subgrupos o equipos asignados, la consola de administración mostrará un error.

> *No se permite borrar el nodo raíz Todos.*

Para borrar los grupos vacíos de tipo Directorio Activo que cuelgan de uno dado, haz clic en el menú de contexto del grupo y selecciona **Eliminar grupos vacíos**.

Mover grupos

- Selecciona el menú de contexto del grupo a mover.
- Haz clic en **Mover**. Se mostrará una ventana emergente con el árbol de grupos de destino.

- Selecciona el grupo de destino y pulsa **Aceptar**.

> *No se permite el movimiento del nodo raíz Todos ni de grupos Directorio Activo.*

Renombrar grupos

- Selecciona el menú de contexto del grupo a renombrar.
- Haz clic en **Cambiar nombre**.
- Introduce el nuevo nombre.

> *No es posible renombrar el grupo raíz Todos ni grupos Directorio Activo.*

Importar reglas de asignación por IPs en grupos ya creados

Para añadir direcciones IP a un grupo nativo ya creado sigue los pasos mostrados a continuación:

- Selecciona el menú de contexto de un grupo nativo que no sea el grupo Todos y haz clic en la opción **Importar reglas de asignación por IPs**. Se mostrará una ventana para poder arrastrar un fichero con las direcciones IP.
- El fichero deberá contener una o más lineas de texto con el formato mostrado a continuación:
  - Para direcciones IP independientes añadir una linea por cada una de ellas a asignar:

```
.\Grupo\Grupo\Grupo (tabulación) IP
```

  - Para rangos de IPs, añadir una linea por cada rango a asignar:

```
.\Grupo\Grupo\Grupo (tabulación) ExtremoInferiorIP-ExtremoSuperiorIP
```

  - Todos las rutas indicadas son interpretadas por Cytomic EPDR como relativas a la rama del árbol seleccionada.
  - Si los grupos indicados en el fichero no existieran, Cytomic EPDR los creará y asignará la direcciones IP indicadas.
- Haz clic en **Importar**. Las IPs se asignarán a los grupos indicados en el fichero y el árbol de grupos actualizará sus iconos para mostrar el cambio de tipo de grupo.

> *Las direcciones IP previamente asignadas a un grupo IP se borrarán al importar un fichero con nuevos pares grupo - IP.*

Una vez terminado el procedimiento, todos los equipos nuevos que se integren en Cytomic EPDR se moverán al grupo indicado según su dirección IP.

Exportar reglas de asignación por IPs

Para exportar un fichero con las reglas de grupos IP ya asignadas sigue los pasos mostrados a continuación:

- Selecciona el menú de contexto de un grupo IP, y haz clic en la opción **Exportar reglas de asignación por IPs**. Se descargará un fichero .csv con las reglas de asignación de IPs establecidas en el grupo IP y en todos sus descendientes.
- El formato del fichero .csv es el indicado en el punto "**Importar reglas de asignación por IPs en grupos ya creados**".

Mover equipos entre grupos

Para mover uno o varios equipos a un grupo, el administrador puede seguir varias estrategias:

Mover conjuntos de equipos a grupos

- Selecciona el grupo **Todos** para listar todos los equipos administrados o utiliza la herramienta de búsqueda para localizar los equipos a mover.
- Selecciona con las casillas los equipos en el panel de listado de equipos.
- Haz clic en el icono ⋮ situado a la derecha de la barra de búsqueda. Se mostrará un menú desplegable con la opción **Mover a**. Haz clic para mostrar el árbol de grupos destino.
- Selecciona el grupo destino del árbol de grupos mostrado.

Mover un único equipo a un grupo

Para asignar un único equipo a un grupo se pueden seguir varias estrategias:

- Seguir el método mostrado más arriba para asignar conjuntos de equipos a grupos, pero seleccionando un único equipo.
- Seleccionar con la casilla el equipo dentro del panel de listado de equipos que quieras asignar y haz clic en el icono de menú ⋮ situado en la parte derecha de la fila de ese equipo.
- Desde la ventana de detalles del propio equipo a mover:
  - Dentro en el panel de listado de equipos haz clic en el equipo que quieras mover para mostrar la ventana de detalles.
  - Localiza el campo **Grupo** y haz clic en el botón **Cambiar**. Se mostrará una ventana con el árbol de grupos de destino.
  - Selecciona el grupo destino y haz clic en **Aceptar**.

Mover equipos desde grupos Active Directory

Un equipo que reside en un grupo Directorio Activo puede moverse a un grupo estándar, pero nunca a otro grupo Directorio Activo.

Mover equipos hacia grupos Active Directory

No es posible mover un equipo desde un grupo nativo a un grupo Directorio Activo específico. El único movimiento que se permite es mover el equipo al grupo de tipo Directorio Activo en el que reside dentro del servidor de Directorio Activo de la empresa. Para ello haz clic en el menú de contexto del equipo y selecciona **Mover a su ruta de Active Directory**.

Restaurar la pertenencia de varios equipos a su grupo Active Directory

Para restablecer la pertenencia de equipos a su grupo Directorio Activo original haz clic en el menú de contexto de un grupo de Directorio Activo y selecciona la opción **Recuperar los equipos de esta rama de Active Directory**. Todos los equipos que pertenecen a ese grupo en el Directorio Activo de la empresa y que el administrador movió a otros grupos dentro de la consola Cytomic EPDR serán devueltos a su grupo original.

Tareas de análisis y desinfección

El árbol de grupos permite asignar tareas de análisis inmediatas o programadas a todos los equipos que pertenecen a un grupo y a sus grupos descendientes.

*Para ampliar el detalle de los tipos de análisis consulta la sección "**Opciones de análisis**" en la página **498**.*

Análisis inmediato

Haz clic en la entrada **Analizar ahora** para lanzar un análisis inmediato sobre los equipos que pertenecen al grupo o a alguno de los subgrupos. Se mostrará una ventana con el tipo de análisis a ejecutar: **Todo el ordenador** o **Áreas críticas**.

Análisis programado

Haz clic en la entrada **Programar análisis** para crear una tarea programada de análisis.

Listados disponibles para gestionar equipos

El panel Listado de equipos

El listado de equipos muestra los puestos de usuario y servidores correspondientes al grupo o filtro seleccionado en el árbol de equipos. Además, incluye herramientas de permiten gestionar uno o varios equipos simultáneamente.

Para mostrar el panel Listado de dispositivos sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Equipos**. Se mostrará el panel lateral izquierdo el árbol de equipos o de

carpetas y en el panel lateral derecho un listado con todos los equipos administrados en la red.

- Haz clic en un elemento del árbol de grupos o de filtros en el panel lateral izquierdo. El panel derecho se refrescará con el contenido del elemento seleccionado.

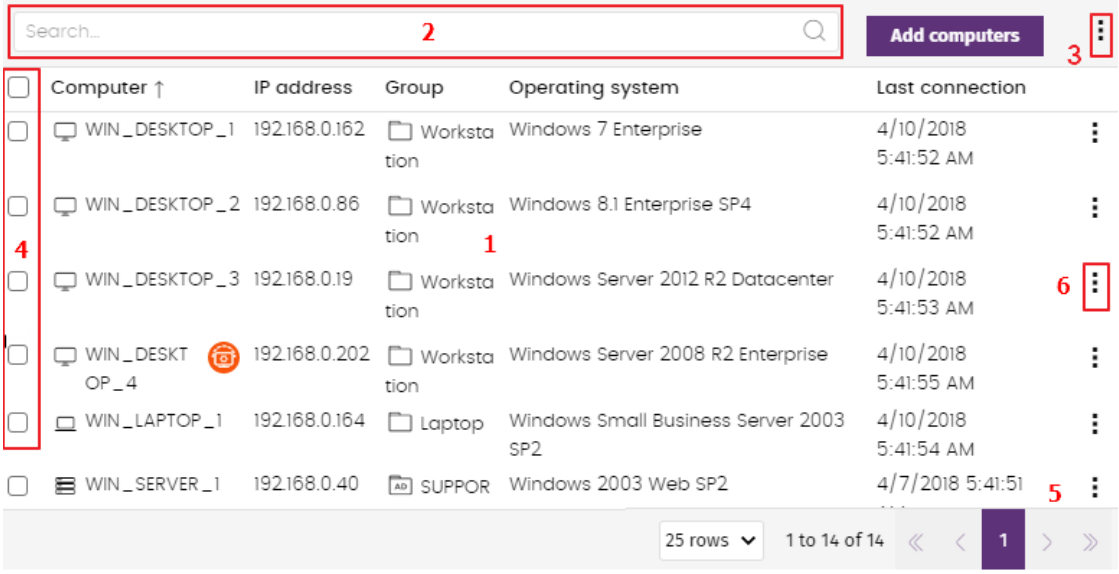


Figura 9.4: el panel Listado de equipos

A continuación, se muestra un esquema del panel listado de equipos:

- **(1)** Listado de equipos que pertenecen a la rama del árbol seleccionada.
- **(2) Herramienta de búsqueda**: localiza equipos por su nombre, descripción, dirección IP o último usuario registrado, admitiendo coincidencias parciales sin tener en cuenta mayúsculas y minúsculas.
- **(3)** Menú de contexto general: aplica una misma acción a varios equipos.
- **(4)** Casillas de selección de equipos.
- **(5)** Sistema de paginación en la parte inferior del panel.
- **(6)** Menú de contexto del equipo.

Al marcar uno o más equipos con las casillas de selección **(4)**, la herramienta de búsqueda **(2)** se oculta para mostrarse en su lugar la barra de Acciones **(7).**

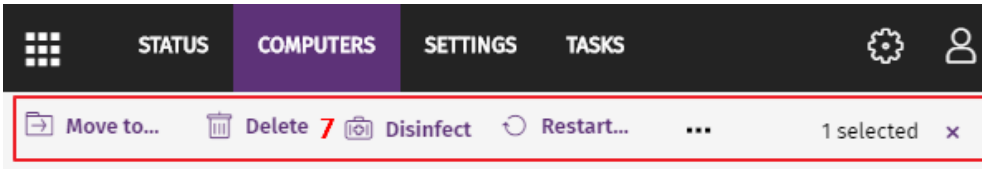


Figura 9.5: barra de acciones solapando a la herramienta de búsqueda

Al hacer clic en la casilla de selección situada a la altura de la cabecera de la tabla **(4)** se marcarán todos los equipos de la página actual del listado y se mostrará el mensaje **Seleccionar las xx** filas del listado, que permite marcar todos los equipos del listado independientemente de la paginación.

Listado de equipos

El listado de equipos es configurable para poder adaptar la información mostrada a las necesidades del administrador.

Para añadir o quitar columnas haz clic en el menú de contexto situado en la parte superior derecha y elige la opción **Añadir o eliminar columnas**. Se mostrarán las columnas disponibles y el enlace **Columnas por defecto** para restaurar la configuración del listado a sus valores iniciales.

Por cada equipo se incluye la información mostrada a continuación:

Campo	Descripción	Valores
Equipo	Nombre del equipo y su tipo.	Cadena de caracteres: • Equipo de sobremesa (puesto de trabajo, servidor Windows, Linux o macOS) • Equipo portátil Dispositivo móvil (smartphone o tablet Android)
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Ruta del directorio Activo	Ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres • Equipo en proceso de entrar en aislamiento • Equipo aislado • Equipo en proceso de salir del aislamiento
Grupo	Carpeta dentro del árbol de grupos de Cytomic EPDR a la que pertenece el equipo y su tipo.	Cadena de caracteres: • Grupo • Grupo IP

Tabla 9.3: campos del Listado de equipos

Campo	Descripción	Valores
		• Dominio AD o raíz del Directorio Activo • Unidad Organizativa • Raíz del árbol de grupos
Sistema operativo	Nombre y versión del sistema operativo instalado en el equipo.	Cadena de caracteres
Última conexión	Fecha del último envío del estado del equipo a la nube de Cytomic.	Fecha
Último usuario logueado	Nombre de las cuentas de usuario propietarias de las sesiones activas en el equipo.	Cadena de caracteres

Tabla 9.3: campos del Listado de equipos

- **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Lista separada por comas de todas las direcciones IP de las tarjetas instaladas en el equipo.	Cadena de caracteres
Direcciones físicas (MAC)	Lista separada por comas de todas las direcciones físicas de las tarjetas instaladas en el equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Directorio Activo	Ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Cytomic EPDR a la que pertenece el equipo	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres
Fecha arranque del sistema	Fecha en la que se inicio el equipo por última vez.	Fecha

Tabla 9.4: campos del fichero exportado Listado de equipos

Campo	Descripción	Valores
Fecha de instalación	Fecha en la que el Software Cytomic EPDR se instaló con éxito en el equipo.	Fecha
Fecha de última conexión	Fecha más reciente en la que el equipo contactó con la nube.	Fecha
Plataforma	Tipo de sistema operativo instalado.	• Windows • Linux • macOS • Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Máquina virtual	Indica si el equipo es físico o esta virtualizado.	Booleano
Es equipo no persistente	Indica si el sistema operativo de la máquina virtual reside en un dispositivo de almacenamiento que perdura entre reinicios o por el contrario se regenera a su estado original.	Booleano
Servidor Exchange	Versión del servidor de correo instalada en el servidor.	Cadena de caracteres
Versión de la protección	Versión interna del módulo de protección instalado en el equipo.	Cadena de caracteres
Fecha de última actualización	Fecha de la última actualización de la protección.	Fecha
Licencias	Producto licenciado en el equipo.	Cytomic EPDR
Configuración de red	Nombre de la configuración de red que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de red.	Cadena de caracteres
Seguridad para estaciones y servidores	Nombre de la configuración de seguridad que afecta al puesto de trabajo o servidor.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguridad.	Cadena de caracteres
Seguridad para dispositivos Android	Nombre de la configuración de seguridad que afecta al dispositivo móvil.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguridad.	Cadena de caracteres
Ajustes por equipo	Nombre de la configuración de ajustes que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de ajustes.	Cadena de caracteres

Tabla 9.4: campos del fichero exportado Listado de equipos

Campo	Descripción	Valores
Data Control	Nombre de la configuración de seguimiento de información personal (Cytomic Data Watch) que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguimiento de información personal.	Cadena de caracteres
Gestión de parches	Nombre de la configuración de parcheo (Cytomic Patch) que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de parcheo.	Cadena de caracteres
Cifrado	Nombre de la configuración de cifrado (Cytomic Encryption) que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de cifrado.	Cadena de caracteres
Bloqueo de programas	Nombre de la configuración de programas bloqueados por el administrador que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de bloqueo de programas.	Cadena de caracteres
Estado de aislamiento	Muestra el estado del aislamiento del equipo.	• Aislado • Aislando • Dejando de aislar • No aislado
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Último usuario logueado	Nombres de las cuentas de usuario separados por coma que mantienen una sesión interactiva abierta en equipos Windows.	Cadena de caracteres
Acción solicitada	Petición pendiente de ejecutar o en ejecución.	• Reinicio • Reinstalación de protección • Reinstalación de agente
Error en la acción solicitada	Tipo de error reportado en la acción solicitada.	• Credenciales incorrectas • Equipo descubridor no disponible

Tabla 9.4: campos del fichero exportado Listado de equipos

Campo	Descripción	Valores
		• No es posible conectar con el equipo • Sistema operativo no soportado • No es posible descargar el instalador del agente • No es posible copiar el instalador del agente • No es posible desinstalar el agente • No es posible instalar el agente • No es posible registrar el agente • Requiere intervención del usuario

Tabla 9.4: campos del fichero exportado Listado de equipos

- **Herramientas de filtrado**

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres.

Tabla 9.5: filtros disponibles en el listado Equipos

Herramientas de gestión

Utiliza las casillas de selección **(4)** de la figura 9.4 para indicar los equipos que recibirán las acciones administrativas. Al activar una casilla, se mostrará la barra de acciones con las siguientes opciones.

Acción	Descripción
Actualizar información del equipo	Fuerza el envío desde el agente instalado en el equipo de la siguiente información: • Comprobación de acciones pendientes. • Comprobación de tareas.

Tabla 9.6: herramientas para gestionar equipos

Acción	Descripción
	• Comprobación de configuraciones aplicadas. • Envío de información de estado. Este icono solo se muestra en los equipos que tienen activada la funcionalidad **Comunicación en tiempo real**. Consulta el apartado "**Configuración de la comunicación en tiempo real**" en la página **219**.
Mover a	Muestra una ventana con el árbol de grupos. Elige un grupo como destino de los equipos seleccionados. Los equipos heredarán las configuraciones asignadas al grupo de destino. Consulta el apartado "**Crear y gestionar configuraciones**" en la página **202**.
Mover a su ruta de directorio activo	Mueve los equipos seleccionados al grupo que se corresponde con la unidad organizativa del directorio activo de la empresa.
Eliminar	Borra el equipo de la consola y desinstala el software de cliente Cytomic EPDR. Consulta el apartado "**Desinstalar el software**" en la página **126**.
Analizar ahora	Consulta el apartado "**Tareas de análisis y desinfección**" en la página **163** para una introducción a las tareas de análisis o el capítulo "**Tareas**" en la página **503** para una descripción completa.
Programar análisis	Consulta el apartado "**Tareas de análisis y desinfección**" en la página **163** para una introducción a las tareas de análisis o el capítulo "**Tareas**" en la página **503** para una descripción completa.
Reiniciar	Reinicia el equipo. Consulta el apartado "**Reiniciar equipos**" en la página **499**.
Aislar equipo	Impide todas las comunicaciones del equipo excepto las necesarias para conectar con la nube de Cytomic. Consulta el apartado "**Aislar uno o varios equipos de la red de la organización**" en la página **500**.
Dejar de aislar equipo	Restaura las comunicaciones del equipo. Consulta el apartado "**Quitar el aislamiento de un equipo**" en la página **501**.
Programar instalación de parches	Consulta el capítulo "**Cytomic Patch (Actualización de programas vulnerables)**" en la página **307** para obtener información sobre cómo instalar parches en equipos Windows.
Reinstalar la protección (requiere reinicio)	Reinstala la protección en caso de mal funcionamiento. Consulta"**Reinstalación remota**" en la página **128** el apartado para obtener más información.
Seleccionados	Anula la selección actual de equipos.

Tabla 9.6: herramientas para gestionar equipos

El panel Mis listados

Haz clic en el menú superior **Estado** y en el panel lateral **Mis listados** para mostrar una ventana con todos los listados disponibles. Consulta el apartado "**Gestión de listados**" en la página **57** para obtener información sobre los tipos de listados y como operar con ellos.

Listado de hardware

Contiene los componentes hardware instalados en cada equipo del parque informático. Un mismo componente hardware se mostrará de forma independiente cada vez que sea detectado en un equipo.

Campo	Descripción	Valores
Equipo	Nombre y tipo del equipo que contiene el componente hardware.	Cadena de caracteres: • Equipo de sobremesa (puesto de trabajo, servidor Windows, Linux o macOS). • Equipo portátil. • Dispositivo móvil (smartphone o tablet Android).
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
CPU	Marca y modelo del microprocesador instalado en el equipo. Se indica el número de núcleos / cores instalados entre paréntesis.	Cadena de caracteres
Memoria	Cantidad total de memoria RAM instalada.	Cadena de caracteres
Capacidad de disco	Suma de la capacidad de todos los discos duros internos conectados al equipo.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Cytomic EPDR a la nube de Cytomic.	Fecha
Menú de contexto	Herramientas de gestión. Consulta el apartado "**Herramientas de gestión**".	

Tabla 9.7: campos del Listado de hardware

- **Campos mostrados en fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres

Tabla 9.8: campos del fichero exportado Hardware

Campo	Descripción	Valores
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Cytomic EPDR a la nube de Cytomic.	Fecha
Plataforma	Tipo de sistema operativo instalado.	• Windows • Linux • macOS • Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Sistema	Nombre del modelo hardware del equipo.	Cadena de caracteres
CPU-X	Marca, modelo y características de la CPU numerada X.	Cadena de caracteres
CPU-X Número de núcleos	Número de núcleos o cores de la CPU numerada X.	Numérico
CPU-X Número de procesadores lógicos	Número de núcleos lógicos mostrados al sistema operativo por el sistema de HyperThreading / SMT (Simultaneous MultiThreading).	Numérico
Memoria	Suma de todos los bancos de memoria RAM instalados en el equipo.	Cadena de caracteres
Disco-X Capacidad	Espacio total del medio de almacenamiento interno numerado X.	Cadena de caracteres
Disco-X Particiones	Numero de particiones reportadas al sistema operativo del medio de almacenamiento interno numerado X.	Numérico
Versión de especificación del TPM	Versiones de las APIs compatibles con el chip TPM.	Cadena de caracteres

Tabla 9.8: campos del fichero exportado Hardware

- **Herramienta de filtrado**

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Plataforma	Marca del sistema operativo.	• Windows • Android

Tabla 9.9: filtros disponibles en el Listado de hardware

Listado de software

Contiene todos los programas instalados en los equipos de la red. Por cada paquete se indica el número de equipos que lo tienen instalado e información sobre la versión y su fabricante.

Al hacer clic en un paquete software se abrirá el "**Listado de equipos**" filtrado por el paquete seleccionado, para mostrar los equipos que lo tienen instalado.

Campo	Descripción	Valores
Nombre	Nombre del paquete software encontrado en el parque.	Cadena de caracteres
Editor	Fabricante del paquete software.	Cadena de caracteres
Versión	Versión interna del paquete software.	Cadena de caracteres
Equipos	Número de equipos que contienen el paquete encontrado.	Numérico

Tabla 9.10: campos del Listado de software

- **Campos mostrados en fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Nombre	Nombre del paquete software encontrado en el parque.	Cadena de caracteres
Editor	Fabricante del paquete software.	Cadena de caracteres
Versión	Versión interna del paquete software.	Cadena de caracteres
Equipos	Número de equipos que contienen el paquete encontrado.	Numérico

Tabla 9.11: campos del Listado de software

- **Herramienta de filtrado**

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Plataforma	Marca del sistema operativo.	• Windows • Linux • macOS • Android

Tabla 9.12: filtros disponibles en el Listado de software

- **Ventana listado de equipos**

Al hacer clic en una de las filas del listado se mostrará el listado de equipos filtrado por el paquete de software seleccionado. Consulta el apartado "**Listado de equipos**" para obtener más información.

Listado Equipos con nombre duplicado

Muestra los equipos detectados en la red con el mismo nombre y que pertenecen al mismo dominio. De cada grupo de equipos duplicados Cytomic EPDR considerará correcto el equipo con la fecha de conexión a la nube de Cytomic más reciente, y el resto como erróneos. El equipo considerado correcto se excluirá del listado para que el administrador seleccione y elimine el resto de equipos de una vez.

Para eliminar los equipos duplicados selecciónalos mediante las casillas de selección y la opción **Eliminar** del menú de herramientas. Se mostrará una ventana preguntando si quieres desinstalar el agente Cytomic EPDR o no.

*Borrar equipos del listado **Equipos con nombre duplicado** sin desinstalar el agente Cytomic EPDR únicamente los borra de la consola de Cytomic EPDR. Un equipo así eliminado volverá a aparecer en la consola de Cytomic EPDR al ponerse en contacto con la nube. Ante un borrado masivo de equipos sin tener la seguridad de cuales están realmente duplicados se recomienda no desinstalar previamente el agente de ningún equipo y comprobar qué equipos reaparecen en la consola.*

Campo	Descripción	Valores
Equipo	Nombre y tipo del equipo.	Cadena de caracteres: • Equipo de sobremesa (puesto de trabajo, servidor Windows, Linux o macOS). • Equipo portátil. • Dispositivo móvil (smartphone o tablet Android).
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Cytomic EPDR a la nube de Cytomic.	Fecha

Tabla 9.13: campos del Listado de Equipos con nombre duplicado

- **Campos mostrados en fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres

Tabla 9.14: campos del fichero exportado Equipos con nombre duplicado

Campo	Descripción	Valores
Versión de la protección	Versión interna del módulo de protección instalado en el equipo.	Cadena de caracteres
Fecha de instalación	Fecha en la que el Software Cytomic EPDR se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha del último envío del estado de Cytomic EPDR a la nube de Cytomic.	Fecha
Plataforma	Tipo de sistema operativo instalado.	• Windows • Linux • macOS • Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Directorio Activo	Ruta completa del equipo en el Directorio Activo de la empresa.	Cadena de caracteres
Servidor Exchange	Versión del servidor de correo instalada en el servidor.	Cadena de caracteres
Último usuario logueado	Nombre de las cuentas de usuario propietarias de las sesiones activas en el equipo.	Cadena de caracteres
Fecha arranque del sistema	Fecha en la que se inició el equipo por última vez.	Fecha

Tabla 9.14: campos del fichero exportado Equipos con nombre duplicado

- **Herramienta de filtrado**

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Plataforma	Marca del sistema operativo.	• Todos • WindowsLinux • macOS • Android
Última conexión	Fecha del último envío del estado de Cytomic EPDR a la nube de Cytomic.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días

Tabla 9.15: filtros disponibles en el listado Equipos con nombre duplicado

Campo	Descripción	Valores
		• Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días

Tabla 9.15: filtros disponibles en el listado Equipos con nombre duplicado

- **Ventana detalle del equipo**

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta el apartado "**Información de equipo**" para obtener más información.

Información de equipo

Al seleccionar un dispositivo en el panel de listado de equipos se muestra una ventana con el detalle de la información del hardware y software instalado, así como de la configuración de seguridad asignada.

La ventana de detalle del equipo se divide en varias secciones:

Figura 9.6: vista general de la información de equipo

- **General (1)**: información que ayuda a identificar el equipo.
- **Alertas de equipo (2)**: mensajes con problemas potenciales asociados al equipo.
- **Detalles (3)**: resumen ampliado del hardware, software y seguridad configurada en el equipo.
- **Hardware (4)**: hardware instalado en el equipo, componentes y periféricos conectados, su consumo y uso.
- **Software (5)**: paquetes de software instalados en el equipo, su versión y un registro de cambios.
- **Configuración (6)**: configuraciones de seguridad y otras asignadas al equipo.
- **Barra de herramientas (7)**: agrupa las operaciones disponibles para aplicar sobre el equipo

administrado.

- **Iconos ocultos (8)**: si la ventana no es lo suficientemente grande, parte de las herramientas se ocultan agrupadas.

Sección general (1)

Contiene la siguiente información para todos los tipos de dispositivo excepto Android:

Campo	Descripción
Nombre del equipo e icono indicando el tipo de equipo	Nombre del equipo.
IP	Dirección IP del equipo.
Ruta del directorio activo	Ruta completa del equipo en el Directorio Activo de la empresa.
Grupo	Carpeta del árbol de grupos a la que pertenece el equipo.
Sistema operativo	Versión completa del sistema operativo instalado en el equipo.
Rol del equipo	Indica si el equipo hace las funciones de descubridor, caché o proxy.

Tabla 9.16: campos de la sección general de la información del equipo

Sección alertas de equipo (2)

Las alertas describen los problemas encontrados en los equipos de la red en lo que respecta al funcionamiento de Cytomic EPDR y su motivo, así como indicaciones para solucionarlos. A continuación, se muestra un resumen de los tipos de alertas generadas y las acciones recomendadas para su resolución.

Equipos aislados

Alerta	Descripción	Referencia
Equipo aislado	El administrador ha aislado el equipo y se bloquean todas las conexiones excepto aquellas necesarias para el buen funcionamiento de Cytomic EPDR.	Consulta el apartado "**Aislar un equipo**" en la página **499**.
Estamos intentando aislar este equipo	El servidor Cytomic EPDR está tratando de aislar el equipo pero la operación todavía no se ha completado por estar el equipo apagado o sin conexión a Internet.	Consulta el widget "**Equipos sin conexión**" en la página **383**.

Tabla 9.17: alertas relacionadas con la funcionalidad de aislar equipos

Alerta	Descripción	Referencia
Estamos intentando dejar de aislar este equipo	El servidor Cytomic EPDR está tratando de retirar el aislamiento del equipo pero la operación todavía no se ha completado por estar el equipo apagado o sin conexión a Internet.	Consulta el widget "**Equipos sin conexión**" en la página **383**.

Tabla 9.17: alertas relacionadas con la funcionalidad de aislar equipos

Licencias

Alerta	Descripción	Referencia
Equipo sin licencia	No hay licencias libres para asignar al equipo. Retira una licencia asignada o adquiere más licencias de Cytomic EPDR.	Consulta el apartado "**Liberar licencias**" en la página **134**.
	Hay licencias libres pero no se han asignado a este equipo.	Consulta "**Asignar licencias**" en la página **133**.

Tabla 9.18: alertas relacionadas con la asignación de licencias

Errores en el proceso de instalación del software de protección

Alerta	Descripción	Referencia
Equipo desprotegido	Se ha producido un error instalando la protección en el equipo. En el caso de errores de origen conocido se mostrará una descripción de la causa que lo motiva. Si el origen es desconocido se mostrará el código de error asociado.	Consulta el apartado "**Requisitos de instalación**" en la página **103**.
	El equipo requiere un reinicio para completar la instalación debido a una desinstalación previa.	Consulta el apartado "**Reiniciar equipos**" en la página **499**.
Error instalando Data Control	Se ha producido un error instalando Data Control en el equipo.	Consulta el apartado "**Requisitos de Cytomic Data Watch**" en la página **259**.
Error instalando la protección y Data Control	Se ha producido un error instalando la protección y el módulo en el equipo.	Consulta el apartado "**Requisitos de instalación**" en la página **103** y el apartado "**Requisitos de Cytomic Data Watch**" en la página **259**.
Error instalando el gestor de parches	Se ha producido un error instalando el módulo de gestión de parches.	Consulta el apartado "**Comprobar que Cytomic Patch funciona correctamente**" en la página **309**.

Tabla 9.19: alertas relacionadas con la instalación del software Cytomic EPDR

Alerta	Descripción	Referencia
Error instalando el módulo de cifrado	Se ha producido un error instalando el módulo de cifrado.	Consulta el aparatado "**Requisitos mínimos de Cytomic Encryption**" en la página **354**.
Error instalando el agente de Cytomic	Credenciales incorrectas.	Consulta el apartado "**Instalación remota de equipos descubiertos**" en la página **118**.
	El equipo descubridor no está disponible.	Consulta el widget "**Equipos sin conexión**" en la página **383** y el apartado "**Asignar el rol de descubridor a un equipo de la red**" en la página **110**.
	No es posible conectar con el equipo destinatario del paquete de instalación por estar apagado o no cumplir con los requisitos de hardware y de red.	Consulta el widget "**Equipos sin conexión**" en la página **383** y el apartado "**Requisitos de instalación**" en la página **103**.
	El sistema operativo del equipo no está soportado.	Consulta el apartado "**Requisitos de instalación**" en la página **103**.
	No es posible descargar el instalador del agente por un fallo de red.	Consulta el apartado "**Requisitos de red**" en la página **104**.
	No es posible copiar el instalador del agente en el equipo por falta de espacio.	Consulta el apartado "**Requisitos por plataforma**" en la página **103**.
	No es posible instalar el agente por no cumplirse los requisitos de instalación remota o el equipo está apagado.	Consulta el widget "**Equipos sin conexión**" en la página **383** y el apartado "**Requisitos de instalación**" en la página **103**.
	No es posible registrar el agente.	Consulta el widget "**Equipos sin conexión**" en la página **383** y el apartado "**Requisitos de instalación**" en la página **103**.

Tabla 9.19: alertas relacionadas con la instalación del software Cytomic EPDR

Errores en el proceso de reinstalación del software de protección

Alerta	Descripción	Referencia
Pendiente de reinstalación de la protección	El administrador solicitó la reinstalación de la protección de este equipo pero todavía no se ha realizado porque el equipo está apagado, sin conexión o porque todavía no ha terminado el plazo configurado antes de forzar el reinicio.	Consulta el widget "**Equipos sin conexión**" en la página **383** y el apartado "**Requisitos de la funcionalidad de reinstalación remota**" en la página **128**

Tabla 9.20: alertas relacionadas con la reinstalación del agente Cytomic EPDR

Alerta	Descripción	Referencia
Pendiente de reinstalación del agente	El administrador solicitó la reinstalación del agente en este equipo pero todavía no se ha realizado porque el equipo está apagado, sin conexión o porque todavía no ha terminado el plazo configurado antes de forzar el reinicio.	Consulta el widget "**Equipos sin conexión**" en la página **383** y el apartado "**Requisitos de la funcionalidad de reinstalación remota**" en la página **128**
Error instalando el agente de Cytomic	Credenciales incorrectas.	
	Equipo descubridor no disponible.	Consulta el widget "**Equipos sin conexión**" en la página **383**
	No es posible conectar con el equipo por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget "**Equipos sin conexión**" en la página **383** y el apartado "**Requisitos de la funcionalidad de reinstalación remota**" en la página **128**
	Sistema operativo no soportado por no cumplir con los requisitos de instalación remota.	Consulta el apartado "**Requisitos de la funcionalidad de reinstalación remota**" en la página **128**
	No es posible descargar el instalador del agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget "**Equipos sin conexión**" en la página **383** y el apartado "**Requisitos de la funcionalidad de reinstalación remota**" en la página **128**
	No es posible copiar el instalador del agente por no estar encendido o no cumplir los requisitos de instalación remota.	Consulta el widget "**Equipos sin conexión**" en la página **383** y el apartado "**Requisitos de la funcionalidad de reinstalación remota**" en la página **128**
	No es posible desinstalar el agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget "**Equipos sin conexión**" en la página **383** y el apartado "**Requisitos de la funcionalidad de reinstalación remota**" en la página **128**
	No es posible instalar el agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget "**Equipos sin conexión**" en la página **383** y el apartado "**Requisitos de la funcionalidad de reinstalación remota**" en la página **128**
	No es posible registrar el agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget "**Equipos sin conexión**" en la página **383** y el apartado "**Requisitos de la funcionalidad de reinstalación remota**" en la página **128**
	Requiere intervención del usuario.	

Tabla 9.20: alertas relacionadas con la reinstalación del agente Cytomic EPDR

Errores de funcionamiento del software Cytomic EPDR

Alerta	Descripción	Referencia
Equipo desprotegido	Se ha detectado un error en la protección de Exchange Server. Reinicia el equipo para solucionar el problema.	Consulta el apartado "**Reiniciar equipos**" en la página **499**.
Equipo desprotegido	Se ha detectado un error en las protecciones antivirus y avanzada. Reinicia el equipo para solucionar el problema.	Consulta el apartado "**Reiniciar equipos**" en la página **499**.
Error en Data Control	Se ha detectado un error en Data Control. Reinicia el equipo para solucionar el problema.	Consulta el apartado "**Reiniciar equipos**" en la página **499**.
Error cifrando el equipo	No se puede cifrar el equipo por un error.	Consulta el apartado "**Reiniciar equipos**" en la página **499**.

Tabla 9.21: alertas relacionadas con el mal funcionamiento del software Cytomic EPDR

Acción del usuario o del administrador pendiente

Alerta	Descripción	Referencia
Cifrado pendiente de acción del usuario	Para completar el proceso de cifrado es necesario que el usuario reinicie el equipo o introduzca las credenciales de cifrado.	Consulta el apartado "**Reiniciar equipos**" en la página **499**. Consulta el apartado "**Proceso de cifrado y descifrado**" en la página **355**.
Pendiente de reinicio	El administrador ha solicitado el reinicio de este equipo pero todavía no se ha completado por falta de conexión o por no haberse cumplido el plazo para ejecutar un inicio forzoso.	Consulta el widget "**Equipos sin conexión**" en la página **383**.
Reinstalando la protección	El administrador ha solicitado la reinstalación de la protección en este equipo y todavía no se ha completado por estar el equipo apagado, sin conexión, sin completar el plazo configurado antes del reinicio o por estar el proceso en curso.	Consulta el apartado "**Reinstalación remota**" en la página **128**.

Tabla 9.22: alertas relacionadas con la falta de acción del usuario o administrador de la red

Alerta	Descripción	Referencia
Equipo desprotegido	La protección de Exchange Server está desactivada. Activa la protección.	Consulta el apartado "**Asignación manual y automática de configuraciones**" en la página **203**, el apartado "**Crear y gestionar configuraciones**" en la página **202** y el apartado "**Antivirus para servidores Exchange**" en la página **245**.
Equipo desprotegido	Las protecciones antivirus y avanzada están desactivadas. Activa la protección.	Consulta el apartado "**Asignación manual y automática de configuraciones**" en la página **203**, el apartado "**Crear y gestionar configuraciones**" en la página **202** y los apartados "**Antivirus**" en la página **232** y "**Protección avanzada (Equipos Windows)**" en la página **229**.
Equipo sin conexión desde hace X días	Es posible que el equipo esté apagado o no se cumplan los requisitos de acceso a la red.	Consulta el apartado "**Requisitos de red**" en la página **104**.
Protección desactualizada	La protección necesita que el usuario local reinicie manualmente el equipo para completar la instalación*.	* solo reproducible en las versiones Windows Home y Starter.

Tabla 9.22: alertas relacionadas con la falta de acción del usuario o administrador de la red

Equipo desactualizado

Alerta	Descripción	Referencia
Protección desactualizada	• La protección requiere que el equipo se reinicie para terminar la actualización.	Consulta el apartado "**Reiniciar equipos**" en la página **499**.
	• Se ha producido un error intentando actualizar la protección. Comprueba que se cumplen los requisitos de hardware y de red.	Consulta el apartado "**Requisitos de instalación**" en la página **103** y el espacio disponible en disco en "**Sección Hardware (4)**".
	• Las actualizaciones están desactivadas para este equipo. Asigna un perfil de configuración con las actualizaciones activadas.	Consulta el apartado "**Actualización del motor de protección**" en la página **144**.

Tabla 9.23: alertas relacionadas con el software Cytomic EPDR desactualizado

Alerta	Descripción	Referencia
Conocimiento sobre malware y otras amenazas desactualizado	Las actualizaciones de conocimiento están desactivadas para este equipo. Asigna un perfil de configuración con las actualizaciones activadas.	Consulta el apartado "**Actualización del conocimiento**" en la página **146**.

Tabla 9.23: alertas relacionadas con el software Cytomic EPDR desactualizado

Sección general en dispositivos Android

En los dispositivos Android la sección general **(1)** y la sección de alertas de equipo **(2)** se sustituyen por el panel de antirrobo, que le permite al administrador lanzar acciones remotas sobre los dispositivos gestionados.

> *Consulta el apartado "**Antirrobo**" en la página **252** para activar la funcionalidad antirrobo en los dispositivos Android y la configuración del modo privado.*

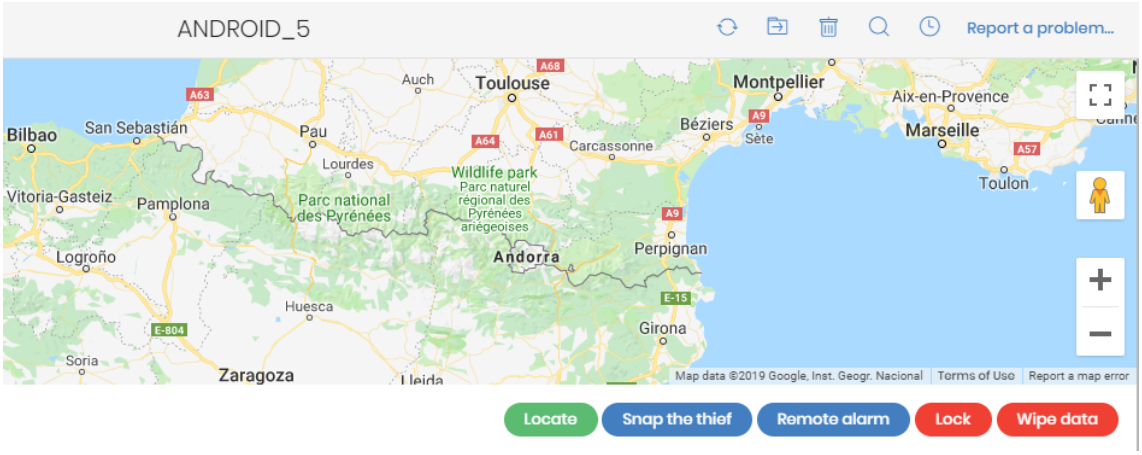


Figura 9.7: panel de antirrobo mostrado en dispositivos Android

Las acciones disponibles son:

Acción	Descripción
Localizar	• **Modo privado activado**: la consola muestra una ventana donde se solicita al administrador el número que el usuario del dispositivo tecleó al activar el modo privado. Si el número es correcto el servidor Cytomic EPDR solicita al dispositivo sus coordenadas y el mapa de la consola se actualiza con la nueva posición. • **Modo privado desactivado**: el servidor Cytomic EPDR solicita directamente al dispositivo sus coordenadas y el mapa de la consola se actualiza con la nueva posición.

Tabla 9.24: acciones soportadas por el módulo antirrobo para Android

Acción	Descripción
Foto al ladrón	Muestra una ventana donde el administrador puede introducir la dirección de correo a la que se enviará la fotografía y permite elegir el momento en el que se realizará: • **Ahora**: el agente Cytomic EPDR enviará la fotografía a la cuenta de correo indicada en el momento de recibir la petición. • **Al tocar la pantalla**: el agente Cytomic EPDR enviará la fotografía a la cuenta de correo indicada en el momento en que el usuario o el ladrón toquen la pantalla del terminal.
Alarma remota	Muestra una ventana donde el administrador podrá introducir un mensaje para el usuario y un número de contacto. Una vez enviada la petición el mensaje se mostrará en el dispositivo del usuario junto a la reproducción de un sonido al máximo volumen, aunque el dispositivo esté bloqueado. Haz clic en la casilla de selección **No reproducir ningún sonido** si unicamente quieres mostrar el mensaje.
Bloquear	La consola pide un código de 4 dígitos y acto seguido el dispositivo del usuario quedará bloqueado. Para desbloquearlo es necesario el código de 4 dígitos previamente establecido por el administrador.
Borrar datos	El dispositivo se formatea y se devuelve a su estado original, destruyendo todos los datos y aplicaciones que contenía.

Tabla 9.24: acciones soportadas por el módulo antirrobo para Android

Sección Detalles (3)

La información se divide en los siguientes apartados:

- **Equipo**: información de la configuración del dispositivo ofrecida por el agente Cytomic.
- **Seguridad**: estado de las protecciones de Cytomic EPDR.
- **Protección de datos**: estado de los módulos que protegen el contenido de los datos almacenados en el equipo.

Equipo

Campo	Descripción
Nombre	Nombre del equipo.
Descripción	Texto descriptivo asignado por el administrador.
Direcciones físicas (MAC)	Dirección física de las tarjetas de red instaladas.
Direcciones IP	Listado con todas las direcciones IP (principal y alias).
Dominio	Dominio Windows al que pertenece el equipo. Vacío si no pertenece a un dominio.
Ruta de directorio activo	Ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo.

Tabla 9.25: campos de la sección detalles del equipo

Campo	Descripción
Grupo	Grupo dentro del árbol de grupos al que pertenece el equipo. Para cambiar el grupo del equipo haz clic en el botón **Cambiar**.
Sistema operativo	Sistema operativo instalado en el equipo.
Servidor de correo	Versión del servidor Microsoft Exchange instalada en el equipo.
Máquina virtual	Indica si el equipo es físico o esta virtualizado.
Es equipo no persistente	Indica si el sistema operativo de la máquina virtual reside en un dispositivo de almacenamiento que perdura entre reinicios o por el contrario se regenera a su estado original.
Licencias	Licencias de productos de Cytomic instalados en el equipo. Consulta el capítulo "**Licencias**" en la página **131** para más información.
Versión del agente	Versión interna del agente Cytomic instalado en el equipo.
Fecha de arranque del sistema	Fecha en la que se inició el equipo por ultima vez.
Fecha de instalación	Fecha en la que se instaló el sistema operativo del equipo por última vez.
Último proxy utilizado	Método de acceso empleado por Cytomic EPDR en su ultima conexión con la nube de Cytomic. Este dato no se actualiza de forma inmediata y puede tardar hasta 1 hora en reflejar su valor correcto.
Última conexión del agente con la infraestructura Cytomic	Fecha de la última conexión del software de cliente con la nube de Cytomic. Como mínimo el agente de comunicaciones contactará cada 4 horas.
Último chequeo de la configuración	Fecha en la que Cytomic EPDR comprobó por última vez la configuración en la nube de Cytomic en busca de cambios.
Último usuario logueado	Nombre de las cuentas de usuario propietarias de las sesiones activas en el equipo.

Tabla 9.25: campos de la sección detalles del equipo

Seguridad

En esta sección se indican el estado (Activado, Desactivado, Error) de las distintas tecnologías de Cytomic EPDR que protegen al equipo del malware.

Campo	Descripción
Protección avanzada	Protección frente a amenazas avanzadas, APTs y exploits.
Antivirus de archivos	Protección del sistema de ficheros.
Antirrobo	Acciones para mitigar la exposición de datos ante robos de dispositivos móviles Android.

Tabla 9.26: campos de la sección detalles de la seguridad

Campo	Descripción
Antivirus de correo	Protección de los protocolos empleados en el envío y recepción de correos electrónicos.
Antivirus para navegación web	Protección frente al malware descargado de páginas web con el navegador instalado en el equipo.
Firewall	Protección frente a tráfico de red generado por aplicaciones.
Control de dispositivos	Protección frente a la infección mediante dispositivos externos de almacenamiento o que permiten conectar el equipo a Internet sin pasar por la infraestructura de comunicaciones de la organización (módems).
Control de acceso a páginas web	Protección frente a la navegación por páginas web no autorizadas por el administrador.
Gestión de parches	Instalación de parches y actualizaciones de sistemas operativos Windows y aplicaciones de terceros. Detección del estado de parcheo y rollback de parches problemáticos.
Bloqueo de programas	Bloqueo de la ejecución de los programas que el administrador considere peligrosos o no compatibles con la actividad desarrollada en la empresa.
Última comprobación	Fecha en la que Cytomic Patch consultó a la nube para comprobar si se publicaron nuevos parches.
Antivirus para servidores Exchange	Protección frente a virus recibidos en servidores Microsoft Exchange.
Anti-spam para servidores Exchange	Protección frente a los correos electrónicos no deseados en servidores Microsoft Exchange.
Filtrado de contenidos para servidores Exchange	Protección frente a los correos recibidos en servidores Microsoft Exchange que llevan ficheros adjuntos con extensiones peligrosas.
Versión de la protección	Versión interna del módulo de la protección instalado en el equipo.
Versión de actualización del conocimiento	Fecha de la última descarga del fichero de firmas en el equipo.

Tabla 9.26: campos de la sección detalles de la seguridad

Protección de datos

En esta sección se indica el estado de los módulos que protegen los datos almacenados en el equipo.

Campo	Descripción
Seguimiento de información personal	Monitorización de los ficheros que contienen datos susceptibles de poder identificar a usuarios o clientes de la empresa (módulo Cytomic Data Watch).

Tabla 9.27: campos de la sección Protección de datos

Campo	Descripción
Permitir búsquedas de información en este equipo	Indica si el equipo tiene asignado un perfil de configuración que le permita recibir búsquedas de ficheros y reportar sus resultados.
Inventario de información personal	Si se permiten búsquedas de ficheros por contenido, es necesario que Cytomic Data Watch examine todos los ficheros de los medios de almacenamiento soportados para recuperar su contenido y generar una base de datos.
Estado de indexación	• No indexado • Indexado • Indexado (solo el texto) • Indexado (todo el contenido) • Indexando
Estado del cifrado	Estado del módulo de cifrado: • **No disponible**: el equipo no es compatible con Cytomic Encryption. • **Sin información**: el equipo todavía no ha enviado información del módulo de cifrado. • **Activado**: el equipo tiene asignada una configuración que establece el cifrado de sus dispositivos de almacenamiento y no se han producido errores. • **Desactivado**: el equipo tiene asignada una configuración que establece el descifrado de sus dispositivos de almacenamiento y no se han producido errores. • **Error**: la configuración establecida por el administrador no permite aplicar un método de autenticación soportado por Cytomic Encryption en la versión del sistema operativo instalada en el equipo. • **Error instalando**: error en la descarga o instalación de los ejecutables necesarios para gestionar el servicio de cifrado en caso de no estar disponibles previamente en el equipo. • **Sin licencia**: el equipo no tiene una licencia de Cytomic Encryption asignada.
Estado del proceso de cifrado	• **Desconocido**: alguna unidad no tiene un estado conocido. • **Discos no cifrados**: alguna de las unidades compatibles con la tecnología de cifrado no esta cifrada ni en proceso de cifrado. • **Discos cifrados**: todas las unidades compatibles con la tecnología de cifrado están cifradas. • **Cifrando**: al menos una unidad del equipo está siendo cifrada. • **Descifrando**: al menos una unidad del equipo está siendo descifrada. • **Cifrado por el usuario**: todos los medios de almacenamiento se encuentran cifrados por el usuario. • **Cifrado por el usuario (parcialmente)**: algunos de los medios de almacenamiento se encuentran cifrados por el usuario.

Tabla 9.27: campos de la sección Protección de datos

Campo	Descripción
Método de autenticación	• **Desconocido**: método de autenticación no compatible con los soportados por Cytomic Patch. • **Procesador de seguridad (TPM).** • **Procesador de seguridad (TPM) + Contraseña.** • **Contraseña:** método de autenticación por PIN, PIN extendido o passphrase. • **USB** método de autenticación por llave USB. • **Sin cifrar**: ninguna de las unidades compatibles con la tecnología de cifrado está cifrada ni en proceso de cifrado.
Fecha de cifrado	Fecha del proceso de cifrado completado más antigua dentro de la primera vez que se cifró de forma total el equipo.

Tabla 9.27: campos de la sección Protección de datos

Sección Hardware (4)

Contiene información sobre los recursos hardware instalados en el equipo:

Campo	Descripción	Valores
CPU	Información del microprocesador instalado en el equipo y serie temporal con el consumo de CPU en diferentes periodos e intervalos según la selección del desplegable.	• Intervalos de 5 minutos para la última hora. • Intervalos de 10 minutos para las 3 últimas horas. • Intervalos de 40 minutos para las últimas 24 horas.
Memoria	Información sobre las características de los chips de memoria instalados y serie temporal con el consumo de memoria en diferentes períodos e intervalos según la selección del desplegable.	• Intervalos de 5 minutos para la última hora. • Intervalos de 10 minutos para las 3 últimas horas. • Intervalos de 40 minutos para las últimas 24 horas.
Disco	Información sobre las características del sistema de almacenamiento masivo y un gráfico de tarta con el porcentaje de espacio libre y ocupado en el momento de la consulta.	• ID de dispositivo • Tamaño • Tipo • Particiones • Revisión de firmware • Número de serie • Nombre

Tabla 9.28: campos de la sección hardware de la información del equipo

Campo	Descripción	Valores
Disco óptico	Información sobre las unidades ópticas (CD-ROM, DVD etc.).	• **Unidad**: letra asignada por el sistema operativo. • **Tipo**: características de la unidad. • **Nombre**: marca y modelo.
Placa base	Información sobre la placa madre del equipo.	• Producto • Número de serie • Fabricante
BIOS	Información sobre la versión de la BIOS instalada en el equipo.	• Versión • Fecha de fabricación • Número de serie • Nombre • Fabricante
Sistema	Información sobre el fabricante del equipo, marca, modelo y número de serie.	• **Arquitectura**: 32 o 64 bits • **Nombre**: modelo del equipo. • **Fabricante**: empresa que ensambló el equipo. • **Hostname**: nombre del equipo asignado en el sistema operativo. • **Domain**: dominio Windows al que pertenece el equipo. • **Número de serie**
Batería	Información de la batería del dispositivo.	• ID de dispositivo • Localización • Capacidad • Capacidad del multiplicador • Voltaje • Química • Nombre • Fabricante
Dispositivo de audio	Marca y fabricante de la tarjeta de sonido.	• Nombre • Fabricante
Adaptador de red	Información del fabricante, modelo y configuración IP de las tarjetas de red.	• **ID de dispositivo** • **Tipo**: protocolo de nivel 2 • **Velocidad** • **Direcciones IP**: dirección principal asignada al adaptador y alias. • **Máscaras de subred**

Tabla 9.28: campos de la sección hardware de la información del equipo

Campo	Descripción	Valores
		• **Servidores DHCP**: servidor de IPs asignado. • **Servidores DNS**: servidor de nombres asignado • **Puertas de enlace** • **Dirección MAC**: dirección física asignada al adaptador. • **Nombre** • **Fabricante**
Monitor	Información de la marca y modelo del monitor.	• **ID de dispositivo** • **Tipo** • **Fabricante**
Controladora de vídeo	Información de la marca y modelo de la tarjeta de vídeo y de los controladores asignados.	• **ID de dispositivo** • **RAM**: memoria instalada en la controladora de vídeo. • **Tipo de DAC** • **Resolución horizontal** • **Resolución vertical** • **Velocidad de refresco** • **Versión del driver** • **Nombre**: marca y modelo de la controlador de vídeo
Otro hardware	Información del hardware que no encaja en ninguna de las categorías mostradas.	• Categoría • Nombre • Fabricante
TPM	Información del chip de seguridad integrado en la placa base del equipo. Para poder ser utilizado por Cytomic EPDR el TPM debe de estar activado, habilitado y ser propietario.	• **Versión del fabricante**: versión interna del chip. • **Versión de especificación**: versiones de las APIs compatibles. • **Versión** • **Fabricante** • **Activado**: el TPM está preparado para recibir comandos. Se utiliza en sistemas con varios TPMs. • **Habilitado**: el TPM esta preparado para funcionar ya que ha sido activado desde la BIOS. • **Propietario**: el sistema operativo puede interactuar con el TPM.

Tabla 9.28: campos de la sección hardware de la información del equipo

Sección Software (5)

Contiene información del software instalado en el equipo, de las actualizaciones del sistema operativo Windows y un histórico de sus movimientos.

Herramienta de búsqueda

- Introduce el nombre o editor en la caja de texto **Buscar** y pulsa la tecla Enter para efectuar una búsqueda. A continuación se muestra la información del software encontrado:

Campo	Descripción
Nombre	Nombre del programa instalado.
Editor	Empresa que desarrolló el programa.
Fecha de instalación	Fecha en la que se instaló el programa por última vez.
Tamaño	Tamaño del programa instalado.
Versión	Versión interna del programa instalado.

Tabla 9.29: campos de la sección software de la información del equipo

- Para limitar la búsqueda selecciona en el desplegable el tipo de software que se mostrará:
  - Solo programas
  - Solo actualizaciones
  - Todo el software

Instalaciones y desinstalaciones

- Haz clic en el link **Instalaciones y desinstalaciones** para mostrar un histórico de los cambios efectuados en el equipo:

Campo	Descripción
Evento	• Software desinstalado en el equipo. • Software instalado en el equipo.
Nombre	Nombre del programa instalado.
Editor	Empresa que desarrolló el programa.
Fecha	Fecha en la que se instaló o desinstaló el programa.
Versión	Versión interna del programa instalado.

Tabla 9.30: campos de la sección Instalaciones y desinstalaciones

Sección Configuración (6)

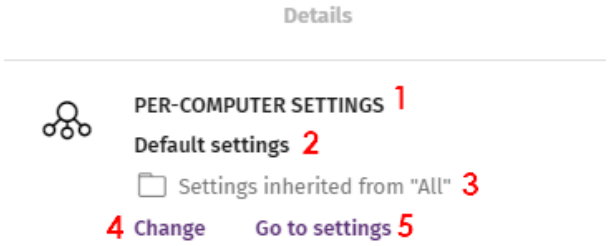


Figura 9.8: ejemplo de asignación heredada y manual

Muestra toda la información relevante de la asignación de configuraciones al equipo, y permite su gestión y modificación:

• **(1) Nombre de la categoría de la configuración**: indica el tipo de configuración. Consulta el apartado "**Introducción a las clases de configuraciones**" en la página **198** para conocer los distintos tipos de configuraciones disponibles en Cytomic EPDR.

- **(2) Nombre de la configuración asignada**.
- **(3) Método de asignación de la configuración**: directamente al equipo o heredada de un grupo superior.
- **(4) Botón para cambiar la asignación de la configuración**.
- **(5) Botón para editar el contenido de la configuración**.

> *Consulta el capítulo "**Crear y gestionar configuraciones**" en la página **202** para crear, editar y modificar perfiles de configuración.*

Barra de acciones (7)

Recurso que agrupa múltiples operaciones disponibles para aplicar sobre los equipo administrados:

Acción	Descripción
Mover a	Mueve el equipo a un grupo estándar.
Mover a su ruta de Active Directory	Mueve el equipo a su grupo Directorio Activo original.
Eliminar	Libera la licencia de Cytomic EPDR y elimina el equipo de la consola Web.
Analizar ahora	Programa una tarea de análisis de ejecución inmediata. Consulta el apartado "**Análisis y desinfección bajo demanda de equipos**" en la página **495**.
Programar análisis	Programa una tarea de análisis. Consulta el apartado "**Análisis y desinfección bajo demanda de equipos**" en la página **495**.
Aislar equipo	Impide las comunicaciones con el exterior para facilitar las tareas de análisis forense remoto al administrador, en el caso de que el equipo haya sido comprometido. Consulta el apartado "**Aislar uno o varios equipos de la red de la organización**" en la página **500**.

Tabla 9.31: acciones disponibles en la ventana de información del equipo

Acción	Descripción
Dejar de aislar equipo	Restaura las comunicaciones con el exterior. Consulta el apartado "**Quitar el aislamiento de un equipo**" en la página **501**.
Programar instalación de parches	Crea una tarea que instalará los parches publicados y no aplicados en el equipo. Consulta la sección "**Descargar e instalar los parches**" en la página **311**.
Reiniciar	Reinicia el equipo de forma inmediata. Consulta el apartado "**Reiniciar equipos**" en la página **499**.
Reinstalar la protección (requiere reinicio)	Reinstala la protección en caso de mal funcionamiento. Consulta"**Reinstalación remota**" en la página **128** el apartado para obtener más información.
Notificar un problema	Abre un ticket de mantenimiento con el departamento técnico de Cytomic. Consulta el apartado "**Notificar un problema**" en la página **502**.

Tabla 9.31: acciones disponibles en la ventana de información del equipo

Iconos ocultos (8)

Dependiendo del tamaño de la ventana y del número de iconos a mostrar, parte de ellos pueden quedar ocultos bajo el icono ▪▪▪. Haz clic para desplegar el menú con los iconos restantes.

Capítulo 10

Gestión de configuraciones

Las configuraciones, también llamados "perfiles de configuración" o simplemente "perfiles", ofrecen a los administradores un modo rápido de establecer los parámetros de seguridad, productividad y conectividad gestionados por Cytomic EPDR en los equipos que administran.

CONTENIDO DEL CAPÍTULO

Estrategias para crear la estructura de configuraciones

El administrador de la red creará tantos perfiles como variaciones de configuraciones sean necesarias para gestionar la seguridad de la red. Se genera una nueva configuración por cada grupo de equipos con necesidades de protección similares:

- Equipos de usuario utilizados por personas con distintos niveles de conocimientos en informática requieren configuraciones más o menos estrictas frente a la ejecución de software, acceso a Internet o a dispositivos externos.
- Usuarios que desempeñan diferentes tareas tienen diferentes usos y necesidades, y por tanto requerirán de configuraciones que permitan el acceso a diferentes recursos.
- Usuarios que manejan información confidencial o delicada para la empresa requieren un nivel de protección superior frente a amenazas e intentos de robo de la propiedad intelectual de la compañía.
- Equipos en distintas delegaciones requieren configuraciones distintas que les permitan conectarse a Internet utilizando diferentes infraestructuras de comunicaciones.
- Servidores críticos para el funcionamiento de la empresa requieren configuraciones de seguridad específicas.

Visión general para asignar configuraciones a equipos

La asignación de configuraciones a los equipos de la red es un proceso de cuatro pasos:

1. Crear los grupos que reúnan equipos del mismo tipo o con idénticos requisitos de conectividad y seguridad.
2. Asignar los equipos de la red a su grupo correspondiente.
3. Asignar los distintos tipos de configuraciones a los grupos creados.
4. Difundir las configuraciones a todos los equipos de la red.

Todas estas operaciones se realizan desde el árbol de grupos, accesible desde el menú superior **Equipos**. El árbol de grupos es la herramienta principal para asignar configuraciones de forma rápida y sobre conjuntos amplios de equipos.

Por lo tanto, la estrategia principal del administrador consiste en reunir todos los equipos similares en un mismo grupo y crear tantos grupos como conjuntos diferentes de equipos existan en la red que gestiona.

*Para obtener más información sobre el manejo del árbol de grupos y asignación de equipos a grupos consulta el apartado "***El panel Árbol de equipos***" en la página* **151**.

Difusión inmediata de la configuración

Una vez que una configuración es asignada a un grupo, esa configuración se aplicará a los equipos del grupo de forma inmediata y automática, siguiendo las reglas de la herencia mostradas en el apartado "**Asignación indirecta de configuraciones: las dos reglas de la herencia**". La configuración así establecida se aplica a los equipos sin retardos, en cuestión de unos pocos segundos.

*Para desactivar la difusión inmediata de la configuración consulta el apartado "***Configuración de la comunicación en tiempo real***" en la página* **219**.

Árbol multinivel

En empresas de tamaño mediano y grande, la variedad de configuraciones puede ser muy alta. Para facilitar la gestión de parques informáticos grandes, Cytomic EPDR permite generar árboles de grupos de varios niveles para que el administrador pueda gestionar los equipos de la red con la suficiente flexibilidad.

Herencia

En redes de tamaño amplio es muy probable que el administrador quiera reutilizar configuraciones ya establecidas en grupos de orden superior dentro del árbol de grupos. El mecanismo de herencia permite asignar una configuración sobre un grupo y, de forma automática, sobre todos los grupos que dependen de éste, ahorrando tiempo de gestión.

Configuraciones manuales

Para evitar la propagación de configuraciones en todos los niveles inferiores de una rama del árbol, o asignar una configuración distinta a la recibida mediante la herencia sobre un determinado equipo dentro de una rama, es posible asignar de forma manual configuraciones a equipos individuales o a grupos.

Configuración por defecto

Inicialmente todos los equipos en el árbol de grupos heredan la configuración establecida en el nodo raíz **Todos**. Este nodo tiene asignadas las configuraciones por defecto creadas en Cytomic EPDR para proteger a los equipos desde el primer momento, incluso antes de que el administrador haya accedido a la consola para establecer una configuración de seguridad.

Introducción a las clases de configuraciones

Cytomic EPDR distribuye la configuración a aplicar en los equipos administrados a lo largo de varias clases de perfiles, cada una de las cuales cubre un área concreta de la seguridad.

A continuación se muestra una introducción a cada una de las clases soportadas en Cytomic EPDR:

- Configuración de red
- Ajustes por equipo
- Estaciones y servidores
- Bloqueo de programas
- Dispositivos Android
- Gestión de parches
- Data Control
- Cifrado

Configuración de red

Define el idioma del agente instalado en el equipo de usuario y establece los parámetros necesarios para poder conectar con Internet. Consulta el capítulo "**Configuración remota del agente**" en la página **211**.

Ajustes por equipo

Define varios parámetros del agente Cytomic:

- Intervalo de actualizaciones del software Cytomic EPDR en los equipos.
- Contraseña de instalación en los equipos de usuario.
- Protección anti-tamper.

*Consulta el capítulo "**Actualización del software cliente**" en la página **143** para obtener más información.*

Estaciones y servidores

Define la configuración de seguridad de los equipos de la red Windows, macOS y Linux, tanto de los puestos de trabajo como servidores.

*Consulta el capítulo "**Configuración de estaciones y servidores**" en la página **225**.*

Bloqueo de programas

Define la configuración de bloqueo de programas establecida por el administrador para equipos Windows.

*Consulta el capítulo "**Configuración del bloqueo de programas**" en la página **373**.*

Dispositivos Android

Define la configuración de seguridad y antirrobo de dispositivos Android (tablets y smartphones).

*Consulta el capítulo "**Configuración del bloqueo de programas**" en la página **373**.*

Gestión de parches

Define la configuración que permitirá descubrir los parches que publican los proveedores de las aplicaciones instaladas en la red de la empresa.

*Consulta el capítulo "**Cytomic Patch (Actualización de programas vulnerables)**" en la página **307**.*

Data Control

Define el comportamiento del servicio Cytomic Data Watch para detectar y hacer un seguimiento de la información personal (PII) en ficheros de datos no estructurados.

*Consulta el capítulo "**Cytomic Data Watch (Supervisión de información sensible)**" en la página **255**.*

Cifrado

Establece el estado y los parámetros de cifrado de los volúmenes de almacenamiento masivo conectados al equipo.

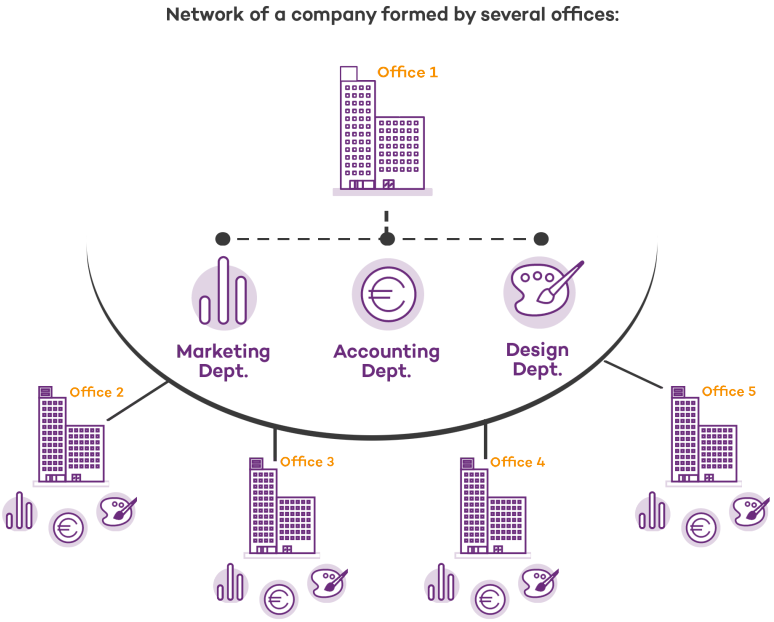
*Consulta el capítulo "**Cytomic Encryption (Cifrado de dispositivos)**" en la página **349**.*

Perfiles de configuración modulares vs monolíticos

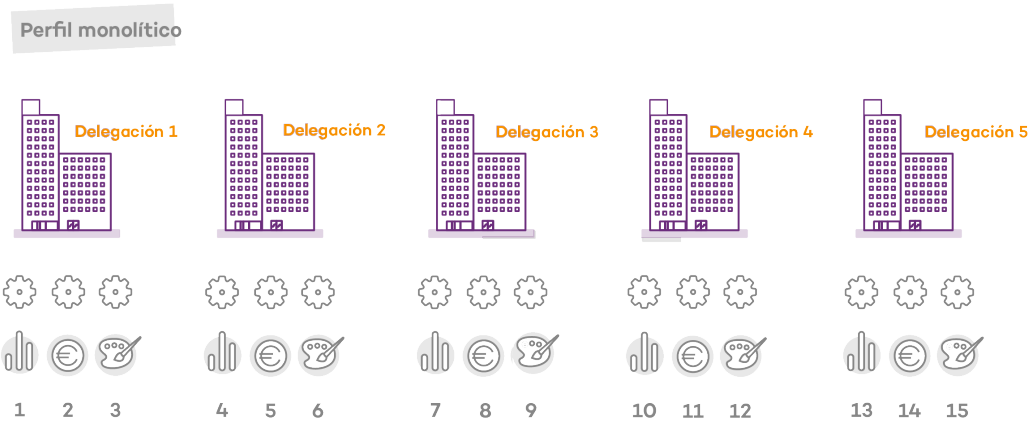
Con el soporte de las distintas clases de perfiles, Cytomic EPDR adopta un enfoque modular para crear y distribuir las configuraciones a aplicar en los equipos administrados. El objetivo de utilizar perfiles modulares y no un único perfil de configuración monolítico que abarque toda la configuración es el de reducir el número de perfiles distintos que el administrador tendría que manejar en la consola y así minimizar el tiempo de gestión. El enfoque modular permite generar configuraciones más pequeñas y ligeras, frente a perfiles monolíticos que fomentan la aparición de muchos perfiles de configuración muy largos y redundantes, con muy pocas diferencias entre sí.

Caso práctico: Creación de configuraciones para varias delegaciones

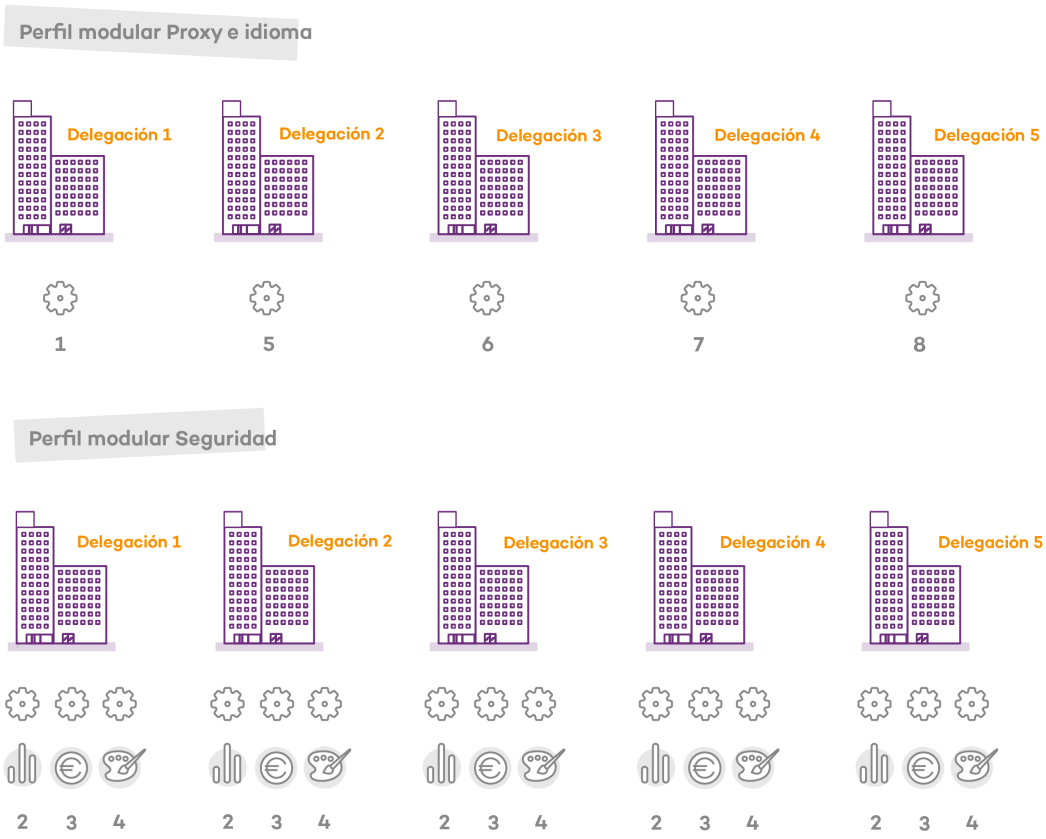
En este caso práctico tenemos una empresa con 5 delegaciones, cada una de ellas tiene una infraestructura de comunicaciones distinta y por tanto una configuración de proxy diferente. Además, dentro de cada delegación se requieren 3 configuraciones de seguridad diferentes, una para el departamento de diseño, otro para el departamento de contabilidad y otra para el departamento de marketing.



Con un perfil monolítico son necesarios 15 perfiles de configuración distintos (5 oficinas x 3 clases de configuración en cada oficina = 15) para dar servicio a todos los departamentos de todas las delegaciones de la empresa.



Como Cytomic EPDR separa la configuración de proxy de la de seguridad, el número de perfiles a crear se reduce (5 perfiles de proxy + 3 perfiles de departamento = 8) ya que los perfiles de seguridad por departamento de una delegación se pueden reutilizar y combinar con los perfiles de proxy en otras delegaciones.



Crear y gestionar configuraciones

Haz clic en el menú superior **Configuración** para crear, copiar y borrar configuraciones. En el panel de la izquierda se encuentran las entradas correspondientes a las clases de configuraciones posibles **(1)**. En el panel de la derecha se muestran los perfiles de configuración ya creados **(2)** de la clase seleccionada y los botones para añadir **(3)**, copiar **(4)** y eliminar perfiles **(5).** Utiliza la barra de búsqueda **(6)** para localizar los perfiles ya creados de forma rápida.

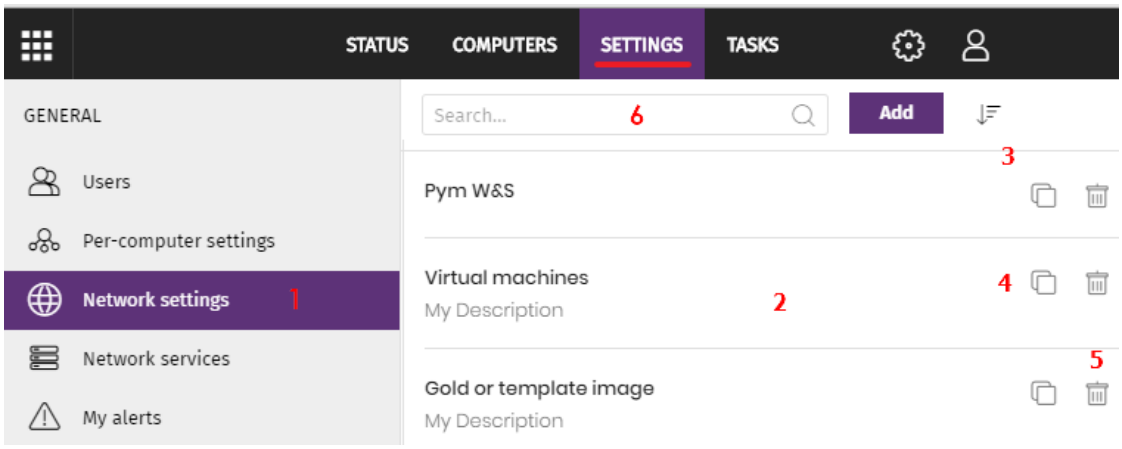


Figura 10.1: pantalla para crear y gestionar configuraciones

Crear configuraciones

Haz clic sobre el botón **Añadir** para mostrar la ventana de creación de configuraciones. Todos los perfiles tienen un nombre principal y una descripción que se muestran en los listados de configuraciones.

Ordenar configuraciones

Haz clic en el icono **(7)** para desplegar un menú de contexto con las opciones de ordenación disponibles:

- Ordenado por fecha de creación
- Ordenado por nombre
- Ascendente
- Descendente

Copiar, borrar y editar configuraciones

- Para copiar y borrar un perfil de configuración utiliza los iconos **(4)** y **(5)**. Si el perfil ha sido asignado a uno o más equipos se impedirá su borrado hasta que sea liberado.

- Haz clic en el perfil de configuración para editarlo.

Antes de modificar un perfil comprueba que la nueva configuración sea correcta ya que, si el perfil ya está asignado a equipos de la red, esta nueva configuración se propagará y aplicará de forma automática y sin retardos.

Asignación manual y automática de configuraciones

Una vez creados los perfiles de configuración, éstos pueden ser asignados a los equipos de la red siguiendo dos estrategias diferentes:

- Mediante asignación manual (asignación directa).
- Mediante asignación automática a través de la herencia (asignación indirecta).

Ambas estrategias son complementarias y es muy recomendable que el administrador comprenda las ventajas y limitaciones de cada mecanismo para poder definir una estructura de equipos lo más simple y flexible posible, con el objetivo de minimizar las tareas de mantenimiento diarias.

Asignación directa / manual de configuraciones

Consiste en establecer de forma directa los perfiles de configuración a equipos o grupos. De esta manera es el administrador el que, de forma manual, asigna una configuración a un grupo o equipo.

Una vez creados los perfiles de configuración, estos se asignan de tres maneras posibles:

- Desde el menú superior **Equipos**, en el árbol de grupos mostrado en el panel de la izquierda.
- Desde el detalle del equipo en el panel de listado de equipos, accesible desde el menú superior **Equipos**.
- Desde el propio perfil de configuración creado o editado.

*Para obtener más información sobre el árbol de grupos consulta el apartado "***Árbol de grupos***" en la página* **158**.

Desde el árbol de grupos

Para asignar un perfil de configuración a un conjunto de equipos que pertenecen a un grupo:

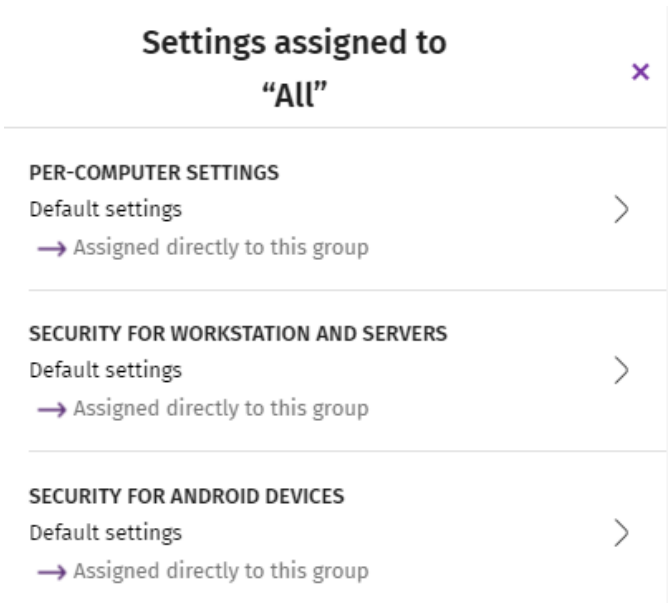


Figura 10.2: ejemplo de asignación heredada y manual

• Haz clic en el menú superior **Equipos** y selecciona el árbol de grupos en el panel izquierdo.

• Haz clic en el menú contextual en la rama apropiada del árbol de grupos.

• Haz clic en el menú emergente **Configuraciones**, se mostrará una ventana con el nombre de los perfiles ya asignados al grupo seleccionado, separados por su clase, y el tipo de asignación:

• **Manual / Asignación directa**: mediante la leyenda **Asignada directamente a este grupo**.

• **Heredada / Asignación indirecta**: mediante la leyenda **Configuración heredada de** y el nombre del grupo del cual se hereda la configuración, junto con la ruta completa para llegar al mismo.

• Haz clic en una de las clases disponibles, selecciona la nueva configuración y haz clic en **Aceptar** para asignar la configuración al grupo. La configuración se propagará de forma inmediata a todos los equipos miembros del grupo y sus descendientes.

Desde el panel listado de equipos

Para asignar un perfil de configuración a un equipo concreto:

• En el menú superior **Equipos** haz clic en el grupo o filtro donde reside el equipo a asignar la configuración. Haz clic sobre el equipo en la lista de equipos mostrada en el panel derecho para ver la pantalla detalles de equipo.

• Haz clic en la pestaña **Configuración**. Se mostrarán los perfiles asignados al equipo separados por su clase, y el tipo de asignación:

  • **Manual / Asignación directa**: mediante la leyenda **Asignada directamente a este grupo**.

  • **Heredada / Asignación indirecta**: mediante la leyenda **Configuración heredada de** y el nombre del grupo del cual se hereda la configuración, junto con la ruta completa para llegar al mismo.

• Haz clic en una de las clases disponibles, selecciona la nueva configuración y haz clic en **Aceptar** para asignar la configuración al equipo. La configuración se aplicará de forma inmediata.

Desde el propio perfil de configuración

La forma más rápida de asignar una configuración a varios equipos que pertenecen a grupos distintos es a través del propio perfil de configuración.

Para asignar equipos o grupos de equipos a un perfil de configuración:

- En el menú superior **Configuración**, panel lateral, haz clic en la clase de perfil que quieres asignar.
- Selecciona la configuración a asignar y haz clic en el botón **Destinatarios**. Se mostrará una ventana dividida en dos secciones: **Grupos de equipos y Equipos adicionales**.
- Haz clic en los botones ⊕ para añadir equipos individuales o grupos de equipos al perfil de configuración.
- Haz clic en el botón **Atrás**. El perfil quedará asignado a los equipos seleccionados y la nueva configuración se aplicará de forma inmediata.

> *Al retirar un equipo de la lista de equipos asignados a una configuración, el equipo volverá a heredar las configuraciones asignadas al grupo al que pertenece. La consola de administración resaltará este hecho mostrando una ventana de advertencia antes de aplicar los cambios.*

Asignación indirecta de configuraciones: las dos reglas de la herencia

La asignación indirecta de configuraciones se realiza a través del mecanismo de la herencia. Esta funcionalidad permite propagar de forma automática un mismo perfil de configuración a todos los equipos subordinados del nodo sobre el cual se asignó la configuración.

Las reglas que rigen la interacción entre los dos tipos de asignaciones (manuales / directas y automática / herencia) se muestran por orden de prioridad:

- **Regla de la herencia automática**

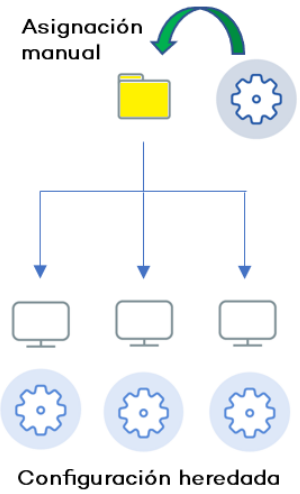


Figura 10.3: herencia / asignación indirecta

Un grupo o equipo hereda de forma automática las configuraciones del grupo del cual depende (grupo padre o de orden superior).

La asignación de configuración es manual sobre el grupo padre y todos sus descendientes (equipos y otros grupos con equipos en su interior) reciben la configuración de forma automática.

- **Regla de la prioridad manual**

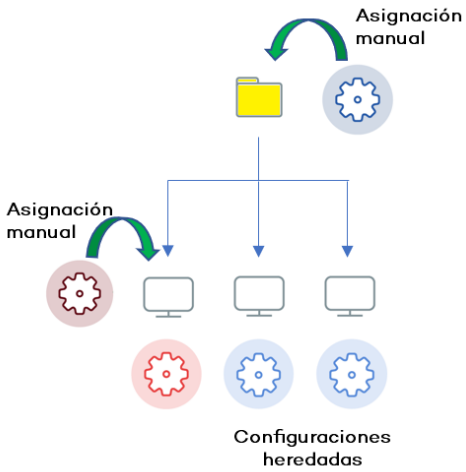


Figura 10.4: prevalencia de configuración manual sobre heredada

Una configuración manual prevalece sobre una configuración heredada.

Los equipos reciben las configuraciones heredadas por defecto pero si se establece una configuración manual sobre un grupo o equipo, todos sus descendientes recibirán la configuración manual, y no la configuración heredada de orden superior.

Límites de la herencia

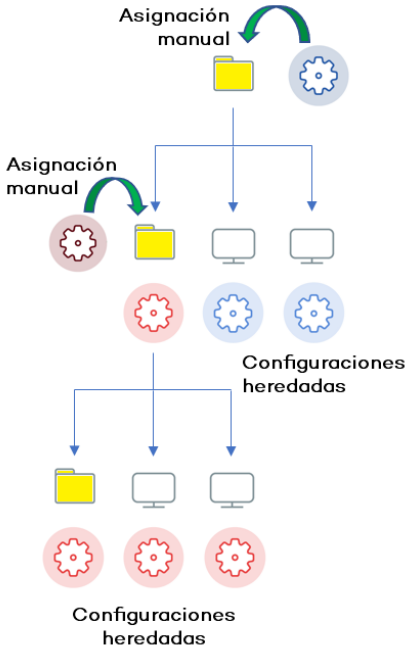


Figura 10.5: Limite de la herencia

La configuración asignada a un grupo (manual o heredada) se propaga a todos los elementos de la rama del árbol hasta que se encuentra una asignación manual.

Este nodo y todos sus descendientes reciben la configuración manual asignada, y no la establecida en el nodo de orden superior.

Sobre-escritura de configuraciones

La regla de la prioridad manual indica que las configuraciones manuales prevalecen sobre las configuraciones heredadas en un escenario típico donde primero se establece la configuración sobre el nodo de orden superior para que todos sus descendientes la hereden, y posteriormente se asignan de forma manual aquellas configuraciones especiales sobre ciertos nodos de orden inferior.

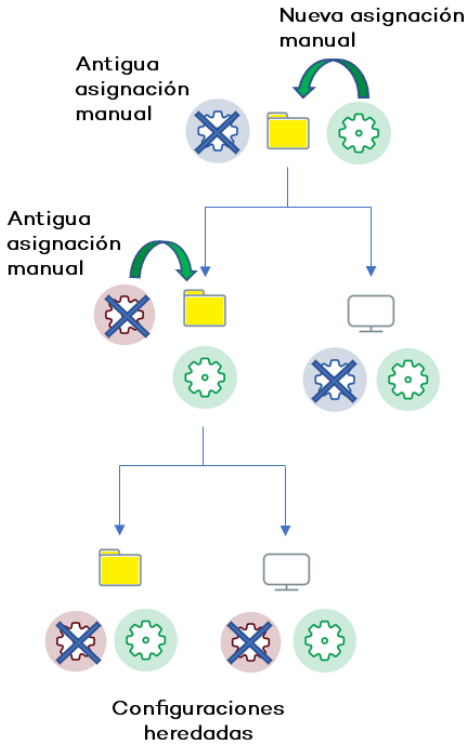


Figura 10.6: Sobre escritura de configuraciones manuales

Sin embargo, es frecuente que una vez establecidas las configuraciones heredadas y manuales, haya un cambio de configuración en un nodo de orden superior. Se distinguen dos casos:

- **No hay configuraciones manuales en los nodos descendientes**: el nodo padre recibe una nueva configuración que se propaga a todos sus nodos descendientes.
- **Sí hay configuraciones manuales en algún nodo descendiente**: el nodo padre recibe una configuración que intenta propagar a todos los nodos descendientes, pero el sistema de herencia no permite asignar una configuración de forma automática sobre un nodo que recibió anteriormente una configuración manual.

De esta manera, cuando el sistema detecta un cambio de configuración que tenga que propagar a los nodos subordinados, y alguno de estos tenga una configuración manual (sin importar el nivel en el que se encuentre) se presentará la pantalla de selección, preguntando al administrador sobre el comportamiento a seguir: **Hacer que todos hereden esta configuración** o **Mantener todas las configuraciones**.

Hacer que todos hereden esta configuración

> ⚠ *¡Utiliza esta opción con mucho cuidado, esta acción no tiene vuelta atrás! Todas las configuraciones manuales que dependan del nodo padre se perderán y se aplicará la configuración heredada de forma inmediata en los equipos. El comportamiento de Cytomic EPDR podrá cambiar en muchos equipos de la red.*

La nueva asignación directa se propaga mediante la herencia a todo el árbol por completo, sobrescribiendo la asignación directa anterior y llegando hasta los nodos hijos de último nivel.

Mantener todas las configuraciones

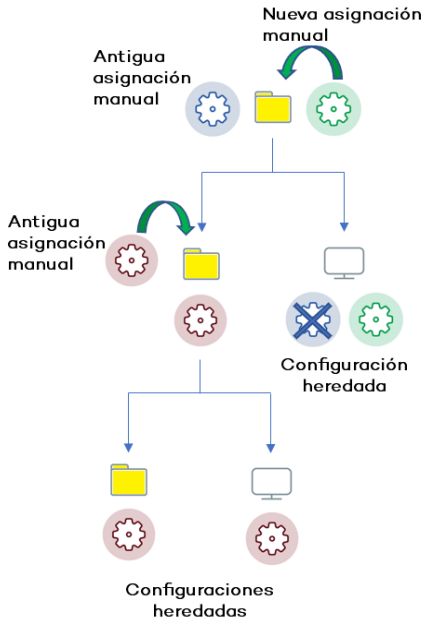


Figura 10.7: Mantener las configuraciones manuales

La nueva configuración solo se propaga a aquellos nodos subordinados que no tengan configuraciones manuales establecidas.

Si eliges la opción de mantener las configuraciones establecidas de forma manual, la propagación de la nueva configuración heredada se detiene en el primer nodo configurado manualmente. Aunque los nodos subordinados a un nodo configurado de forma manual heredan su configuración, la propagación la configuración se detiene en el primer nodo subordinado del árbol que tiene asignada una configuración manual.

- **Eliminar asignaciones manuales y restaurar la herencia**

Para eliminar una asignación manual aplicada sobre una carpeta y volver a heredar la configuración de la rama padre:

- En el menú superior **Equipos** haz clic en el grupo que tiene la asignación manual a eliminar, dentro del árbol de grupos situados en el panel izquierdo.
- Haz clic en el icono del menú contextual de la rama apropiada. Se mostrará una ventana emergente con las configuraciones asignadas. Elige el perfil que esté asignado de forma manual y quieres eliminar.
- Se desplegará un listado con todos los perfiles disponibles para realizar una nueva asignación manual, y al final de la lista se mostrará el botón **Heredar del grupo padre** junto con información de la configuración que se heredaría, y el grupo del cual se heredará.

Movimiento de grupos y equipos

Al mover un equipo o grupo de equipos a otra rama del árbol con una configuración aplicada, el comportamiento de Cytomic EPDR con respecto a las configuraciones que tomará el equipo o grupo movido varia en función de si se trata de grupos completos o equipos individuales.

Movimiento de equipos individuales

Se respetan las configuraciones manuales establecidas sobre los equipos movidos, y se sobrescriben de forma automática las configuraciones heredadas con las configuraciones establecidas en el nuevo grupo padre.

Movimiento de grupos

Se muestra una ventana con la pregunta **¿Quieres que las configuraciones asignadas a este grupo mediante herencia, sean sustituidas por las del nuevo grupo padre?**

- En el caso de contestar **SI** el procedimiento será el mismo que en el movimiento de equipos: las configuraciones manuales se respetan y las heredadas se sobrescriben con las configuraciones establecidas en el grupo padre.
- En el caso de contestar **NO**, las configuraciones manuales se respetan pero las configuraciones heredadas originales del grupo movido prevalece, pasando de esta forma a ser configuraciones manuales.

Visualizar las configuraciones asignadas

La consola de administración implementa hasta cuatro formas de mostrar los perfiles de configuración asignados a un grupo o equipo:

- En el árbol de grupos.
- En la pantalla de definición de la configuración.
- En la pestaña **Configuración** del equipo.
- En el listado de equipos exportado.

Mostrar las configuraciones en el árbol de grupos

- Haz clic en el menú superior **Equipos** y en la pestaña situada en la parte superior del panel lateral para mostrar el árbol de grupos.
- Selecciona el menú de contexto de la rama elegida y haz clic en el menú emergente **Configuraciones** para mostrar una ventana con las configuraciones asignadas a la carpeta.

A continuación, se indica la información mostrada en cada entrada:

- **Tipo de configuración**: indica la clase a la que pertenece la configuración mostrada.
- **Nombre de la configuración**: nombre asignado por el administrador en la creación de la configuración.
- **Tipo de herencia aplicada**:
  - **Configuración heredada de…:** la configuración fue asignada a la carpeta padre indicada, y los equipos que pertenecen a la rama actual la heredan.
  - **Asignada directamente a este grupo**: → la configuración de los equipos es la que el administrador asigno de forma manual a la carpeta.

Mostrar las configuraciones en la definición de la configuración

- Haz clic en el menú superior **Configuraciones** y selecciona el tipo de configuración en el menú lateral.
- Selecciona una configuración en el listado de configuraciones.
- Si la configuración esta asignada a uno o más equipos o grupos, se mostrará el botón **Ver equipos**.

- Haz clic en el botón **Ver equipos**. Se mostrará la zona **Equipos** con un único listado formado por todos los equipos que tienen la configuración asignada, tanto si se asignó de forma individual o mediante grupos de equipos. En la parte superior de la ventana se mostrará el criterio de filtrado establecido.

Mostrar las configuraciones en la pestaña configuración del equipo

En el menú superior **Equipos**, selecciona un equipo del panel de la derecha para mostrar la ventana de detalle. En la pestaña **Configuración** se listan los perfiles asignados al equipo.

Mostrar las configuraciones en el listado de equipos exportado

Desde el árbol de equipos (árbol de grupos o árbol de filtros) haz clic en el menú contextual y elige la opción **Exportar**.

*Consulta el apartado "**Campos mostrados en el fichero exportado**" en la página **166**.*

Capítulo 11

Configuración remota del agente

El administrador puede cambiar desde la consola web el funcionamiento de varios aspectos del agente Cytomic instalado en los equipos de la red:

- El papel o rol que el equipo representa para el resto de puestos y servidores protegidos.
- Las protecciones frente al tampering o manipulación indebida del software cliente Cytomic EPDR por parte de amenazas avanzadas y APTs.
- La visibilidad del agente en el equipo de usuario o servidor y su idioma.
- Configuración de las comunicaciones de los equipos con la nube de Cytomic.

CONTENIDO DEL CAPÍTULO

Configuración de los roles del agente Cytomic

El agente Cytomic instalado en los equipos Windows de la red puede adoptar tres roles diferentes:

- Proxy
- Descubridor
- Caché

Para asignar un rol a un equipo con el agente Cytomic ya instalado haz clic en el menú superior **Configuración** y en el panel lateral **Servicios de red**. Se mostrarán tres pestañas: **Cytomic Proxy**, **Caché** y **Descubrimiento**.

> ⚠ *Solo los equipos con sistema operativo Windows instalado pueden adquirir el rol de Proxy, Descubridor o Caché.*

Rol de Proxy

Para los equipos que no tienen acceso directo a Internet, Cytomic EPDR permite la utilización del proxy instalado en la red de la organización. En el caso de no existir ningún proxy disponible, puedes asignar el rol de proxy a un equipo con Cytomic EPDR instalado.

> ⚠ *No se permite la descarga de parches y actualizaciones del módulo Cytomic Patch a través de un equipo con el rol de proxy asignado. Los equipos que descarguen parches deberán de tener acceso a la nube de Cytomic directamente o a través de un proxy corporativo.*

Requisitos para asignar el rol de proxy a un equipo

- Cytomic EPDR instalado en un equipo con sistema operativo Windows.
- Soporte para el formato de ficheros 8+3. Consulta el artículo de la MSDN **https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778996(v=ws.10)?redirectedfrom=MSDN** para habilitar esta funcionalidad.

Asignar el rol de proxy a un equipo

En las máquinas designadas como Proxy Cytomic EPDR, los puertos UDP 21226 y TCP 3128 no podrán ser utilizados por otras aplicaciones. Además, la configuración del cortafuegos del equipo deberá permitir el tráfico entrante y saliente por ambos puertos.

- Haz clic en el menú superior **Configuración,** panel lateral **Servicios de red** y en la pestaña **Proxy**. Se mostrarán todos los equipos con el rol de proxy ya asignado.
- Haz clic en el botón **Añadir servidor proxy**. Se mostrará una ventana con todos los equipos administrados por Cytomic EPDR que cumplen los requisitos para ejercer de proxy en la red.
- Utiliza la caja de búsqueda para localizar el equipo y haz clic sobre el mismo para agregarlo al listado de equipos con el rol de proxy asignado.

Retirar el rol de proxy a un equipo

- Haz clic en el menú superior **Configuración,** panel lateral **Servicios de red** y en la pestaña **Proxy**. Se mostrarán todos los equipos con el rol de proxy ya asignado.
- Haz clic en el icono  del equipo que quieres retirar el rol de proxy.

Para configurar el uso de un equipo con el rol de proxy asignado consulta el apartado "**Configuración de listas de acceso a través de proxy**".

Rol de Caché / repositorio

Cytomic EPDR permite asignar el rol de caché a uno o más puestos de la red. Estos equipos descargan y almacenan de forma automática todos los ficheros que necesitan otros puestos con Cytomic EPDR instalado. Esto produce un ahorro de ancho de banda, ya que cada equipo no descargará de forma independiente las actualizaciones, sino que se hará una única vez de forma centralizada.

Elementos cacheados

Un equipo con el rol de cache asignado puede cachear los elementos siguientes durante un periodo de tiempo variable dependiendo de su tipo:

- **Archivo de identificadores**: hasta que dejan de ser válidos.
- **Paquetes de instalación**: hasta que dejan de ser válidos.
- **Parches de actualización para** Cytomic Patch: 30 días.

Dimensionamiento de un nodo caché

El dimensionamiento de un equipo con el rol de caché asignado depende completamente del número de conexiones simultáneas en los picos de carga y del tipo de tráfico que gestione

(descargas de ficheros de firmas, instaladores etc.). Como aproximación un equipo con el rol de caché asignado puede servir en torno a 1000 equipos de forma simultánea.

Asignar el rol de caché a un equipo

- En el menú superior **Configuración**, panel lateral **Servicios de red** haz clic en la pestaña superior **Caché**.
- Haz clic en el botón **Añadir equipo caché**.
- Utiliza la herramienta de búsqueda situada en la parte superior de la ventana para localizar equipos candidatos a asignar el rol de caché.
- Selecciona un equipo de la lista y pulsa **Aceptar**.

A partir de ese momento el equipo seleccionado adoptará el rol de caché y comenzará la descarga de todos los archivos necesarios, manteniendo sincronizado su repositorio de forma automática. El resto de los puestos de la subred contactarán con el caché para la descarga de actualizaciones.

Retirar el rol de caché a un equipo

- Haz clic en el menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Caché.**
- Haz clic en el icono del equipo que quieres retirar el rol caché.

Establecer la unidad de almacenamiento

Es posible configurar el agente Cytomic EPDR para almacenar los elementos a cachear en un volumen / unidad concreta del equipo, aunque la ruta de la carpeta dentro del volumen es fija. Para configurar esta característica sigue los pasos mostrados a continuación:

- En el menú superior **Configuración**, panel lateral **Servicios de red** haz clic en la pestaña superior **Caché**.
- En un equipo con el rol de caché asignado y que ya haya reportado a la nube su estado haz clic en el enlace **Cambiar**. Se mostrará una ventana con las unidades locales disponibles.
- Por cada unidad se muestra el nombre del volumen, la unidad asignada, el espacio ocupado y el

espacio libre.

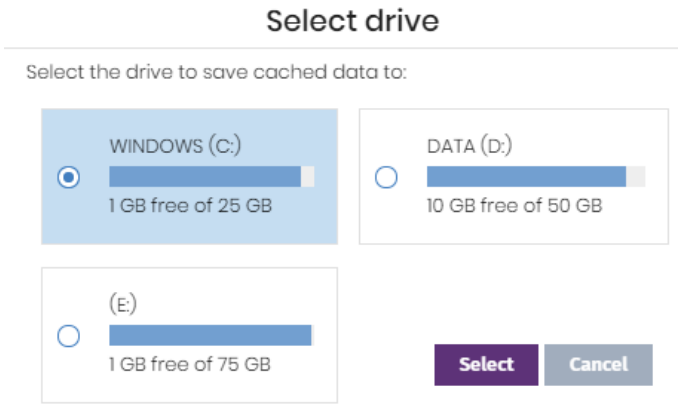


Figura 11.1: ventana de selección de volumen en un equipo con el rol de caché asignado

- Para ver los porcentajes de espacio ocupado y libre pasa el ratón por encima de las barras y se mostrará un tooltip con la información.
- Indica con el selector la unidad con 1 Gigabyte libre o más que almacenará los elementos cacheados, y haz clic en el botón **Seleccionar**. Cytomic EPDR comenzará a copiar los elementos ya cacheados y, una vez completado el proceso, los borrará de su ubicación original.

> *Solo es posible seleccionar la unidad donde se almacenarán los elementos a cachear en los equipos que hayan reportado su estado al servidor Cytomic EPDR. Si no se cumple esta condición se tomará por defecto la unidad que almacena los ficheros de instalación de Cytomic EPDR. Una vez reportado se mostrará el enlace **Cambiar** en el equipo con el rol de cache asignado y se podrá modificar la unidad de almacenamiento. Un equipo puede tardar en reportar su estado varios minutos.*

Si no hay espacio suficiente o se produce algún error de escritura al cambiar la unidad de almacenamiento se mostrará un mensaje debajo del equipo con el nodo caché asignado, indicando la fuente del problema.

Rol de descubridor

En el menú superior **Configuración**, panel lateral **Servicios de red**, la pestaña **Descubrimiento** está directamente relacionada con el procedimiento de instalación y despliegue de Cytomic EPDR en la red del cliente.

> *Consulta el apartado "**Descubrir equipos**" en la página 110 para obtener más información acerca del proceso de descubrimiento e instalación de Cytomic EPDR.*

Configuración de listas de acceso a través de proxy

Cytomic EPDR permite asignar a los equipos de la red uno o más métodos de conexión con el exterior, en función de los recursos existentes en la infraestructura IT de la compañía.

Cytomic EPDR maneja una lista de métodos de acceso configurable por el administrador, que recorre cuando necesita conectar con la nube de Cytomic. Una vez seleccionado, el método de acceso elegido no cambia hasta que éste queda inaccesible, momento en el cual Cytomic EPDR seguirá recorriendo la lista hasta encontrar uno nuevo que sea válido. Si llega al final de la lista volverá a iniciar el recorrido hasta que todos los métodos de conexión hayan sido probados al menos una vez.

Los tipos de conexión soportados por Cytomic EPDR son:

Tipo de proxy	Descripción
No usar proxy	Acceso directo a Internet. Los equipos acceden de forma directa a la nube de Cytomic para descargar las actualizaciones y enviar los reportes de estado del equipo. En este caso, el software Cytomic EPDR utilizará la configuración del equipo para comunicarse con Internet.
Proxy corporativo	Acceso a Internet vía proxy instalado en la red de la organización. • **Dirección**: dirección IP del servidor de proxy. • **Puerto**: puerto del servidor de proxy. • **El proxy requiere autenticación**: habilitar si el proxy requiere información de usuario y contraseña. • **Usuario**: cuenta de un usuario del proxy que permita su uso. • **Contraseña**: contraseña de la cuenta de usuario.
Descubrimiento automático de proxy a través de Web Proxy Autodiscovery Protocol (WPAD)	Pregunta a la red mediante DNS o DHCP para recuperar la url de descubrimiento que apunta al archivo PAC de configuración. Alternativamente se puede indicar directamente el recurso HTTP o HTTPS donde se encuentra el archivo PAC de configuración.
Proxy Cytomic EPDR	Acceso a través del agente Cytomic EPDR instalado en un equipo de la red. Centraliza todas las comunicaciones de la red a través de un equipo con un agente Cytomic instalado. Para configurar la salida de un equipo a través de un proxy Cytomic EPDR haz clic en el enlace **Seleccionar equipo.** Se desplegará una ventana con el listado de equipos disponibles que tienen el rol de proxy en la red. Selecciona uno de la lista y haz clic en el botón **Añadir**.

Tabla 11.1: tipos de acceso a la red soportados por Cytomic EPDR

*Es posible configurar una lista de accesos formada por varios equipos con el rol de proxy asignado. Asigna previamente el rol de proxy Cytomic EPDR a uno o más equipos de la red con Cytomic EPDR instalado siguiendo los pasos indicados en el apartado "***Asignar el rol de proxy a un equipo***".*

Configurar una lista de acceso

Para configurar una lista de acceso crea una configuración de tipo Configuración de red:

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y en el botón **Añadir** o selecciona una configuración ya creada para modificarla.
- En la sección **Proxy** haz clic en el icono ⊕. Se mostrará una ventana con los tipos de conexión disponibles.
- Selecciona un tipo de conexión (tabla 11.1) y haz clic en el botón **Aceptar**. El tipo de conexión se añadirá a la lista.
- Para modificar el orden de los métodos de conexión selecciona un elemento haciendo clic en la casilla de selección y utiliza las fechas ↑ y ↓ para subirlo o bajarlo.
- Para borrar un método de conexión haz clic en el icono 🗑.
- Para modificar un método de conexión selecciónalo con las casillas de selección y haz clic en el icono ✎. Se mostrará una ventana donde editar la configuración del método.

Mecanismo de fallback

Cuando un agente Cytomic no puede conectar con la plataforma Cytomic y ha probado todos los métodos de conexión indicados en su lista de acceso configurada, ejecutará la siguiente lógica de fallback para restaurar la conexión mediante otro método disponible:

- **Internet Explorer**: Cytomic EPDR intenta recuperar la configuración de proxy de Internet Explorer impersonado como el usuario que inició sesión en el equipo.
  - Si la configuración de las credenciales para el uso del proxy está definida de forma explícita este método de acceso no se podrá utilizar.
  - Si la configuración de proxy de Internet Explorer utiliza PAC (Proxy Auto-Config) se recupera la URL del archivo de configuración, siempre que el protocolo de acceso al recurso sea HTTP o HTTPs.
- **WinHTTP / WinInet**: Cytomic EPDR lee la configuración del proxy por defecto.
- **Conexión directa**: Cytomic EPDR intenta conectarse directamente a la nube de Cytomic.

Configuración de las descargas mediante equipos caché

> *El acceso a equipos con el rol de caché asignado para acelerar las actualizaciones y las descargas de parches solo está disponible en sistemas operativos Windows.*

La utilización de un equipo con el rol de caché puede establecerse de dos maneras:

- **Método automático**: el equipo que inicia la descarga utiliza los equipos con el rol de caché descubiertos en la red y que cumplan con los requisitos indicados en el apartado "**Requisitos para usar un equipo con el rol de caché en modo automático**". Si se encuentran varios equipos caché se

balancearán las descargas para no sobrecargar a un único equipo caché.

- **Método manual**: el administrador establece de forma manual el equipo de la red con el rol de caché que será utilizado para descargar datos de la nube de Cytomic. El comportamiento de un nodo cache asignado de forma manual tiene las siguientes diferencias con respecto al modo automático:
  - El administrador puede elegir cualquier equipo de la red con el rol de cache asignado, sin importar la subred a la que pertenezca.
  - Si un equipo tiene varios nodos cache asignados de forma manual no se repartirán las descargas.
  - Si el primer equipo caché no está accesible se recorrerá la lista hasta encontrar un equipo que funcione. Si no se encuentra ningún equipo se intentará la salida directa a Internet.

Para que un equipo pueda conectarse en modo manual a un nodo caché es necesario que los dos tengan el puerto 18226 TCP abierto en ambos sentidos de la comunicación.

Requisitos para usar un equipo con el rol de caché en modo automático

- A diferencia del modo manual, en el modo automático el ámbito de un equipo con rol de caché está limitado al segmento donde esté conectada su interface de red. Si un equipo caché tiene varias tarjetas de red podrá servir de repositorio en cada uno de los segmentos a los que esté conectado.

Se recomienda asignar un equipo como rol caché en cada segmento de la red de la compañía.

- El resto de equipos descubrirán de forma automática la presencia de un nodo caché y redirigirán hacia él sus peticiones de actualización.
- Se requiere asignar una licencia de protección al nodo caché para su funcionamiento.
- Configura el cortafuegos para permitir el tráfico SSDP (uPnP) entrante y saliente en el puerto UDP 21226 y 18226 TCP.

Descubrimiento de nodos caché

En el momento de la asignación del rol al equipo, éste lanzará un broadcast hacia los segmentos de red a los que pertenecen sus interfaces. Los puestos de trabajo y servidores con el método automático de asignación recibirán la publicación del servicio y, en el caso de que en un mismo segmento haya más de un nodo caché designado, los equipos se conectarán al más adecuado en función de los recursos libres que posea.

Adicionalmente, cada cierto tiempo los equipos de la red con el método automático de asignación configurado preguntarán si existe algún nodo con el rol de caché instalado.

Configuración del método de asignación de nodos caché

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y elige una configuración.
- En la sección **Caché** elige una opción:
  - **Utilizar automáticamente los equipos caché vistos en la red**: los equipos que reciben esta configuración buscarán de forma automática los nodos caché de su segmento de red.
  - **Utilizar los siguientes equipos caché (por orden de preferencia)**: haz clic en el icono ⊕ para añadir equipos con el rol de caché asignado y configurar una lista de nodos caché. Los equipos que reciban esta configuración conectaran con los nodos caché indicados en la lista para realizar las descargas.

Configuración de la comunicación en tiempo real

Cytomic EPDR se comunica en tiempo real con la plataforma Cytomic para recuperar las configuraciones establecidas en la consola sobre los equipos protegidos, transcurriendo unos pocos segundos desde que el administrador asigna una configuración a un equipo hasta que éste la aplica.

Las comunicaciones en tiempo real entre los equipos protegidos y el servidor Cytomic EPDR requieren el mantenimiento de una conexión abierta por cada puesto de forma permanente. Desactiva las comunicaciones en tiempo real cuando el número de conexiones abiertas afecte al rendimiento del proxy instalado en la red, o cuando el impacto en el consumo de ancho de banda sea elevado al cambiar simultáneamente las configuraciones de un gran número de equipos.

Requisitos para comunicació en tiempo real

- Las comunicaciones en tiempo real son compatibles con todos los sistemas operativos soportados por Cytomic excepto Windows XP y Windows 2003.
- Si el equipo accede a Internet mediante un proxy corporativo, se requiere que las conexiones https no sean manipuladas. Muchos proxys utilizan técnicas Man in the Middle para analizar las conexiones https o funcionar como proxys caché. En estos casos la comunicación en tiempo real no funcionará.

Deshabilitar las comunicaciones en tiempo real

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y en el botón **Añadir** o selecciona una configuración ya creada para modificarla.
- En la sección **Proxy** despliega la sección **Opciones avanzadas** y desactiva la casilla **Activar la comunicación en tiempo real**.

Al deshabilitar las comunicaciones en tiempo real, los equipos se comunicarán con el servidor Cytomic EPDR cada 15 minutos.

Configuración del idioma del agente

Para asignar el idioma del agente Cytomic a uno o varios equipos es necesario crear una configuración de tipo **Configuración de red**:

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y en el botón **Añadir** o selecciona una configuración ya creada para modificarla.
- En la sección idioma elige el idioma de entre los disponibles:
  - Alemán
  - Español
  - Finlandés
  - Francés
  - Húngaro
  - Inglés
  - Italiano
  - Japonés
  - Portugués
  - Ruso
  - Sueco

Si se produce un cambio de idioma y la consola local de Cytomic EPDR estaba abierta se pedirá un reinicio de la consola local. Este procedimiento no afecta a la seguridad del equipo.

Configuración de la visibilidad del agente

Para las empresas donde el servicio de seguridad sea 100% administrado por el departamento de IT no es necesario que el icono del agente Cytomic EPDR sea visible en el área de notificaciones de los equipos de la red. Para ocultar o mostrar el icono sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Preferencias** y activa o desactiva la opción **Mostrar icono en la bandeja del sistema.**

Configuración de contraseña y anti-tampering

Anti-tamper

Muchas amenazas avanzadas incorporan técnicas para desactivar el software de seguridad instalado en los equipos, y así evitar todas sus funcionalidades. Este comportamiento también es práctica habitual de los hackers, y Cytomic EPDR incorpora tecnología anti-tamper que impide la modificación no autorizada del funcionamiento de la protección.

Habilitar anti-tamper

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes por equipo**.
- Haz clic en una configuración existen o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**:
  - **Activar protección anti-tamper**: impide que los usuarios o ciertos tipos de malware puedan detener las protecciones. Requiere el establecimiento de una contraseña ya que es posible que el administrador o el equipo de soporte necesiten detener temporalmente desde la consola local las protecciones para diagnosticar problemas.

Protección del agente mediante contraseña

Para evitar que el usuario modifique las características de protección o desinstale completamente el software Cytomic EPDR, el administrador puede establecer una contraseña local que cubra ambos casos.

Asignar una contraseña local

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad** frente a manipulaciones no deseadas de las protecciones:
  - **Solicitar contraseña para desinstalar Cytomic desde los equipos**: evita que el usuario desinstale el software Cytomic EPDR protegiéndolo con una contraseña.
  - **Permitir activar/desactivar temporalmente las protecciones desde la consola de los equipos**: permite administrar las capacidades de seguridad del equipo desde la consola local. Requiere el establecimiento de una contraseña.

Parte 5

Gestión de la seguridad

Capítulo 12: Configuración de estaciones y servidores

Capítulo 13: Configuración de seguridad Android

Capítulo 14: Cytomic Data Watch (Supervisión de información sensible)

Capítulo 15: Cytomic Patch (Actualización de programas vulnerables)

Capítulo 16: Cytomic Encryption (Cifrado de dispositivos)

Capítulo 17: Configuración del bloqueo de programas

Capítulo 12

Configuración de estaciones y servidores

Cytomic EPDR ofrece todas las funcionalidades de protección incluidas en el producto mediante las configuraciones de seguridad para estaciones y servidores. El administrador de la red podrá proteger los activos de la empresa frente a amenazas informáticas de muy diversa índole asignando configuraciones de seguridad a los equipos de la red.

En este capítulo se explican todos los parámetros incluidos en la configuración de seguridad para estaciones y servidores. También se indican algunas recomendaciones prácticas para asegurar los puestos de trabajo de la red y minimizar los inconvenientes ocasionados al usuario.

CONTENIDO DEL CAPÍTULO

Introducción a la configuración de la seguridad

Las configuraciones de seguridad para estaciones y servidores se dividen en varios apartados. Al hacer clic en cada uno de ellos se mostrará un desplegable con la información asociada. A continuación, se muestran las diferentes secciones con una breve explicación.

Sección	Descripción
General	Establece el comportamiento de las actualizaciones, desinstalaciones de los antivirus de otros fabricantes y los ficheros excluidos en el equipo del usuario o servidor protegido que no se analizarán.
Protección avanzada (Dispositivos Windows)	Establece el comportamiento de la protección avanzada y de la protección anti exploit frente a APTs, amenazas dirigidas y malware avanzado o que utiliza exploits.
Antivirus	Establece el comportamiento de la protección antimalware tradicional frente a virus y amenazas.
Firewall (Dispositivos Windows)	Establece el comportamiento del cortafuegos y del IDS que protege al equipo de los ataques de red.
Control de dispositivos (Dispositivos Windows)	Determina el acceso del usuario a los periféricos conectados al equipo.
Control de acceso a páginas web	Regula las visitas del usuario a categorías de páginas web.

Tabla 12.1: descripción de los módulos disponibles en Cytomic EPDR

Sección	Descripción
Antivirus para servidores Exchange	Analiza los mensajes entrantes y salientes de los servidores de correo Exchange en busca de amenazas.
Anti spam para servidores Exchange	Analiza los mensajes entrantes y salientes de los servidores de correo Exchange en busca de correo no deseado.
Filtrado de contenidos para servidores Exchange	Regula el tipo de contenidos que puede recibir el servidor Exchange.

Tabla 12.1: descripción de los módulos disponibles en Cytomic EPDR

No todas las funcionalidades se encuentran disponibles en todas las plataformas soportadas. A continuación se muestra un resumen de las funcionalidades de seguridad incluidas en Cytomic EPDR por plataforma compatible:

Funcionalidad	Windows	macOS	Linux	Windows Exchange
Protección avanzada	X			
Protección Anti-exploit	X			
Antivirus	X	X	X	X
Cortafuegos & IDS	X			
Protección Email	X			
Protección Web	X	X	X	
Control de dispositivos	X			
Filtrado Web	X	X	X	
Anti-spam				X
Filtrado de contenidos				X

Tabla 12.2: funcionalidades de seguridad por plataforma

Acceso a la configuración Estaciones y servidores

Para crear una nueva configuración de Estaciones y servidores o asignar una ya existente a grupos de equipos de la red, sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Configuración**, panel lateral **Estaciones y servidores**. Se mostrará un listado de las configuraciones ya creadas.
- Para crear una nueva configuración haz clic en el botón **Añadir** situado en la parte superior derecha de la ventana. Se mostrará un formulario donde podrás determinar todos los parámetros de la seguridad disponibles para aplicar a los equipos administrados por Cytomic EPDR.

Configuración General

La configuración general establece el comportamiento de Cytomic EPDR relativo a las actualizaciones, desinstalación de programas de la competencia y exclusiones de ficheros y carpetas que no se analizarán.

Actualizaciones

*Consulta el capítulo "**Actualización del software cliente**" en la página **143** para obtener información acerca de los procedimientos necesarios para actualizar el agente, la protección y el fichero de firmas de software cliente instalado en el equipo del usuario.*

Desinstalar otros productos de seguridad

*Consulta el apartado "**Visión general del despliegue de la protección**" en la página **100** para establecer el comportamiento de la instalación de la protección en el caso de que otro producto de seguridad esté instalado previamente en el equipo del usuario.*

*Consulta el capítulo "**Desinstaladores soportados**" en la página **379** para obtener un listado de todos los productos de la competencia que Cytomic EPDR desinstala automáticamente del equipo del usuario.*

Exclusiones

Exclusiones configura los elementos del equipo que no serán bloqueados, borrados o desinfectados en busca de malware.

Esta configuración afecta tanto a la protección antivirus como a la protección avanzada.

Ficheros en disco

Indica los ficheros en el disco de los equipos protegidos que no serán borrados o desinfectados por Cytomic EPDR.

Campo	Descripción
Extensiones	Extensiones de ficheros que no serán analizadas.
Carpetas	Carpetas cuyo contenido no será analizado.

Tabla 12.3: ficheros en disco que no serán analizados por Cytomic EPDR

Campo	Descripción
Archivos	Ficheros que no serán analizados. Se permite el uso de los caracteres comodín '*' y '?'.
Exclusiones recomendadas para Exchange	Al hacer clic en el botón **Añadir**, se cargan de forma automática las exclusiones recomendadas por Microsoft para optimizar el rendimiento del producto en servidores Exchange.

Tabla 12.3: ficheros en disco que no serán analizados por Cytomic EPDR

Excluir archivos adjuntos de correo

Especifica la lista de extensiones de ficheros que no son analizados en caso de encontrarse como adjuntos en mensajes de correo.

Protección avanzada (Equipos Windows)

Comportamiento de la protección avanzada

La protección avanzada establece los diferentes modos de bloqueo frente al malware desconocido, protegiendo al equipo de APTs y amenazas avanzadas.

- **Protección avanzada**: activa o desactiva el motor de protección contra amenazas avanzadas, especifico de Cytomic EPDR.
- **Modo de funcionamiento**:

Campo	Descripción
Auditoria	Solo se informa de las amenazas detectadas, pero no se bloquea ni se desinfecta el malware encontrado.
Hardening	Ejecuta los programas desconocidos ya instalados en el equipo del usuario. Bloquea los programas desconocidos que vienen de fuentes no fiables como Internet, otros equipos de la red o unidades de almacenamiento externas hasta su clasificación. Los programas clasificados como malware serán desinfectados o eliminados.
Lock	Bloquea la ejecución de todos los programas desconocidos hasta que estén clasificados y los programas ya clasificados como malware.

Tabla 12.4: modos de funcionamiento de la protección avanzada de Cytomic EPDR

Anti exploit

> *La protección anti exploit está deshabilitada por defecto para mejorar la compatibilidad con soluciones de seguridad de terceros que también incorporen este tipo de tecnología. En esta situación, ni los ataques de tipo exploit ni el malware de tipo Metasploit serán detectados / bloqueados, aunque el resto de módulos de protección detectarán y bloquearán las acciones consideradas peligrosas para el sistema. Habilita la protección anti exploit de forma gradual en aquellos equipos con soluciones de seguridad de terceros para comprobar su buen funcionamiento.*

La protección anti exploit bloquea de forma automática y sin intervención del usuario en la mayor parte de los casos los intentos de explotación de vulnerabilidades de procesos instalados en el equipo del usuario.

Funcionamiento de la protección anti-exploits

Los equipos de la red pueden contener procesos de origen conocido y fiable pero con fallos de programación. Son conocidos como "procesos vulnerables" debido a que interpretan de forma incorrecta ciertas secuencias de datos que reciben del usuario o de otros procesos.

Cuando un proceso vulnerable recibe un determinado patrón de información conocido por los hackers, se produce un mal funcionamiento interno que deriva en una inyección de fragmentos de código preparados por el hacker en las regiones de memoria gestionadas por el proceso vulnerable. Un proceso así afectado recibe el nombre de "proceso comprometido". La inyección de código provoca que el proceso comprometido ejecute acciones para las que no fue programado, generalmente peligrosas y que comprometen la seguridad del equipo.

La protección anti-exploit de Cytomic EPDR detecta la inyección de código malicioso en los procesos vulnerables ejecutados por el usuario, bloqueándola mediante dos cursos de acción diferentes, dependiendo del exploit encontrado:

- **Bloqueo del exploit**

Detecta la inyección de código en el proceso vulnerable cuando todavía no se ha completado. El proceso no llega a comprometerse y el riesgo del equipo es nulo, con lo que no requiere detener el proceso afectado ni reiniciar el equipo de usuario. No implica pérdida de información por parte del proceso afectado.

El usuario puede recibir una notificación del bloqueo dependiendo de la configuración establecida por el administrador.

- **Detección del exploit**

Detecta la inyección de código en el proceso vulnerable cuando ya se ha producido. Debido a que el proceso vulnerable ya contiene el código malicioso, es imperativo cerrarlo antes de que ejecute acciones que puedan poner en peligro la seguridad del equipo.

Independientemente del tiempo transcurrido desde la detección hasta el cierre del proceso Cytomic EPDR considera en riesgo el equipo, aunque su cuantificación depende del tiempo transcurrido en cerrar el proceso afectado y del diseño del malware. Cytomic EPDR puede cerrar el proceso de forma automática para minimizar los efectos adversos, o delegar en el usuario la decisión, pidiéndole permiso de forma explícita para descargarlo de la memoria.

Si el administrador ha configurado el cierre automático para minimizar la posibilidad de efectos adversos, el usuario puede sufrir la pérdida de información manejada por el proceso afectado. Si, por el contrario, el administrador ha delegado en el usuario la decisión, el usuario podrá retrasar el cierre de la aplicación y minimizar la posibilidad perdida de información.

En los casos en que no sea posible cerrar el proceso afectado se pedirá permiso al usuario para reiniciar el equipo completo.

Configuración de la detección anti - exploits

- **Anti-exploit**: habilita la protección contra exploits.
- **Inyección avanzada de código**: detecta mecanismos avanzados de inyección de código en procesos en ejecución..

Campo	Descripción
Auditar	Notifica en la consola Web la detección del exploit, pero no toma acciones contra él ni informa al usuario del equipo.
Bloquear	Bloquea los ataques de tipo exploit. Puede requerir el cierre del proceso afectado por el exploit. • **Informar del bloqueo al usuario del equipo**: el usuario recibe una notificación, pero el proceso comprometido se cierra de forma automática si es necesario. • **Pedir permiso al usuario**: el usuario recibe una petición de autorización para el cierre del proceso comprometido por el exploit en caso de ser necesario. Esta opción resulta útil para que el usuario pueda salvar la información antes producirse el cierre del proceso. Si se requiere el reinicio del equipo siempre se pide confirmación al usuario, independientemente de la configuración **Pedir permiso al usuario.**

Tabla 12.5: modo de funcionamiento de la protección avanzada anti-exploit en Cytomic EPDR

Dado que muchos exploits continúan ejecutando código malicioso hasta que no se produce el cierre del proceso, la incidencia no se marcará como resuelta en el panel de elementos maliciosos y exploit de la consola Web hasta que el programa haya sido cerrado.

Privacidad

Cytomic EPDR incluye el nombre, la ruta completa de los ficheros y el usuario que inició la sesión en el equipo cuando envía los archivos a la nube de Cytomic para su análisis. Esta información se utiliza posteriormente en los informes y las herramientas de análisis forense mostrados en la consola Web. Para no enviar que esta información desactiva la casilla apropiada en la pestaña **Privacidad**.

Uso de la red

Los ficheros ejecutables desconocidos encontrados en el equipo del usuario se envían a la nube de Cytomic para su análisis. El impacto en el ancho de banda de la red del cliente está configurado de forma predeterminada para pasar desapercibido:

- Se envía un máximo de 50 Mbytes por hora y agente.
- Un fichero concreto desconocido se envía una sola vez para todos los clientes que usan Cytomic EPDR.
- Se implementan mecanismos de gestión del ancho de banda con el objetivo de evitar un uso intensivo de los recursos de red.

Para configurar el número máximo de megabytes que un agente podrá enviar en una hora introduce el valor y haz clic en **Ok**. Para establecer transferencias ilimitadas deja el valor a 0.

Antivirus

Esta sección configura el comportamiento general del motor de antivirus basado en ficheros de firmas.

Campo	Descripción
Protección de archivos	Activa o desactiva la protección antivirus que afecta al sistema de ficheros.
Protección de correo	Activa o desactiva la protección antivirus que afecta al cliente de correo instalado en el equipo del usuario. Cytomic EPDR detectará las amenazas recibidas por el protocolo POP3 y sus variantes cifradas.
Protección web	Activa o desactiva la protección antivirus que afecta al cliente web instalado en el equipo del usuario. Cytomic EPDR detectará las amenazas recibidas por el protocolo HTTP y sus variantes cifradas.

Tabla 12.6: módulos de protección antivirus disponibles en Cytomic EPDR

La acción que ejecuta Cytomic EPDR ante un fichero de tipo malware o sospechoso se define en los laboratorios de Cytomic:

- **Ficheros conocidos como malware desinfectable**: sustituir el fichero original por una copia desinfectada.

- **Ficheros conocidos como malware no desinfectable**: se guarda una copia de seguridad y el fichero original se elimina.

Amenazas a detectar

Configura el tipo de amenazas que Cytomic EPDR busca y elimina en el sistema de archivos, cliente de correo y web instalados en el equipo del usuario.

Campo	Descripción
Detectar virus	Ficheros que contienen patrones identificados por el fichero de firmas como peligrosos.
Detectar herramientas de hacking y PUPs	Programas no deseados (programas que contienen publicidad intrusiva, barras de navegación etc.) y herramientas utilizadas por los hackers para ganar acceso a los sistemas.
Bloquear acciones maliciosas	Activa tecnologías anti exploit y heurísticas para analizar localmente el comportamiento de los procesos y buscar actividades sospechosas
Detectar Phishing	Ataques basados en el engaño por web y correo.
No detectar amenazas en las siguientes direcciones y dominios	Lista blanca de direcciones y dominios que no se analizarán en busca de ataques por phishing. Se compara a nivel de sub cadenas y sin tener en cuenta las mayúsculas y minúsculas por lo que para incluir una dirección en la lista blanca es suficiente con indicar una parte de la misma.

Tabla 12.7: tipos de malware detectados por la protección antivirus de Cytomic EPDR

Tipos de archivos

Indica los tipos de archivos que Cytomic EPDR analiza:

Campo	Descripción
Analizar comprimidos en disco	Descomprime los ficheros empaquetados y analiza su contenido en busca de malware.
Analizar comprimidos en mensajes de correo	Descomprime los ficheros adjuntos que viajan en los correos electrónicos y analiza su contenido en busca de malware.
Analizar todos los archivos independientemente de su extensión cuando son creados o modificados (No recomendado)	Por cuestiones de rendimiento no se recomienda analizar todos los ficheros ya que técnicamente muchos tipos de ficheros de datos no pueden presentar amenazas a la seguridad del equipo.

Tabla 12.8: tipos de archivos analizados por la protección antivirus de Cytomic EPDR

Firewall (Equipos Windows)

Cytomic EPDR incluye tres herramientas para filtrar el tráfico de red que recibe o envía un equipos protegido:

- **Protección mediante reglas de sistema**: describen características de las comunicaciones establecidas por el equipo (puertos, IPs, protocolos etc.), con el objetivo de permitir o denegar los flujos de datos que coincidan con las reglas configuradas.
- **Protección de programas**: permite o deniega la comunicación a determinados programas instalados en el equipo de usuario.
- **Sistema de detección de intrusos**: detecta y rechaza patrones de tráfico mal formado que afectan a la seguridad o al rendimiento del equipo protegido.

Modo de funcionamiento

Se accede mediante el control **La configuración firewall la establece el usuario de cada equipo:**

- **Activado (firewall en modo usuario o auto administrado)**: el propio usuario podrá configurar desde la consola local el firewall de su equipo.
- **Desactivado (firewall en modo administrador)**: el administrador configura el cortafuegos de los equipos a través de perfiles de configuración.

Tipo de red

Los equipos de usuario portátiles pueden conectarse a redes con un grado de seguridad muy diverso según se trate de accesos públicos, como la red wifi de un cibercafé, o de redes gestionadas o de acceso limitado, como la red de una empresa. Para ajustar el comportamiento por defecto del cortafuegos, el administrador de la red puede seleccionar de forma manual el tipo de red al que se conectan usualmente los equipos del perfil configurado, o puede dejar a Cytomic EPDR. la elección de la red mas apropiada.

Tipo de red	Descripción
Red pública	Redes que se encuentran en cibercafés, aeropuertos, etc. Implica establecer limitaciones en el nivel de visibilidad de los equipos protegidos y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.
Red de confianza	Redes que se encuentran en oficinas y domicilios. El equipo es perfectamente visible para el resto de usuarios de la red, y viceversa. No hay limitaciones para compartir archivos, recursos y directorios.
Detectar automáticamente	El tipo de red (red pública o red de confianza) se selecciona de forma automática en función de una serie de criterios que el equipo del usuario debe de cumplir. Haz clic en el enlace **Configurar reglas para determinar cuándo un equipo está conectado a una red de confianza.**

Tabla 12.9: tipos de red compatibles con el cortafuegos

El comportamiento de Cytomic EPDR según la red seleccionada se traduce en un mayor o menor número de reglas añadidas de forma automática. Estas reglas se pueden ver en Reglas de programa y Reglas de conexión como "reglas de Cytomic".

El tipo de red es un concepto aplicable a cada interface de red del equipo de forma independiente. Es posible que equipos con varias interfaces de red tengan distintos tipos de red asignados y por lo tanto las reglas del cortafuegos serán diferentes para cada interface de red.

Configurar criterios para determinar el tipo de red

Cytomic EPDR permite añadir uno o más criterios que el equipo protegido por el cortafuegos deberá de cumplir para seleccionar de forma automática la configuración **Red de confianza**. Si ninguna de estas condiciones se cumplen el tipo de red establecido en el interface de red será **Red pública**.

Un criterio es una regla que determina si una interface de red del equipo se considera que está conectado a una red de confianza. Esta asociación se realiza mediante la resolución de un dominio definido previamente en un servidor DNS interno de la empresa: si el equipo es capaz de conectar con el servidor DNS de la empresa y resolver el dominio configurado querrá decir que está conectado a la red de la empresa, y por lo tanto el cortafuegos puede asumir que el equipo se encuentra en una red de confianza.

A continuación se muestra un ejemplo de configuración completo:

- En este ejemplo se utilizará "`miempresa.com`" como la zona principal del cliente que quiere que sus equipos detecten de forma automática si están conectados a la red corporativa.
- Añade el registro de tipo A "`criteriocortafuegos`" en la zona "`miempresa.com`" del servidor DNS interno de la red, sin especificar dirección IP ya que no tendrá ninguna utilidad.
- Según esta configuración, "`criteriocortafuegos.miempresa.com`" será el dominio que Cytomic EPDR intentará resolver para comprobar que se encuentra dentro de la red corporativa.
- Reinicia el servidor DNS para cargar la nueva configuración si fuera necesario, y comprueba que "`criteriocortafuegos.miempresa.com`" se resuelve correctamente desde todos los segmentos de la red interna con las herramientas `nslookup`, `dig` o `host`.
- En la consola de Cytomic EPDR haz clic en el enlace **Configurar reglas para determinar cuándo un equipo está conectado a una red de confianza**. Se mostrará una ventana con los siguientes campos a completar:
  - **Nombre del criterio**: indica un nombre descriptivo de la regla a configurar. Por ejemplo "`micriterioDNS`".
  - **Servidor DNS**: indica la dirección IP del servidor DNS de la red interna de la empresa que recibirá la petición de resolución.
  - **Dominio**: indica la petición que el equipo enviará al servidor DNS para su resolución. Introduce "`criteriocortafuegos.miempresa.com`".
  - Haz clic en el botón **Aceptar**, en el botón **Guardar** y nuevamente en el botón **Guardar**.

- Una vez configurado y aplicado el criterio el equipo intentará resolver el dominio "`criteriocortafuegos.miempresa.com`" en el servidor DNS especificado cada vez que se produzca un evento en la interface de red (conexión desconexión, cambio de IP etc.). Si la resolución DNS es correcta se asignará a la interface de red que se utilizó la configuración asignada a la red de confianza.

Reglas de programa

En esta sección se configuran los programas del usuario que comunican con la red y los que tienen bloqueado el envío y recepción de datos.

Para desarrollar una correcta estrategia de protección sigue los pasos mostrados a continuación, en el orden indicado:

1. Establecer la acción por defecto.

Acción	Descripción
Permitir	Estrategia permisiva basada en aceptar por defecto las conexiones de todos los programas cuyo comportamiento no ha sido definido explícitamente mediante una regla en el paso 3. Este es el modo configurado por defecto y considerado el más básico.
Denegar	Estrategia restrictiva basada en denegar por defecto las conexiones de los programas cuyo comportamiento no ha sido definido explícitamente mediante una regla en el paso 3. Este es el modo avanzado de funcionamiento ya que requiere añadir reglas para todos los programas que los usuarios utilizan de forma habitual; de otro modo las comunicaciones de esos programas son denegadas, afectando probablemente a su buen funcionamiento.

Tabla 12.10: tipos de acción por defecto en el cortafuegos para los programas instalados en el equipo del usuario

2. Activar reglas de Cytomic.

Activa las reglas generadas automáticamente por Cytomic para el tipo de red definido anteriormente.

3. Añadir reglas para definir el comportamiento específico de una aplicación.

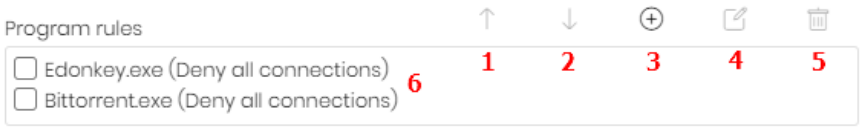


Figura 12.1: controles de edición de reglas de red

Los controles situados a la derecha permiten subir **(1)**, bajar **(2)**, añadir **(3)**, editar **(4)** y borrar **(5)** reglas de programas. Las casillas de selección **(6)** determinan sobre qué reglas se realizarán las acciones.

Al crear una regla es necesario indicar los siguientes campos:

- **Descripción**: descripción de la regla.

- **Programa**: selecciona el programa cuyo comportamiento en red se va a controlar.
- **Conexiones permitidas para este programa**: define las características del tráfico que se controlará:

Campo	Descripción
Permitir conexiones entrantes y salientes	El programa se podrá conectar a la red (Internet y redes locales) y también se permitirá que otros se conecten a él. Existen ciertos tipos de programas que requieren este tipo de permisos para funcionar correctamente: programas de intercambio de archivos, aplicaciones de chat, navegadores de Internet, etc.
Permitir conexiones salientes	El programa se podrá conectar a la red, pero no aceptará conexiones externas por parte de otros usuarios o aplicaciones.
Permitir conexiones entrantes	El programa aceptará conexiones externas de programas o usuarios procedentes de Internet, pero no tendrá permisos para establecer nuevas conexiones.
Denegar todas las conexiones	El programa no podrá acceder a la red.

Tabla 12.11: modos de comunicación de los programas permitidos

- **Permisos avanzados**: define las características exactas del tráfico que es aceptado o denegado.

Campo	Descripción
Acción	Establece la acción que ejecutará Cytomic EPDR si la regla coincide con el tráfico examinado. • **Permitir**: permite el tráfico. • **Denegar**: bloquea el tráfico. Hace un `Drop` de la conexión.
Sentido	Establece la dirección del tráfico para protocolos orientados a conexión, como TCP. • **Salientes**: tráfico con origen el equipo de usuario y destino otro equipo de la red. • **Entrantes**: tráfico con destino el equipo de usuario y origen otro equipo de la red.
Zona	La regla solo se aplica si la zona indicada coincide con la zona configurada en el apartado "**Tipo de red**". Las reglas que tengan en campo **Zona** a **Todos** se aplican siempre sin tener en cuenta la zona configurada en el perfil de protección.
Protocolo	Especifica el protocolo de nivel 3 del tráfico generado: • Todos • TCP • UDP

Tabla 12.12: modos avanzados de comunicación de los programas permitidos

Campo	Descripción
IP	• **Todos**: no tiene en cuenta los campos IP de origen y destino de la conexión. • **Personalizado**: define la IP de origen o destino del tráfico a controlar. Especifica más de una IP separadas por ',' o utiliza el carácter '-' para establecer rangos de IPs. Selecciona en el desplegable si las direcciones IP son IPv4 o IPv6. No es posible mezclar tipos de direcciones IP en una misma regla. • **Puertos**: selecciona el puerto de la comunicación. Elige **Personalizado** para añadir varios puertos separados por comas y rangos de puertos utilizando guiones.

Tabla 12.12: modos avanzados de comunicación de los programas permitidos

Regla de conexión

Son reglas tradicionales de filtrado de tráfico TCP/IP. Cytomic EPDR extrae el valor de ciertos campos de las cabeceras de cada paquete que reciben o envían los equipos protegidos, y explora el listado de reglas introducido por el administrador. Si alguna regla coincide con el tráfico examinado se ejecuta la acción asociada.

Las reglas de conexiones afectan a todo el sistema, independientemente del proceso que las gestione, y son prioritarias con respecto a las reglas por programa, configuradas anteriormente.

Para desarrollar una correcta estrategia de protección frente a tráfico no deseado o peligroso sigue los pasos mostrados a continuación, en el orden que se indica:

1. Establecer la acción por defecto del cortafuegos, situada en Reglas para programas.

Acción	Descripción
Permitir	Estrategia permisiva basada en aceptar por defecto las conexiones cuyo comportamiento no ha sido definido mediante reglas en el paso 3. Este es el modo básico de configuración: todas las conexiones no descritas mediante reglas son automáticamente aceptadas.
Denegar	Estrategia restrictiva basada en denegar por defecto las conexiones cuyo comportamiento no ha sido definido mediante reglas en el paso 3. Este es el modo avanzado de funcionamiento: todas las conexiones no descritas mediante reglas son automáticamente denegadas.

Tabla 12.13: tipos de acción por defecto en el cortafuegos para las conexiones gestionadas en el equipo del usuario

2. Activar reglas de Cytomic

Activa las reglas generadas automáticamente por Cytomic para el tipo de red definido.

3. Añadir reglas que describan conexiones de forma específica junto a una acción

asociada.

Figura 12.2: controles de edición de reglas de red

Los controles situados a la derecha permiten subir **(1)**, bajar **(2)**, añadir **(3)**, editar **(4)** y borrar **(5)** reglas de conexión. Las casillas de selección **(6)** determinan sobre qué reglas se aplican las acciones.

El orden de las reglas en la lista es importante: su aplicación se evalúa en orden descendente y, por lo tanto, al desplazar una regla hacia arriba o abajo en la lista, se modificará su prioridad.

A continuación, se describen los campos que forman una regla de sistema:

Campo	Descripción
Nombre de regla	Asigna un nombre único a la regla.
Descripción	Descripción del tipo de tráfico filtrado por la regla.
Sentido	Establece la dirección del tráfico para protocolos orientados a conexión, como TCP. • **Salientes**: tráfico saliente. • **Entrantes**: tráfico entrante.
Zona	La regla solo se aplica si la zona indicada coincide con la zona configurada en el apartado "**Tipo de red**". Las reglas que tengan en campo **Zona** a **Todos** se aplican siempre sin tener en cuenta la zona configurada en el perfil de protección.

Protocolo	Especifica el protocolo del tráfico. Según la elección se mostrarán unos controles u otros para identificarlo de forma precisa:
	• **TCP, UPD, TCP/UDP:** describe reglas TCP y / o UDP incluyendo puertos locales y remotos.
	  • **Puertos locales:** puerto de la conexión utilizado en el equipo del usuario. Selecciona **Personalizado** para añadir varios puertos separados por comas y rangos de puertos utilizando guiones.
	  • **Puertos remotos**: puerto de la conexión utilizado en el equipo remoto. Selecciona **Personalizado** para añadir varios puertos separados por comas y rangos de puertos utilizando guiones.
	• **Servicios ICMP:** crea reglas que describen mensajes ICMP, indicando su tipo y subtipo.
	• **Servicios ICMPv6:** crea reglas que describen mensajes ICMP sobre IPv6, indicando su tipo y subtipo.
	• **Tipos IP:** crea reglas para el protocolo IP y otros protocolos se orden superior.

Tabla 12.14: campos de las reglas de conexión

Campo	Descripción
Direcciones IP	Direcciones IP de origen o destino del tráfico. Especifica varias direcciones IP separadas por coma o mediante rangos con guión. Selecciona en el desplegable si las direcciones IP son IPv4 o IPv6. No es posible mezclar tipos de direcciones IP en una misma regla.
Direcciones MAC	Direcciones MAC de origen o destino del tráfico.

Tabla 12.14: campos de las reglas de conexión

Las direcciones MAC de origen y destino se reescriben en las cabeceras del paquete de datos cada vez que el tráfico atraviesa un proxy, enrutador etc. Los paquetes llegarán al destino con la MAC del último dispositivo que manipuló el tráfico.

Bloquear intrusiones

El módulo IDS permite detectar y rechazar tráfico mal formado y especialmente preparado para impactar en el rendimiento o la seguridad del equipo a proteger. Este tipo de tráfico puede provocar un mal funcionamiento de los programas del usuario que lo reciben, resultando en problemas de seguridad y permitiendo la ejecución de aplicaciones de forma remota por parte del hacker, extracción y robo de información etc.

A continuación, se detallan los tipos de tráfico mal formado soportados y una explicación de cada uno de ellos:

Campo	Descripción
IP explicit path	Rechaza los paquetes IP que tengan la opción de "explicit route". Son paquetes IP que no se encaminan en función de su dirección IP de destino, en su lugar la información de encaminamiento es fijada de ante mano.
Land Attack	Comprueba intentos de denegación de servicios mediante bucles infinitos de pila TCP/IP al detectar paquetes con direcciones origen y destino iguales.
SYN flood	Controla los el numero de inicios de conexiones TCP por segundo para no comprometer los recursos del equipo atacado. Pasado cierto limite las conexiones se rechazan.
TCP Port Scan	Detecta conexiones simultáneas a varios puertos del equipo protegido en un tiempo determinado y filtra tanto la petición de apertura como la respuesta al equipo sospechoso, para que el origen del tráfico de escaneo no obtenga información del estado de los puertos.
TCP Flags Check	Detecta paquetes TCP con combinaciones de flags inválidas. Actúa como complemento a las defensas de "Port Scanning" al detener ataques de este tipo, tales como "SYN & FIN" y "NULL FLAGS" y los de "OS identification" ya que muchas de estas pruebas se basan en respuesta a paquetes TCP inválidos.

Tabla 12.15: tipos de tráfico mal formado soportados

Campo	Descripción
Header lengths	• **IP**: rechaza los paquetes entrantes con un tamaño de cabecera IP que se salga de los límites establecidos. • **TCP**: rechaza los paquetes entrantes con un tamaño de cabecera TCP que se salga de los límites establecidos. • **Fragmentation control**: comprueba el estado de los fragmentos de los paquetes a reensamblar, protegiendo al equipo de ataques por consumo excesivo de memoria en ausencia de fragmentos, del redireccionado de ICMP disfrazado de UDP y del escaneo de equipos.
UDP Flood	Rechaza los paquetes UDP que llegan a un determinado puerto si superan un limite en un periodo establecido.
UDP Port Scan	Protección contra escaneo de puertos UDP.
Smart WINS	Rechaza las respuestas WINS que no se corresponden con peticiones que el equipo ha solicitado.
Smart DNS	Rechaza las respuestas DNS que no se corresponden con peticiones que el equipo ha solicitado.
Smart DHCP	Rechaza las respuestas DHCP que no se corresponden con peticiones que el equipo ha solicitado.
ICMP Attack	• **SmallPMTU**: detecta valores inválidos en el tamaño de los paquetes ICMP para generar una denegación de servicio o ralentizar el tráfico saliente. • **SMURF**: rechaza las respuestas ICMP no solicitadas si estás superan un limite en un intervalo. Este tipo de ataque envía grandes cantidades de tráfico ICMP (echo request) a la dirección de broadcast de la red con la dirección de origen cambiada (spoofing) apuntando a la dirección de la víctima. La mayoría de los equipos de la red responderán a la víctima, multiplicando el tráfico por cada equipo de la subred. • **Drop unsolicited ICMP replies**: rechaza todas las respuestas ICMP no solicitadas o que han expirado por el timeout establecido.
ICMP Filter echo request	Rechaza las peticiones de Echo request.
Smart ARP	Rechaza las respuestas ARP que no se corresponden con peticiones que el equipo protegido ha solicitado para evitar escenarios de tipo ARP caché poison.
OS Detection	Falsea datos para engañar a los detectores de sistemas operativos y así evitar posteriores ataques dirigidos a aprovechar las vulnerabilidades asociadas al sistema operativo detectado. Esta defensa se complementa con la de "TCP Flags Check".

Tabla 12.15: tipos de tráfico mal formado soportados

Informar de todos los bloqueos del firewall

Envía la información de los bloqueos producidos por el módulo de firewall a la nube de Cytomic EPDR para presentarlos en los listados. Solo se reportarán los bloqueos producidos por las reglas configuradas por el administrador desde la consola web.

El firewall utiliza la información mostrada a continuación de cada conexión bloqueada para agrupar las notificaciones antes de enviarlas al servidor de Cytomic:

- Equipo
- Aplicación bloqueada
- Sentido
- Regla
- Fecha de bloqueo

Si se producen varios bloqueos en el intervalo de una hora de las conexiones gestionadas por una aplicación, con un mismo sentido, y que además han sido bloqueados por una misma regla, se agruparán en una única entrada en el listado.

*Consulta el apartado "**Listado de Conexiones bloqueadas**" en la página **427**.*

Control de dispositivos (Equipos Windows)

Dispositivos de uso común como llaves USB, unidades de CD/DVD, dispositivos de imágenes, bluetooth, módems o teléfonos móviles son una vía de infección muy común para los equipos de la red.

Control de dispositivos define el comportamiento del equipo protegido al conectar u operar con un dispositivo extraíble o de almacenamiento masivo. Para ello, hay que seleccionar el dispositivo o dispositivos autorizados y asignar un nivel de utilización.

Activar el control de dispositivos

- Marca la casilla **Activar control de dispositivos.**
- Elige en el desplegable correspondiente el nivel de autorización a aplicar para el tipo de dispositivo a limitar su uso.
  - En el caso de las llaves USB y las unidades CD/DVD elige entre **Bloquear**, **Permitir lectura** o **Permitir lectura y escritura**.
  - Para Bluetooth, dispositivos de imágenes, módems USB y teléfono móviles las opciones son **Permitir y Bloquear**.

Dispositivos permitidos

Gestiona mediante una lista blanca aquellos dispositivos individuales que sí están permitidos cuando toda su familia esté bloqueada:

- Haz clic en icono ⊕ de **Equipos permitidos** para mostrar un listado con todos los dispositivos conectados a los equipos del parque informático.
- Elige aquellos que quieras excluir del bloqueo general previamente configurado.
- Borra con el botón 🗑 exclusiones ya creadas.

Exportar e importar listas de dispositivos permitidos

Despliega las opciones de **Exportar** e **Importar** del menú de contexto ⋮.

Obtener del identificador único del dispositivo

Para utilizar gestionar dispositivos sin esperar a que el usuario los conecte a su equipo para poder excluirlos de forma manual es necesario obtener el identificador de estos dispositivos:

- En el Administrador de dispositivos de Windows, accede a las propiedades del dispositivo USB que quieres identificar de forma única para excluirlo.
- Accede a la pestaña Detalles y selecciona la propiedad Recursos en el desplegable Propiedad. A continuación, debería mostrarse un valor llamado CM_DEVCAP_UNIQUEID.
- De nuevo en el desplegable Propiedad, selecciona Ruta de acceso a instancia del dispositivo y obtendrás el identificador único de dispositivo.

En el supuesto de que no se muestre ningún valor denominado CM_DEVCAP_UNIQUEID, no será posible obtener el identificador del dispositivo. En este caso puedes utilizar como identificador el correspondiente al hardware del dispositivo: en el desplegable Propiedad, selecciona Identificador de hardware y se mostrará el identificador correspondiente.

Este identificador no identifica de forma única a cada dispositivo, sino que representa a todos los dispositivos de la misma gama.

Apunta todos los identificadores de dispositivo en un fichero de texto según el apartado "**Exportar e importar listas de dispositivos permitidos**".

Control de acceso a páginas web

Con esta protección el administrador de la red restringe el acceso a determinadas categorías Web y a URLs individuales a las que autoriza o restringe el acceso. Esta estrategia optimiza del ancho de banda de la red y mejora la productividad en la empresa.

Para activar o desactivar el control de acceso páginas web haz clic en el botón **Activar el control de acceso a páginas web**.

Configurar horarios del control de accesos a páginas Web

Restringe el acceso a determinadas categorías de páginas Web y listas negras durante las horas de trabajo, y autorízalo en horario no laborable o en el fin de semana.

Para activar el control horario de accesos a páginas Web elige la opción **Activar solo durante las siguientes horas**.

A continuación, selecciona las horas en las que el control horario estará activado. Para activarlo sólo en un horario determinado, marca la casilla correspondiente y utiliza la cuadrícula para señalar las horas.

- Para seleccionar días completos haz clic en el día de la semana.
- Para seleccionar una misma hora en todos los días de la semana haz clic en la hora.
- Para seleccionar todos los días del mes haz clic en el botón **Seleccionar todo**.
- Para limpiar toda la selección y comenzar de cero, haz clic en el botón **Vaciar**.

Denegar el acceso a páginas Web

Cytomic EPDR agrupa las páginas web en categorías. Para impedir la navegación de paginas web selecciona la categoría o categorías a las que pertenecen.

Cuando el usuario visite una página Web que pertenezca a una categoría denegada, se mostrará en su navegador un aviso indicando el motivo.

Denegar el acceso a páginas de categoría desconocida

Para denegar el acceso a páginas no categorizadas haz clic en el botón de activación **Denegar acceso a las páginas cuya categoría sea desconocida**.

Las webs internas o alojadas en intranets y accesibles a través de los puertos 80 u 8080 pueden ser clasificadas como pertenecientes a una categoría desconocida, y por tanto ser denegado su acceso. Añade las páginas Web desconocidas que sean necesarias a la lista blanca de exclusiones para evitar esta situación.

Lista de direcciones y dominios permitidos o denegados

Especifica mediante una lista blanca las páginas web a las que siempre se permite acceder, y mediante una lista negra las páginas a las que nuca se permite, independientemente de la categoría a la que pertenezcan:

- Introduce en la caja de texto la URL del dominio o dirección.
- Haz clic en **Añadir**.
- Utiliza los botones **Eliminar** y **Vaciar** para modificar la lista.
- Finalmente, haz clic en **Aceptar** para guardar la configuración.

La coincidencia de las URLs indicadas en lista blanca y lista negra puede ser completa o parcial. En caso de URLs largas es suficiente con indicar el comienzo de la URL para obtener una coincidencia.

Base de datos de URLs accedidas desde los equipos

Cada equipo de la red recopila información sobre las URLs visitadas. Esta información solo se puede consultar desde el propio equipo durante un plazo de 30 días.

Los datos almacenados son:

- Identificador del usuario.
- Protocolo (http o https).
- Dominio.
- URL.
- Categorías devueltas.
- Acción (Permitir/Denegar).
- Fecha de acceso.
- Contador acumulado de accesos por categoría y dominio.

Antivirus para servidores Exchange

Para activar la protección de servidores Exchange es necesario disponer de un número de licencias igual a la cantidad de buzones en la compañía que requieren protección.

La protección para servidores Exchange es aplicable a las versiones 2003, 2007, 2010, 2013, 2016 y 2019, y está formada por tres módulos:

- Antivirus
- Anti-spam
- Filtrado de contenidos

Configuración de la protección Antivirus según el modo de análisis

Según el momento en el que Cytomic EPDR efectúa el análisis dentro del flujo de correo, se distinguen dos formas de protección: protección de buzones y protección de transporte.

La tabla **12.16** muestra las combinaciones de módulo de protección, modo de análisis y versiones de Exchange soportados.

Módulo de protección / modo de análisis	Antivirus	Antispam	Filtrado de contenidos
Buzón	2003, 2007, 2010	NO	NO
Transporte	2003, 2007, 2010, 2013, 2016, 2019	2003, 2007, 2010, 2013, 2016, 2019	2003, 2007, 2010, 2013, 2016, 2019

Tabla 12.16: módulos de protección, modos de análisis y versiones Microsoft Exchange soportadas

Protección de buzones

Se utiliza en los servidores Exchange con el rol de Mailbox y analiza las carpetas / buzones en segundo plano o cuando el mensaje es recibido y almacenado en la carpeta del usuario.

La protección de buzones es compatible con el módulo Antivirus en los servidores Microsoft Exchange 2003, 2007 y 2010.

Cytomic EPDR ejecuta la acción configurada ante la detección de un elemento clasificado como malware: desinfectar el adjunto si es posible o introducirlo en cuarentena si no es posible. El usuario protegido con Cytomic EPDR recibirá el mensaje original con los adjuntos desinfectados o, en caso de que no fuera posible su desinfección, con un fichero "`security_alert.txt`" adjuntado describiendo el motivo de la detección.

Protección de transporte

Se utiliza en servidores Exchange con el rol de Acceso de clientes, Edge Transport y Hub, y analiza el tráfico que atraviesa al servidor Microsoft Exchange en busca de virus, herramientas de hacking y programas potencialmente no deseados sospechosos, con destino a buzones situados en el servidor Exchange.

La protección de transporte es compatible con todas las versiones de Microsoft Exchange desde 2003 y no permite manipular los mensajes analizados; si el correo contiene un elemento peligroso se introduce íntegro en cuarentena. El usuario protegido con Cytomic EPDR recibirá un mensaje con el asunto original, pero con el cuerpo sustituido por un mensaje de advertencia indicando que, en caso de querer recuperar el mensaje original, contacte con el administrador de la red.

Software a detectar

Haz clic en los botones de activación para detectar diferentes tipos de amenazas:

- Detectar virus
- Detectar herramientas de hacking y PUPs

Escaneo inteligente de buzones

El escaneo inteligente de buzones aprovecha los momentos de baja actividad del servidor Exchange para examinar los correos almacenados en sus buzones. Además, sólo comprueba los archivos que no han sido previamente analizados con el fichero de firmas descargado. Cuando el fichero de firmas se actualiza, Cytomic EPDR lanzará otro escaneo inteligente de buzones de forma automática.

Restauración de mensajes con virus y otras amenazas

Configura el servidor SMTP que reenviará los mensajes restaurados desde la consola de administración. Para ello completa los siguientes campos:

Campo	Descripción
Servidor SMTP	Dirección IP o dominio del servidor de correo.
El servidor requiere autenticación	Haz clic en el botón de activación si el servidor SMTP no es "open relay".
Usuario	Cuenta de usuario con permisos para enviar correos en el servidor.
Contraseña	Contraseña de la cuenta de usuario con permisos para enviar correos en el servidor.

Tabla 12.17: configuración del servidor de correo para el reenvío de mensajes con amenazas detectadas

Si no se configura ningún servidor SMTP, los mensajes se restaurarán en una carpeta del disco duro del servidor Exchange.

Anti spam para servidores Exchange

Para activar o desactivar esta protección, utiliza el botón de activación **Detectar Spam**.

Al activar la protección Anti Spam Cytomic EPDR muestra una ventana emergente sugiriendo añadir varias reglas de exclusión para mejorar el rendimiento del servidor de correo.

Acción para mensajes de spam

Selecciona la acción a realizar con los mensajes de spam:

Acción	Descripción
Dejar pasar el mensaje	Añade la etiqueta Spam al asunto de los mensajes. Esta será la opción configurada por defecto.
Mover el mensaje a...	Reenvía el mensaje a la dirección de correo electrónico especificada y añade la etiqueta Spam al asunto.
Borrar el mensaje	Borra el mensaje del servidor de correo.
Marcar con SCL (Spam Confidence Level)	SCL es una marca que el módulo de protección anti spam añade a las cabeceras de los mensajes de correo, y que representa la probabilidad de que el mensaje sea spam a través de una escala comprendida entre el 0 y el 9, ordenada de menor a mayor probabilidad. Cytomic EPDR no ejecuta ninguna acción sobre los mensajes marcados con SCL, que se tratarán posteriormente en función del umbral configurado en el Directorio Activo por el administrador de la red.

Tabla 12.18: acciones permitidas por Cytomic EPDR frente a los mensajes de spam

Direcciones y dominios permitidos

Son direcciones y dominios cuyos mensajes no serán analizados por la protección anti-spam (lista blanca).

Añade varias direcciones y dominios separados por el carácter ",".

Direcciones y dominios de spam

Son dominios y direcciones cuyos mensajes serán interceptados por la protección y eliminados (lista negra).

Al configurar las listas es importante tener en cuenta:

- Si un dominio se encuentra en lista negra y una dirección que pertenece a dicho dominio se encuentra en lista blanca, se permitirá dicha dirección, pero no el resto de direcciones del dominio.
- Si un dominio se encuentra en lista blanca y una dirección que pertenece a dicho dominio se encuentra en lista negra, dicha dirección no será aceptada, pero sí el resto de direcciones de dicho dominio.
- Si un dominio se encuentra en lista negra y un subdominio de este se encuentra en lista blanca, se permitirán direcciones de dicho subdominio, pero no el resto de direcciones del dominio o de otros subdominios diferentes.
- Si un dominio se encuentra en lista blanca también se consideran incluidos en lista blanca todos sus subdominios.

Filtrado de contenidos para servidores Exchange

Filtra los mensajes de correo electrónico en función de la extensión de los archivos adjuntos incluidos en ellos.

Una vez establecida la lista de mensajes susceptibles de albergar adjuntos sospechosos, indica qué acción ejecutará la protección sobre ellos:

Acción	Descripción
Acción a realizar	Borra los mensajes o los desvía a otra dirección de correo electrónico para analizar posteriormente los adjuntos recibidos.
Considerar archivos adjuntos peligrosos los que tienen las siguientes extensiones	Considera como peligrosos los archivos adjuntos con alguna extensión concreta. Una vez marcada la casilla, utiliza los botones **Añadir**, **Eliminar**, **Vaciar** o **Restaurar** para configurar la lista de extensiones a bloquear.
Considerar archivos adjuntos peligrosos todos los que tienen doble extensión, excepto en los siguientes casos	Impide la entrada de todos los mensajes de correo electrónico con adjuntos de doble extensión, excepto aquellos que tengan las extensiones seleccionadas. Utiliza los botones **Añadir**, **Eliminar**, **Vaciar** o **Restaurar** para configurar la lista de dobles extensiones permitidas.

Tabla 12.19: acciones permitidas por el filtrado de contenidos para servidores Microsoft Exchange

Registro de detecciones

Todas las detecciones producidas en un servidor Exchange son almacenadas localmente en un archivo CSV con información adicional acerca de la imposibilidad de entrega de los mensajes a sus destinatarios.

El fichero recibe el nombre `ExchangeLogDetections.csv` y se almacena en la carpeta:

```
%ProgramData%\Panda Security\Panda Security Protection\Exchange
```

excepto en Windows 2003 que se almacena en la carpeta:

```
%AllUsersProfile%\Panda Security\Panda Security Protection\Exchange
```

El contenido del fichero se ordena en formato tabular con la siguiente distribución de campos:

Campo	Descripción
Date	Fecha de la llegada del correo al servidor Exchange.
From	Origen del mensaje de correo.
To	Destinatario del mensaje de correo.
Subjet	Asunto del mensaje de correo.

Tabla 12.20: campos del fichero ExchangeLogDetections

Campo	Descripción
Attachments	Listado con los ficheros adjuntos al correo.
Protection	Módulo de protección que desencadenó la acción ejecutada sobre el mensaje. • AntiSpam • Content Filter • Antimalware
Action	Acción ejecutada sobre el mensaje. • Borrado • Modificado • SCL Tagged

Tabla 12.20: campos del fichero ExchangeLogDetections

Capítulo 13

Configuración de seguridad Android

Cytomic EPDR centraliza en el menú superior **Configuración** toda la configuración de los parámetros de seguridad para smartphones y tablets. Haz clic en el panel de la izquierda **Dispositivos Android** para mostrar un listado con todas las configuraciones de seguridad ya creadas o para crear nuevas.

En este capítulo se muestran todos los parámetros incluidos en la configuración de seguridad y antirrobo para dispositivos Android y se indican algunas recomendaciones prácticas para asegurar móviles y tablets, minimizando los inconvenientes en su manejo al usuario.

CONTENIDO DEL CAPÍTULO

Introducción a la configuración de dispositivos Android

La configuración para dispositivos Android se divide en varios secciones. Al hacer clic en cada uno de ellas se mostrará un desplegable con su configuración asociada. A continuación, se muestran las secciones con una breve explicación:

- **Actualizaciones**: establece el tipo de conexión que utilizará el dispositivo para descargar las actualizaciones de la nube de Cytomic.
- **Antivirus**: establece la configuración del antivirus.
- **Antirrobo**: establece la activación de la gestión remota del dispositivo en caso de robo o perdida, para minimizar la exposición de los datos contenidos en el mismo.

Actualización

*La configuración de las actualizaciones se describe en el capítulo "**Actualización del software cliente**" en la página **143**.*

Antivirus

La protección antivirus para smartphones Android analiza bajo demanda o de forma permanente tanto el dispositivo móvil como las tarjetas de memoria SD conectadas para proteger a móviles y tablets frente a la instalación de aplicaciones con malware y PUPs.

Haz clic en el botón de activación **Activar protección permanente antivirus** para activar la detección de malware.

Exclusiones

Excluye del análisis las aplicaciones instaladas. Introduce los nombres de los paquetes a excluir separados por el carácter ",".

Para localizar el nombre del paquete correspondiente a una aplicación instalada búscala en la Google Play. En la URL de su ficha se mostrará el parámetro `'?id='`, que contiene la cadena que identifica de forma única a la aplicación.

Antirrobo

La configuración de antirrobo permite enviar acciones a los dispositivos para evitar la filtración de los datos que contienen o favorecer su localización en caso de pérdida o robo del terminal.

Haz clic en el selector **Protección antirrobo** para activar la funcionalidad.

*Consulta el apartado "**Sección general en dispositivos Android**" en la página **184** para obtener información sobre las acciones antirrobo disponibles en Cytomic EPDR.*

Comportamiento

Establece las funcionalidades antirrobo del dispositivo Android:

Campo	Descripción
Informar de la localización del dispositivo	El dispositivo envía sus coordenadas GPS al servidor Cytomic EPDR.

Tabla 13.1: funcionalidades antirrobo de dispositivos Android

Campo	Descripción
Sacar foto al tercer intento de desbloqueo y enviarla por email	Si el usuario del dispositivo falla tres veces consecutivas al desbloquearlo se tomará una fotografía y se enviará por correo electrónico a las direcciones de correo separadas por coma introducidas en la caja de texto.

Tabla 13.1: funcionalidades antirrobo de dispositivos Android

Privacidad

Permite al usuario activar el modo privacidad, que impide la toma de fotografías y el registro de las coordenadas GPS del dispositivo y posterior envío al servidor de Cytomic EPDR.

Capítulo 14

Cytomic Data Watch (Supervisión de información sensible)

Los ficheros clasificados como PII (Personally Identificable Information) son archivos sin estructura interna que contienen información que identifica a personas relacionadas con la empresa (clientes, trabajadores, proveedores etc.). Esta información es de carácter personal y su tipo es muy variado, entre los que se cuentan números de la seguridad social, números de teléfono y direcciones de correo electrónico, entre otros.

Cytomic Data Watch es el módulo de seguridad de Cytomic EPDR que ayuda a cumplir con las regulaciones sobre protección de datos tales como la GDPR, y a dar visibilidad y supervisar la información personal (PII) almacenada en la infraestructura IT de las empresas.

Para ello, Cytomic Data Watch ofrece tres funcionalidades clave:

- Genera un inventario diario y completo de ficheros PII que incluye información básica, como pude ser su nombre, extensión y el nombre del equipo donde se encontró.
- Descubre, audita y monitoriza en tiempo real el ciclo de vida de los ficheros PII: desde los datos en reposo, las operaciones efectuadas sobre ellos y su llegada y comunicación hacia el exterior.
- Ofrece herramientas de búsqueda flexible por contenido y borrado de ficheros duplicados que contienen datos personales con el objetivo de limitar su almacenamiento y difusión en la red de la empresa.

Consulta la Guía de administración de Cytomic Data Watch para obtener más información sobre la consola de gestión específica para este servicio.

CONTENIDO DEL CAPÍTULO

Introducción al funcionamiento de Cytomic Data Watch

Para una correcta comprensión de los procesos involucrados en el descubrimiento y seguimiento de la información personal almacenada en los equipos de la empresa, es necesario asimilar algunos conceptos relativos a las tecnologías utilizadas en Cytomic Data Watch.

Entidad

Cada pieza o grupo de palabras con significado propio referido a un tipo concreto de información personal recibe el nombre de "entidad". Entidades comúnmente analizadas son el DNI, nombres y apellidos y números de teléfono entre otras.

Debido a la naturaleza ambigua y variable del lenguaje natural en sus múltiples idiomas, una misma entidad puede presentarse de formas muy diferentes, por lo que es necesario aplicar algoritmos flexibles y adaptables para su detección. De manera general, el análisis de entidades aplica formatos o expresiones predefinidas, y utiliza el contexto local en torno a esa detección o la presencia o ausencia de determinadas palabras clave para evitar falsos positivos. Consulta el apartado "**Entidades y países soportados**".

Fichero PII

Una vez realizada la identificación de entidades se evalúa el contexto en el que aparecen para determinar si con la información que aportan es posible identificar a una persona concreta. En tal caso el fichero será susceptible de ser protegido por protocolos específicos de tratamiento y acceso a los datos que permitan a la empresa cumplir con la normativa vigente (GDPR, PCI etc.). Esta evaluación combina un modelo Machine learning supervisado y un modelo experto basado en

ponderación de entidades y análisis del contexto global del documento para finalmente clasificar a un fichero con entidades detectadas como un fichero PII a proteger.

Ficheros sin estructura interna y componentes IFilter

Cytomic Data Watch analiza archivos sin estructura (ficheros de texto en múltiples formatos, hojas de cálculo, ficheros de presentación Powerpoint etc.) en busca de entidades para clasificarlos como ficheros PII. Para interpretar correctamente el contenido de este tipo de archivos se requieren ciertos componentes de terceros instalados en el equipo del usuario. Estos componentes reciben el nombre de "IFilters" y no forman parte del paquete de instalación de Cytomic EPDR. Microsoft Search, Microsoft Exchange Server y Microsoft Sharepoint Server entre otros servicios del sistema operativo y productos independientes utilizan los componentes IFilter para indexar los ficheros del usuario y habilitar su búsqueda por contenido.

Cada formato de fichero compatible tiene su propio componente IFilter asociado, y muchos de ellos vienen ya preinstalados en la instalación básica de Windows, aunque otros tienen que ser instalados o actualizados de forma manual.

Microsoft Filter Pack es un paquete de distribución gratuito que contiene todos los componentes IFilter asociados a la suite de ofimática Microsoft Office. Una vez instalado, Cytomic Data Watch será capaz de analizar el contenido de todos los formatos de fichero soportados por la suite. Consulta el apartado "**Instalación del componente Microsoft Filter Pack**".

Proceso de indexación

Es el proceso de inspección y almacenaje del contenido de todos los ficheros soportados por Cytomic Data Watch para poder generar el inventario de ficheros PII y permitir búsquedas de ficheros por su contenido. El proceso de indexación es una tarea de bajo impacto en el rendimiento del equipo, aunque su finalización puede alargarse en el tiempo. Por esta razón el administrador puede programar su inicio o limitarla para acelerar su finalización y para mejorar el resultado de los resultados devueltos por las búsquedas. Consulta el apartado "**El proceso de indexación**".

Proceso de normalización

Al ejecutar el proceso de indexación Cytomic Data Watch aplica ciertas reglas para homogeneizar los datos recogidos. El objetivo de este proceso es almacenar de forma individual cada palabra y facilitar su posterior búsqueda, así como reducir su tiempo de ejecución. La reglas a aplicar en el proceso de normalización varían si se trata de almacenar una entidad o texto plano. Consulta el apartado "**Proceso de normalización**".

Inventario de ficheros PII

Una vez indexado el equipo e identificadas las entidades y los ficheros PII, Cytomic Data Watch construye un inventario accesible por el administrador de la red con los nombres de los ficheros y sus

características, que se envía al servidor Cytomic EPDR una vez al día. Consulta el apartado "**Para acceder al widget Búsquedas haz clic en el menú superior Estado, panel lateral Data Control.**".

> *Cytomic Data Watch no envía el contenido de los ficheros PII al servidor Cytomic EPDR. Unicamente se envían sus atributos (nombre, extensión etc.) y el número y tipo de entidades descubiertas.*

Búsquedas de ficheros

Cytomic Data Watch localiza ficheros por su nombre, extensión o contenido en las unidades de almacenamiento indexadas de los equipos de la red.

Las búsquedas se ejecutan en tiempo real: tan pronto como el administrador lanza una búsqueda, ésta se despliega en los equipos de la red y comienza a reportar resultados conforme se van produciendo, sin esperar a completar la ejecución por completo. Consulta "**Búsqueda de ficheros**".

Seguimiento de las acciones sobre ficheros PII

Cytomic Data Watch monitoriza los eventos realizadas sobre los ficheros PII y los envía a la consola Advanced Visualization Tools. Esta herramienta muestra la evolución de los ficheros PII permitiendo determinar si fueron copiados, movidos, enviados por correo, etc. Para obtener más información sobre Advanced Visualization Tools consulta la Guía para el usuario de Cytomic Data Watch en **https://info.cytomicmodel.com/guides/DataWatch/es/DATAWATCH-guia-ES.pdf**

Requisitos de Cytomic Data Watch

Plataformas soportadas

Cytomic Data Watch es compatible con la plataforma Microsoft Windows desde la versión XP SP3 en adelante y Windows 2003 SP1 y superiores. Otros sistemas operativos como Linux o macOS no están soportados.

Instalación del componente Microsoft Filter Pack

Microsoft Filter Pack y Microsoft Office

El componente Microsoft Filter Pack viene incluido en la suite de ofimática Office, aunque solo se instalarán de forma automática los componentes IFilter que se corresponden con los productos de la suite instalados en el equipo del usuario. Para tener la seguridad de que todos los componentes estén disponibles en el equipo en su versión 2010, consulta el punto "**Instalación independiente del Microsoft Filter Pack**".

Instalación independiente del Microsoft Filter Pack

Para instalar el Microsoft Filter Pack haz clic en la siguiente URL:

https://www.microsoft.com/en-us/download/details.aspx?id=17062

El paquete es compatible con Windows XP SP3, Windows 2013 SP1 y superiores, aunque en algunos casos se requerirá la instalación de la librería Microsoft Core XML Services 6.0.

El proceso de indexación

Es el proceso de inspección y almacenaje del contenido de todos los ficheros soportados por Cytomic Data Watch. Este proceso es imprescindible para poder generar el inventario de ficheros PII y también para buscar ficheros en los equipos por su contenido. El proceso de indexación se configura de forma transparente al activar alguna de estas dos funcionalidades. La información indexada se almacena de forma local en el equipo de cada usuario en la ruta `%ProgramData%\Panda Security\Panda Security Protection\indexstore`.

Aunque el proceso de indexado es una tarea de bajo impacto en el rendimiento del equipo, ésta puede alargarse en el tiempo. Por esta razón, Cytomic Data Watch está configurado para lanzar una única vez el proceso en el momento en que se activa el módulo en cada equipo de la red, y cada vez que la tecnología de detección de entidades cambie para soportar mejoras.

Una vez terminada la indexación, Cytomic Data Watch monitoriza la creación de nuevos ficheros y el borrado y modificación de los ficheros ya existentes para actualizar el índice y enviar al servidor Cytomic EPDR cada 24 horas las nuevas entidades detectadas.

Configurar el alcance, momento y tipo de indexación

Es posible excluir los resultados de ciertas carpetas o ficheros, o incluso variar la precisión de las búsquedas devueltas por Cytomic Data Watch.

- Para no devolver información de ciertas carpetas o ficheros consulta el apartado "**Contenido recuperado en el proceso de indexación**".
- Para variar la precisión de las búsquedas consulta el apartado "**Contenido recuperado en el proceso de indexación**" en la página **276**.
- Para determinar la franja horaria en la que se ejecutará el proceso de indexado consulta el apartado "**Programar períodos de indexación**"

Inventario de ficheros PII

> *Cytomic Data Watch no envía el contenido de los ficheros PII al servidor Cytomic EPDR. Únicamente se envían sus atributos (nombre, extensión etc.) y el número y tipo de entidades descubiertas.*

El inventario de ficheros PII muestra los ficheros PII que Cytomic Data Watch ha encontrado en la red del cliente.

Para activar el inventario consulta el apartado "**Activar el inventario de información personal.**".

Visualizar el inventario

Cytomic Data Watch incorpora varios recursos para controlar los ficheros PII encontrados en la red y determinar el tipo de entidades que contienen.

- Para obtener estadísticas del número de ficheros PII encontrados consulta el apartado "**Archivos con información personal**" en la página **284**.
- Para obtener estadísticas del número de equipos con ficheros PII encontrados consulta el apartado "**Equipos con información personal**" en la página **285**.
- Para obtener un listado con el detalle de los ficheros PII encontrados consulta el apartado "**Listado Archivos con información personal**" en la página **293**.
- Para obtener un listado con el detalle de los equipos que contienen ficheros PII consulta el apartado "**Listado Equipos con información personal**" en la página **296**.

Monitorización continua de ficheros PII

Cytomic Data Watch recopila todos los eventos relativos a la creación, modificación o borrado de ficheros PII para poder visualizar la actividad realizada sobre estos ficheros y detectar situaciones peligrosas tales como robo de datos, acceso no autorizada a información etc.

- Para activar la monitorización de las acciones efectuadas sobre los ficheros PII consulta el apartado "**Activar el seguimiento de información personal**".
- Para visualizar las acciones realizadas sobre los ficheros PII accede a Advanced Visualization Tools desde la parte inferior del panel lateral del menú superior **Estado**. Consulta la Guía para el usuario de Cytomic Data Watch en **https://info.cytomicmodel.com/guides/DataWatch/es/DATAWATCH-guia-ES.pdf** para obtener toda la información necesaria.

Búsqueda de ficheros

Requisitos de las búsquedas

Para realizar una búsqueda en los ficheros almacenados en los equipos de la red es necesario cumplir con los siguientes requisitos:

- La cuenta de usuario que lanza la búsqueda desde la consola web tiene que tener asignado un rol con el permiso **Buscar información en los equipos**. Consulta el capítulo "**Control y supervisión de la consola de administración**" en la página 69 para obtener más información sobre los roles.
- Los equipos sobre los que se efectúan las búsquedas deben de contar con una licencia de Cytomic Data Watch asignada.
- Los equipos sobre los que se efectúan las búsquedas deben de tener asignada una configuración de Data Control con la opción **Permitir realizar búsquedas de información en los equipos** habilitada. Consulta el apartado "**Configuración de Data Control**".

Widget de búsquedas

Es el punto de entrada para toda la funcionalidad. Permite visualizar las búsquedas y gestionarlas.

Para acceder al widget **Búsquedas** haz clic en el menú superior **Estado**, panel lateral **Data Control**.

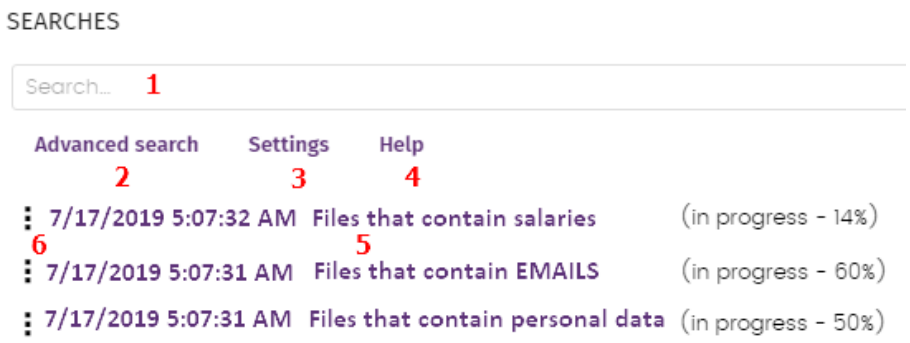


Figura 14.1: panel Búsquedas

El widget contiene los controles mostrados a continuación:

- **(1)** Caja de texto para introducir los términos a buscar. Consulta el apartado "**Sintaxis de las búsquedas**" para una descripción de los comandos aceptados por Cytomic Data Watch.
- **(2) Búsqueda avanzada**: limita el ámbito de búsqueda.
- **(3) Configuración:** acceso al listado de perfiles de configuración de Cytomic Data Watch. Para más información consulta el apartado "**Configuración de Data Control**".
- **(4) Ayuda:** enlace a la página web de soporte de Cytomic donde se muestra la sintaxis de las búsquedas de Cytomic Data Watch actualizada con los últimos cambios introducidos.
- **(5) Búsquedas almacenadas:** búsquedas definidas anteriormente y que pueden ser relanzadas en el parque informático.
- **(6) Menú de contexto de la búsqueda**: permite editar el nombre de la búsqueda, cambiar sus

parámetros, volverla a lanzar y eliminarla.

Propiedades y requisitos de las búsquedas

Para completar con éxito una búsqueda es necesario cumplir con los siguientes requisitos:

- La cuenta de usuario que lanza la búsqueda desde la consola web tiene que tener asignado un rol con el permiso **Buscar información en los equipos**. Consulta el capítulo "**Control y supervisión de la consola de administración**" en la página **69** para obtener más información sobre los roles.
- Los equipos sobre los que se efectúan las búsquedas deben de contar con una licencia de Cytomic Data Watch asignada.
- Los equipos sobre los que se efectúan las búsquedas deben de tener asignada una configuración de Data Control con la opción **Permitir realizar búsquedas de información en los equipos** habilitada.

Propiedades de las búsquedas

- El número de búsquedas concurrentes en la consola de administración por cada cuenta de usuario es 10. Pasado este número se mostrará un mensaje de error en la consola.
- El número máximo de búsquedas guardadas por cuenta de usuario es 30. Pasado este número se mostrará un mensaje de error en la consola.
- El número máximo de resultados en total por cada búsqueda es 10.000. Los resultados más allá de este número no se mostrarán en la consola.
- El número máximo de resultados por cada equipo es 10.000 / número de equipos sobre los que se ejecuta la búsqueda. De esta forma, si se busca sobre un parque de 100 equipos, el número máximo de resultados mostrados será 10.000 / 100 = 100 resultados por equipo.
- El número mínimo de resultados mostrados por equipo, independientemente del número de equipos de la red es 10.
- El número máximo de equipos sobre los que se ejecutan búsquedas de forma simultánea es 50. Si el número total de equipos que participaran en la búsqueda es mayor, las búsquedas más allá del límite de 50 se mantendrán en espera hasta que las primeras se vayan completando.

Proceso de normalización

El proceso de normalización no influye en la detección de entidades.

Cytomic Data Watch aplica una serie de reglas a los datos recibidos del proceso de indexación para homogeneizarlos. Debido a que las búsquedas ejecutadas por el administrador se aplican sobre los datos ya normalizados, es necesario conocer estas reglas dado que pueden influir en los resultados mostrados en la consola.

- **Transformación de las cadenas a minúsculas**

Antes de almacenar una cadena en la base de datos, ésta se transforma a minúsculas.

- **Caracteres de separación**

Cytomic Data Watch detecta un grupo de caracteres especiales que considera como separadores entre palabras y que retira completamente del índice, excepto si esos caracteres forma parte de una entidad:

- **Retorno de carro**: `\r`
- **Salto de línea**: `\n`
- **Tabulador**: `\t`
- **Caracteres**: `" : ; ! ? - + _ * = ( ) [ ] { } , . | % \ / '`

Por ejemplo "`Cytomic.Data(Watch`" se almacenará como tres palabras sueltas sin los caracteres de puntuación: "`cytomic`", "`data`" y "`watch`".

- **Normalización de entidades**

El proceso de normalización de entidades sigue reglas independientes:

Entidad	Caracteres de separación	Configuración de la indexación
• Cuentas bancarias • Tarjetas de crédito • Número de identidad personal • Números de teléfono • Números de carnet de conducir • Números de pasaporte • Números de la seguridad social	Se eliminan. La entidad se almacena en el índice como un único grupo.	No se tiene en cuenta
• Direcciones IP • Direcciones de correo electrónico	Se respetan. La entidad se almacena en el índice como un único grupo.	No se tiene en cuenta
• Nombres y apellidos • Direcciones físicas	Se utilizan como carácter separador. La entidad se almacena en el índice como varios elementos.	Si se tiene en cuenta

Tabla 14.1: reglas de normalización de entidades

- **Ejemplos de normalización de entidades**
  - "1.42.67.116-C" se almacena como la entidad de tipo IDCARD "14267116C".
  - "192.168.1.1" se almacena como la entidad de tipo IP "192.168.1.1".

- "Calle Santiago de Compostela 5 1º Izquierda" se almacenará como "calle", "santiago", "de", "compostela", "izquierda" si el método de indexación es Solo texto o como "calle", "santiago", "de", "compostela", "5", "1", "izquierda" si el método de indexación es Todo.

Crear una búsqueda

Crear una búsqueda libre

- Haz clic en el menú superior **Estado**, panel lateral **Data Control.**
- Introduce en la caja de texto del widget **Búsquedas** los términos de búsqueda según la sintaxis mostrada en el apartado "**Sintaxis de las búsquedas**".
- Haz clic en el icono o pulsa la tecla Enter.

Una vez introducida la búsqueda se abrirá la ventana **Resultados de la búsqueda**. Consulta el apartado "**Búsquedas almacenadas**" para editar la búsqueda introducida.

Crear una búsqueda guiada

- Haz clic en el menú superior **Estado**, panel lateral **Data Control**.
- Haz clic en el enlace **Búsqueda avanzada**.
- Elige en el selector **Búsqueda guiada.**
- Configura los parámetros de la búsqueda.
- **Parámetros de búsqueda avanzada:**

Parámetro	Descripción
Nombre de la búsqueda	Establece un nombre para la búsqueda almacenada.
Buscar archivos con	Introduce el contenido a buscar. Se incluyen tres cajas de texto. • **Todas estas palabras o frases exactas**: busca los ficheros que contienen todas las palabras o entidades indicadas. • **Alguna de estas palabras o frases exactas**: busca los ficheros que contienen alguna o todas las palabras o entidades indicadas. • **Ninguna de estas palabras o frases exactas**: busca los ficheros que no contienen ninguna de las palabras.

Tabla 14.2: parámetros de la búsqueda avanzada

Parámetro	Descripción
Información personal	Marca las casillas de selección para indicar las entidades que deberán de aparecer en los ficheros PII buscados. • **Todos**: todas las entidades seleccionadas deberán de detectarse en el fichero PII (lógica AND) para que el fichero se incluya en la lista de encontrados. • **Alguno**: algunas o todas las entidades seleccionadas deberán de detectarse en el fichero PII (lógica OR) para que el fichero se incluya en la lista de encontrados.
Limitar la búsqueda a	**Equipos**: • **Todos**: busca el contenido introducido en todos los equipos que tengan una licencia de Cytomic Data Watch asignada y esté habilitada la opción de búsqueda en su configuración. • **Los siguientes equipos**: muestra un listado de los equipos que tengan una licencia de Cytomic Data Watch asignada. Indica con las casillas de selección los equipos en los que se buscará el contenido introducido. • **Los siguientes grupos de equipos**: muestra el árbol de carpetas con la jerarquía de equipos configurada en Cytomic EPDR. Indica con la casilla de selección los grupos donde se buscará el contenido introducido.
Cancelar automáticamente la búsqueda	Indica el tiempo de espera para los equipos apagados o sin conexión antes de cancelar la búsqueda.

Tabla 14.2: parámetros de la búsqueda avanzada

Búsquedas almacenadas

Tanto las búsquedas libres como las guiadas se almacenan para poder ser lanzadas posteriormente de forma rápida.

Una vez creada una nueva búsqueda, ésta aparecerá en el widget **Búsquedas** con la fecha y hora de su creación, junto al nombre y una leyenda indicando su estado (**En curso**, **Cancelada**) o sin estado (**Finalizada**).

Cambiar el nombre de una búsqueda almacenada

Haz clic en el menú de contexto (**6** en la figura 14.1) de la búsqueda y elige **Cambiar nombre**.

Hacer una copia de una búsqueda almacenada

Para duplicar una búsqueda almacenada haz clic en el menú de contexto (**6** en la figura 14.1) de la búsqueda y elige **Hacer una copia**. Se mostrará la ventana de configuración de la búsqueda y se renombrará a "Copia de ".

Volver a lanzar una búsqueda almacenada

Haz clic en el menú de contexto de la búsqueda (**6** en la figura 14.1) y elige **Relanzar búsqueda**. El estado de la búsqueda cambiará e indicará el porcentaje de la tarea realizada.

Cancelar y eliminar búsquedas almacenadas

Haz clic en el menú de contexto de la búsqueda (**6** en la figura 14.1) y elige **Cancelar** para interrumpir la búsqueda o en **Borrar** para cancelarla y borrarla del widget **Búsquedas**.

Editar búsquedas almacenadas

Haz clic en el menú de contexto (**6** en la figura 14.1) y elige **Editar búsqueda** para abrir la ventana de búsqueda avanzada con sus parámetros cargados y modificarla.

Visualizar los resultados de una búsqueda

Para visualizar el resultado de una búsqueda accede al listado **Buscar en los equipos** de dos formas:

- Haciendo clic en una búsqueda almacenada.
- Creando una nueva búsqueda.

Este listado muestra los equipos que contienen la cadena de búsqueda introducida, junto al nombre del fichero encontrado y otra información útil.

- **Cabecera de listado**

Configura los parámetros de la búsqueda rápida:

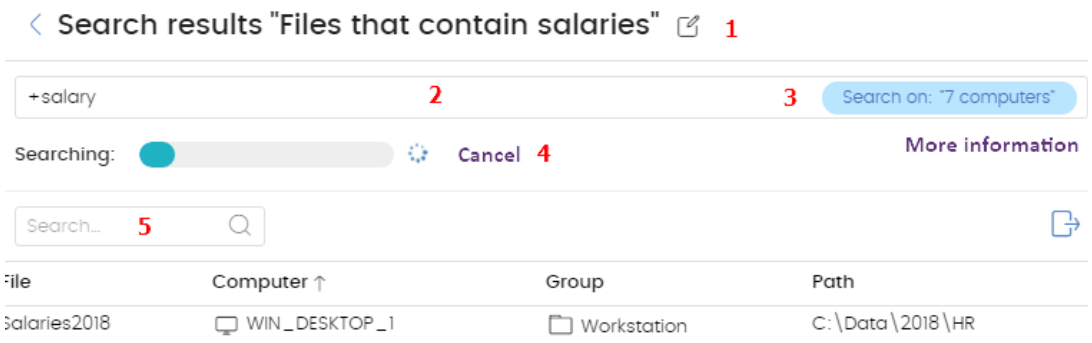


Figura 14.2: ventana Resultados de una búsqueda

- **(1) Icono** : cambia el nombre de la búsqueda.
- **(2) Caja de texto**: contenido de la búsqueda.
- **(3) Buscar en: "x equipos"**: abre la ventana de búsqueda avanzada para refinarla.
- **(4) Buscando**: estado de la búsqueda (**En curso**, **Cancelada).** Si la búsqueda no se ha iniciado o ha terminado no se indica el estado.
- **(5) Caja de texto Buscar**: filtra los resultados mostrados en la tabla de resultados por el nombre de

equipo.

- **Campos del listado**

Campo	Comentario	Valores
Archivo	Nombre del fichero encontrado.	Cadena de caracteres
Equipo	Nombre del equipo donde se encontró el fichero.	Cadena de caracteres
Grupo	Grupo de Cytomic EPDR al que pertenece el equipo.	Cadena de caracteres
Ruta	Ruta dentro del dispositivo de almacenamiento donde se encuentra el fichero.	Cadena de caracteres

Tabla 14.3: campos del listado Búsqueda de información personal en los equipos

- **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Archivo	Nombre del fichero encontrado.	Cadena de caracteres
Equipo	Nombre del equipo donde se encontró el fichero.	Cadena de caracteres
Grupo	Grupo de Cytomic EPDR al que pertenece el equipo.	Cadena de caracteres
Ruta	Ruta dentro del dispositivo de almacenamiento donde se encuentra el fichero.	Cadena de caracteres
DNIs	Indica si se detectó una o más entidades del tipo Documento Nacional de Identidad o equivalentes (Documento de identidad, Cédula de identidad / ciudadanía, Registro civil etc.) en el fichero.	Booleano
Pasaportes	Indica si se detectó una o más entidades del tipo Pasaporte en el fichero.	Booleano
Tarjeta de crédito	Indica si se detectó una o más entidades del tipo Número de tarjeta de crédito en el fichero.	Booleano
Cuentas bancarias	Indica si se detectó una o más entidades del tipo Número de cuenta bancaria en el fichero.	Booleano
Permisos de conducir	Indica si se detectó una o más entidades del tipo Permiso de conducir en el fichero.	Booleano
Números de la Seguridad Social	Indica si se detectó una o más entidades del tipo Número de la seguridad social en el fichero.	Booleano
Direcciones de correo electrónico	Indica si se detectó una o más entidades del tipo Dirección de correo electrónico en el fichero.	Booleano

Tabla 14.4: campos del fichero exportado Búsqueda de información personal en los equipos

Campo	Comentario	Valores
IPs	Indica si se detectó una o más entidades del tipo Dirección IP en el fichero.	Booleano
Nombres y apellidos	Indica si se detectó una o más entidades del tipo Nombre y apellidos en el fichero.	Booleano
Direcciones	Indica si se detectó una o más entidades del tipo Dirección en el fichero.	Booleano
Números de teléfono	Indica si se detectó una o más entidades de tipo Número de teléfono en el fichero.	Booleano

Tabla 14.4: campos del fichero exportado Búsqueda de información personal en los equipos

Sintaxis de las búsquedas

Cytomic Data Watch permite búsquedas flexibles de ficheros por contenido utilizando texto plano y modificadores para acotar el ámbito de los resultados.

Sintaxis admitida en búsquedas rápidas

- **Palabra**: busca "palabra" en el contenido del documento y en los metadatos.
- **PalabraA PalabraB**: busca "`palabraa`" o "`palabrab`" (operador OR) en el contenido del documento.
- **"PalabraA PalabraB"**: busca "`palabraa`" y "`palabrab`" seguidas en el contenido del documento.
- **+PalabraA +PalabraB**: busca "`palabraa`" y "`palabrab`" en el contenido del documento.
- **+Palabraa -Palabrab**: busca "`palabraa`" y no "`palabrab`" en el contenido del documento.
- **Palabra***: busca todas las palabras que empiezan por "palabra". El carácter "*" solo se permite al final de la cadena de caracteres a buscar.
- **Pa?abra**: busca todas las palabras que empiezan por "`pa`", terminan por "`abra`" y tienen entre los dos grupos un único carácter alfabético. El carácter "`?`" puede ir colocando en cualquier punto de la cadena de caracteres a buscar.
- **Palabra~**: busca todas las palabras que contienen la cadena de caracteres "palabra".

Sintaxis admitida en búsquedas guiadas

En las búsquedas guiadas no se utilizan los caracteres "+" y "–". En su lugar las palabras a buscar se distribuyen en las diferentes cajas de texto presentadas en la pantalla. Si utilizas los caracteres "+" y "–", éstos formarán parte de la búsqueda.

Entidades disponibles

Para acotar el ámbito de los resultados Cytomic Data Watch admite el uso de calificadores para indicar entidades o características del fichero en las búsquedas rápidas y avanzadas. Los calificadores disponibles son:

- **PiiType**: especifica si un tipo de entidad fue detectada en el fichero.
- **HasPii**: indica que el fichero contiene entidades detectadas.
- **Filename**: indica el nombre del fichero.
- **FileExtension**: indica la extensión del fichero.

Los valores admitidos para los calificadores son:

- **PiiType:BANKACCOUNT**: ficheros que contienen una o más entidades de tipo Cuenta bancaria.
- **PiiType:CREDITCARD**: ficheros que contienen una o más entidades de tipo Tarjeta de crédito.
- **PiiType:IDCARD**: ficheros que contienen una o más entidades de tipo Documento de identidad (documento nacional de identidad, Cédula de identidad / ciudadanía, Registro civil etc.).
- **PiiType:SSN**: ficheros que contienen una o más entidades de tipo Número de la seguridad social.
- **PiiType:IP**: ficheros que contienen una o más entidades de tipo Dirección IP.
- **PiiType:EMAIL**: ficheros que contienen una o más entidades de tipo Dirección de correo electrónico.
- **PiiType:PHONE**: ficheros que contienen una o más entidades de tipo Teléfono.
- **PiiType:ADDRESS**: ficheros que contienen una o más entidades de tipo Dirección.
- **PiiType:FULLNAME**: ficheros que contienen una o más entidades de tipo Nombre y apellidos.
- **PiiType:PASSPORT**: ficheros que contienen una o más entidades de tipo Número de pasaporte.
- **PiiType:DRIVERLIC**: ficheros que contienen una o más entidades de tipo Numero de licencia / permiso de conducción.
- **HasPii:True**: ficheros que contienen alguna entidad detectada.
  - **Filename**:"nombre del fichero": ficheros que tienen como nombre la cadena indicada.
  - **Fileextension**:"extensión del fichero": ficheros que tienen como extensión la cadena indicada.

Sintaxis de las búsquedas con entidades

Las entidades se pueden utilizar en todos los tipos de búsqueda (rápida o guiada) de forma individual o combinadas con otras cadenas de caracteres.

- **PiiType:IDCARD**: busca todos los ficheros con alguna entidad detectada de tipo Documento de identidad.
- **+PiiType:IDCARD +"Empresa"**: busca el fichero que contiene el listado de documentos de identidad (con alguna detección de entidad IDCARD) de la empresa (que contenta la cadena de caracteres "Empresa").
- **+Filename:analisis* +fileextension:docx -PiiType:fullname**: busca todos los ficheros de análisis (su nombre empieza por la palabra "análisis") en formato Word (extensión docx) y no están firmados (no se detectó ninguna entidad de tipo Fullname – Nombre y apellidos).

Consejos para construir búsquedas compatibles con la normalización

- Utiliza preferiblemente letras en minúsculas.
- Ten en cuenta la configuración establecida sobre el contenido de los ficheros a indexar y los que ficheros excluidos ya que de ello dependerá el número de resultados mostrados en las búsquedas.
- Para buscar **números de cuentas bancarias, números de tarjetas de crédito, números de identidad, números de la seguridad social, números de pasaporte, números de permiso** elimina los caracteres de separación.
- Para buscar **direcciones IP** y **direcciones de correo electrónico** introdúcelas tal cual.
- Para buscar **números de teléfono** elimina los caracteres de separación, introduciendo el código del país si es necesario sin el signo "+".
- Para buscar **direcciones físicas** elimina los caracteres numéricos.

Búsqueda de ficheros duplicados

Con el objetivo de ayudar a centralizar la información sensible en un único punto y por tanto minimizar la exposición de este tipo de datos, Cytomic Data Watch incluye la funcionalidad de búsqueda de ficheros duplicados y posterior borrado.

Definición de fichero duplicado

Se consideran a dos ficheros como duplicados cuando su contenido es idéntico, independientemente del proceso de normalización descrito en el apartado "**Proceso de normalización**" ni de la configuración establecida por el administrador en el apartado "**Contenido recuperado en el proceso de indexación**". En la comparación no se consideran ni el nombre ni la extensión de los ficheros.

Búsqueda de ficheros duplicados

Para buscar un fichero duplicado sigue los pasos mostrados a continuación:

- Desde el panel lateral **Mis listados:**
  - En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el link **Añadir**. Se mostrará una ventana con todos los listados disponibles.
  - Elige el listado **Archivos con información personal**. Se mostrará el listado de ficheros PII encontrados en la red.
- Desde el widget **Archivos con información personal**:
  - En el menú superior **Estado**, panel lateral **Data Control**, haz clic en una serie del widget **Archivos con información personal.** Se mostrará el listado **Archivos con información personal** con un criterio de filtrado establecido.
- Desde el widget **Archivos por tipo de información personal**:
  - En el menú superior **Estado**, panel lateral **Data Control**, haz clic en una serie del widget **Archivos**

por tipo de información personal. Se mostrará el listado **Archivos con información personal** con un criterio de filtrado establecido.

- En el menú de contexto asociado al archivo que se quiere buscar, haz clic en la opción **Buscar copias de archivo**. Se abrirá un nuevo listado con los todos los ficheros duplicados encontrados en la red.

Borrado y restauración de ficheros

Borrar ficheros de los equipos de la red

Cytomic Data Watch permite borrar los ficheros indexados y mostrados en el inventario de los equipos de la red. El borrado de ficheros es una operación asíncrona que inicia el administrador de la red desde la consola y se produce cuando el agente recibe una petición desde el servidor Cytomic EPDR y se cumplen las siguientes condiciones:

- El fichero no está en uso.
- El contenido del fichero no ha cambiado con respecto al almacenado en inventario.
- El fichero no ha sido borrado por el usuario en el periodo comprendido entre la generación del inventario y la acción de borrado por parte del administrador.
- El equipo está online. Si esta condición no se cumple, Cytomic Data Watch marcará el fichero como **Pendiente de eliminar** hasta que el equipo se conecte al servidor Cytomic EPDR.

Estados de la acción de borrado

Al ser una operación asíncrona, el borrado de ficheros admite los estados mostrados a continuación:

- **Eliminado**: el fichero se ha movido a la zona de backup.
- **Pendiente de eliminar**: Cytomic Data Watch está esperando a que el equipo se conecte al servidor Cytomic EPDR para ejecutar la tarea de borrado.
- **Error**: el fichero no se ha podido borrar por un error.

Backup de ficheros borrados por Cytomic Data Watch

Lo ficheros borrados por Cytomic Data Watch no se eliminan definitivamente del disco duro de los equipos. En su lugar se mueven a un área de backup donde residen durante 30 días, pasados los cuales el fichero es eliminado por completo.

Esta área es excluida automáticamente del inventario, de las búsquedas y de la monitorización de ficheros, y es inaccesible para el software instalado en el equipo de usuario.

Borrado de ficheros

Para borrar uno o varios ficheros sigue los pasos mostrados a continuación:

- Desde el panel lateral **Mis listados:**

- En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el link **Añadir**. Se mostrará una ventana con todos los listados disponibles.
- Elige el listado **Archivos con información personal**. Se mostrará el listado de ficheros PII encontrados en la red.

- Desde el widget **Archivos con información personal**:
  - En el menú superior **Estado**, panel lateral **Data Control**, haz clic en una serie del widget **Archivos con información personal.** Se mostrará el listado **Archivos con información personal** con un criterio de filtrado establecido.
- Desde el widget **Archivos por tipo de información personal**:
  - En el menú superior **Estado**, panel lateral **Data Control**, haz clic en una serie del widget **Archivos por tipo de información personal.** Se mostrará el listado **Archivos con información personal** con un criterio de filtrado establecido.
- Para borrar varios ficheros:
  - Haz clic en las casillas de selección asociadas a los ficheros que quieres borrar.
  - Haz clic en el icono de la parte superior de la ventana. Se mostrará una ventana pidiendo confirmación.
- Para borrar un único fichero:
  - Utiliza el menú de contexto asociado al fichero que quieres eliminar y haz clic en la opción **Eliminar**. Se mostrará una ventana pidiendo confirmación.
- Si confirmas el borrado del fichero, éste se mostrará en el listado de ficheros en rojo y con el icono indicando que está pendiente de borrado.

Visualizar ficheros borrados

Para visualizar los ficheros borrados por el administrador sigue los pasos mostrados a continuación:

- En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el link **Añadir**. Se mostrará una ventana con todos los listados disponibles.
- Elige el listado **Archivos eliminados por el administrador**. Se mostrará el listado de ficheros PII encontrados en la red que el administrador borró o restauró previamente.

Restaurar ficheros previamente borrados por el administrador

Cytomic Data Watch permite restaurar en su ruta original los ficheros previamente borrados por el administrador desde la consola, en tanto en cuanto estos ficheros permanezcan en el área de backup (30 días desde su borrado). La restauración de ficheros es una operación asíncrona que inicia el administrador de la red desde la consola y se produce cuando el agente recibe una petición desde el servidor Cytomic EPDR y se cumplen las siguientes condiciones:

- **El fichero permanece en la zona de backup:** los ficheros borrados permanecen en el área de backup durante 30 días, transcurridos los cuales se procede a eliminar el fichero definitivamente sin

posibilidad de restauración.

- **No existe otro fichero en la ruta de restauración con el mismo nombre el fichero:** si existe otro fichero con el mismo nombre en la ruta de restauración Cytomic Data Watch seguirá restaurando el fichero, pero lo hará en la carpeta `Lost&Found`.
- **La ruta de restauración existe**: si la ruta de restauración no existe, Cytomic Data Watch seguirá restaurando el fichero, pero lo hará en la carpeta `Lost&Found`.
- **El equipo está online:** si el equipo está offline Cytomic Data Watch marcará el fichero como **Pendiente de restaurar** hasta que se conecte al servidor Cytomic EPDR.

Estados de la acción de restaurar

Al ser una operación asíncrona, la restauración de ficheros admite los estados mostrados a continuación:

- Restaurado
- Pendiente de restaurar
- Error

Restaurar ficheros borrados

Para restaurar los ficheros borrados por el administrador sigue los pasos mostrados a continuación:

- **Acceso a la funcionalidad de restauración:**
  - En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el link **Añadir**. Se mostrará una ventana con todos los listados disponibles.
  - Elige el listado **Archivos eliminados por el administrador**. Se mostrará el listado de ficheros PII encontrados en la red que el administrador borró o restauró previamente.

o

  - En el menú superior **Estado**, panel lateral **Data Control** haz clic en el widget **Archivos eliminados por el administrador.** Se abrirá el listado **Archivos eliminados por el administrador** sin filtros preconfigurados.

- **Para restaurar varios ficheros:**
  - Haz clic en las casillas de selección asociadas a los ficheros que quieres recuperar.
  - Haz clic en el icono de la parte superior de la ventana. Se mostrará una ventana pidiendo confirmación.
  - Si el administrador confirma la recuperación del fichero, éste pasará al estado **Restaurando**.
- **Para restaurar un único fichero:**
  - Utiliza el menú de contexto asociado al fichero que quieres recuperar.
  - Haz clic en la opción **Restaurar**. Se mostrará una ventana pidiendo confirmación.

- Si el administrador confirma la recuperación del fichero, éste pasará al estado **Restaurando**.

Configuración de Data Control

Para acceder a la configuración de Data Control:

- Haz clic en el menú superior **Configuración**, menú lateral **Data Control**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración de **Data Control**.

Búsqueda de equipos que no cumplen con los requisitos

Para localizar los equipos que no tienen instalado alguno o ninguno de los componentes iFilter haz clic en el enlace **Comprobar ahora** de la pantalla de configuración. Se abrirá la zona **Equipos** con un listado filtrado por el criterio **Equipos sin Microsoft Filter Pack**.

Configuración general

Activar el inventario de información personal.

Si la opción **Activar el inventario de información personal** está activada, Cytomic Data Watch mostrará los ficheros PII detectados en la red utilizando los widgets del dashboard y los listados. Consulta el apartado "**Paneles / widgets en Cytomic Data Watch**" y "**Listados en Cytomic Data Watch**".

Para que los ficheros PII almacenados en un equipo concreto se muestren es necesario que el proceso de inventariado se haya completado para ese equipo.

Para ver el estado de la indexación haz clic en el enlace Ver estado de indexación de los equipos. Se abrirá el "**Listado Estado de Data Control**".

Permitir realizar búsquedas de información en los equipos

Cytomic Data Watch permite localizar ficheros por su nombre o contenido, siempre que hayan sido previamente indexados. Para activar las búsquedas de ficheros haz clic en el botón **Permitir realizar búsquedas de información en los equipos** y Cytomic Data Watch comenzará el proceso de indexación de los ficheros almacenados en los equipos de los usuarios. Consulta el apartado "**Búsqueda de ficheros**".

Para ver el estado de la indexación haz clic en el enlace **Ver estado de indexación de los equipos**. Se abrirá el "**Listado Estado de Data Control**".

Activar el seguimiento de información personal

Para que Cytomic Data Watch comience a monitorizar las acciones de los procesos ejecutadas sobre ficheros PII almacenados en el equipo, haz clic en el botón de activación **Activar seguimiento de información personal**.

Contenido recuperado en el proceso de indexación

Permite establecer el tipo de contenido que se considerará a la hora de generar el inventario y que se devolverá como resultado de las búsquedas.

> *Los equipos que ya tengan un índice generado y reciban un cambio de configuración borrarán el índice y reiniciarán el proceso de indexado desde el principio.*

Dependiendo de si el administrador únicamente quiere generar un inventario de ficheros PII o, por el contrario, también desea realizar búsquedas por contenido, seleccionará el tipo de indexación:

- **Indexar solo el texto**: se indexa solo el texto a no ser que forme parte de una entidad reconocida por Cytomic Data Watch. Las búsquedas por contenido producidas con este tipo de índice serán más limitadas, por lo tanto se recomienda si el administrador únicamente quiere generar el inventario de ficheros PII.
- **Indexar todo el contenido**: se indexan tanto los textos como los caracteres numéricos. Se recomienda cuando el administrador además de mantener el inventario de ficheros PII quiere realizar búsquedas precisas por contenido.

> *Cytomic Data Watch buscará sobre los contenidos del fichero según la configuración **Contenido del índice en los equipos** asignada. Si los equipos tienen configuraciones de indexación distintas, el resultado de las búsquedas pueden no ser homogéneo.*

Programar períodos de indexación

Configura la franja horaria en la que el proceso de indexación se iniciará en caso de ser necesario:

- **Siempre activado**: no se indica una franja horaria y el proceso de indexación se iniciará en el momento que sea necesario.
- **Activar sólo durante las siguientes horas**: indica mediante un calendario mensual los días y horas en los que el proceso de indexación podrá iniciarse.
- Utiliza los botones **Vaciar** y **Seleccionar todo** para limpiar el calendario o marcarlo por completo (equivalente a **Siempre activado**).

Exclusiones

El administrador puede excluir del proceso de búsqueda a aquellos ficheros almacenados en los equipos de la red cuyo contenido no considere oportuno tener en cuenta.

- **Extensiones**: excluye a los ficheros con las extensiones indicadas.
- **Archivos**: excluye del proceso a los ficheros con el nombre indicado. Se pueden utilizar los caracteres comodín * y ?.
- **Carpetas**: excluye del proceso a todos los ficheros contenidos en las carpetas indicadas. Se pueden utilizar variables del sistema.

Paneles / widgets en Cytomic Data Watch

A continuación, se detallan los distintos widgets implementados en el dashboard de **Cytomic Data Watch,** las distintas áreas y zonas activas incorporadas y los tooltips y su significado. Para acceder haz clic en el menú superior **Estado**, panel lateral **Data Control**.

Estado del despliegue

Muestra los equipos donde Cytomic Data Watch está funcionando correctamente y aquellos que presentan algún tipo de error. El estado de los equipos se representa mediante un círculo con distintos colores y contadores asociados. El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

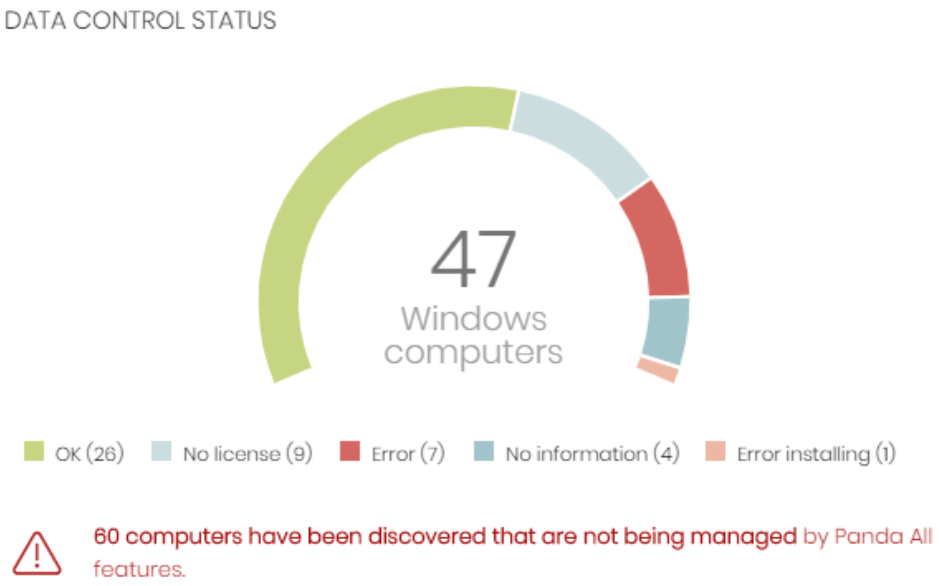


Figura 14.3: Panel Estado de Data Control

- **Significado de las series**

Serie	Descripción
Ok	Equipos con Cytomic Data Watch instalado, licenciado y funcionando correctamente.
Error	Equipos con Cytomic Data Watch instalado pero que, por alguna razón, el módulo no responde a las peticiones enviadas desde los servidores de Cytomic.
Sin licencia	Equipos no gestionados por Cytomic Data Watch debido a la falta de licencias suficientes, o a la no asignación de licencias disponibles.
Error instalando	Equipos cuya instalación no se pudo completar.
Sin información	Equipos con licencia recientemente asignada y que todavía no han reportado su estado al servidor, o equipo con un agente sin actualizar.

Tabla 14.5: descripción de la serie Estado de Data Control

Serie	Descripción
Parte central	Suma de todos equipos compatibles con Cytomic Data Watch.

Tabla 14.5: descripción de la serie Estado de Data Control

- **Filtros preestablecidos desde el panel**

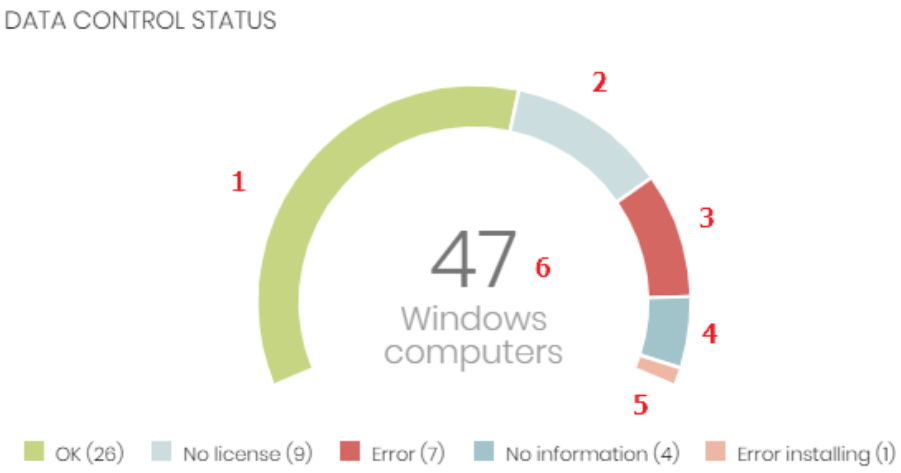


Figura 14.4: zonas activas del panel Estado de Data Control

Al hacer clic en las zonas indicadas en la figura 14.4 se abre el listado **Estado de Cytomic Data Watch** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de Data Control = Correcto.
(2)	Estado de Data Control = Sin licencia.
(3)	Estado de Data Control = Error.
(4)	Estado de Data Control = Sin información.
(5)	Estado de Data Control = Error instalando.
(6)	Sin filtros.

Tabla 14.6: definición de filtros del listado Estado de Data Control

Equipos sin conexión

Equipos sin conexión muestra los equipos de la red que no han conectado con la nube de Cytomic en un determinado periodo de tiempo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.

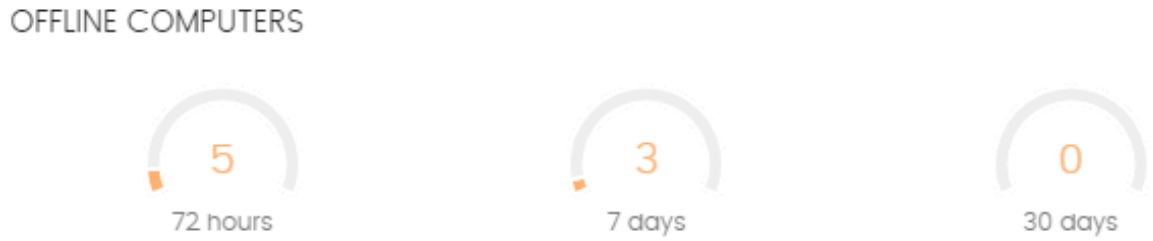


Figura 14.5: panel Equipos sin conexión

- **Significado de las series**

Serie	Descripción
72 horas	Número de equipos que no enviaron su estado en las últimas 72 horas.
7 días	Número de equipos que no enviaron su estado en las últimas 7 días.
30 días	Número de equipos que no enviaron su estado en las últimas 30 días.

Tabla 14.7: descripción de la serie Equipos sin conexión

- **Filtros preestablecidos desde el panel**

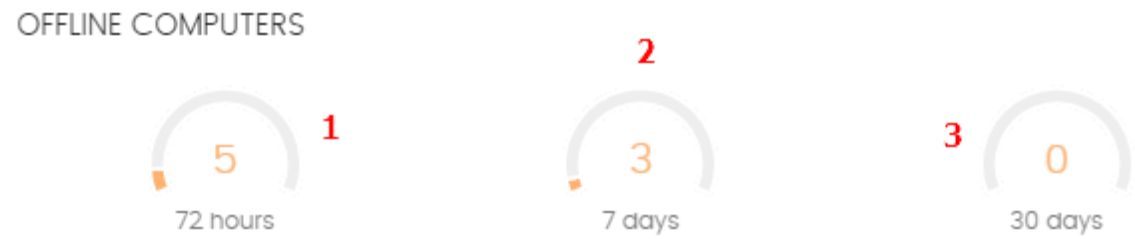


Figura 14.6: zonas activas del panel Equipos sin conexión

Al hacer clic en las zonas indicadas en la figura 14.6 se abre el listado **Estado de Data Control** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 72 horas.
(2)	Última conexión = Hace más de 7 días.
(3)	Última conexión = Hace más de 30 días.

Tabla 14.8: definición de filtros del listado Estado de Data Control

Estado de la actualización

Muestra el estado de los equipos con respecto a la actualización del motor de Cytomic Data Watch.

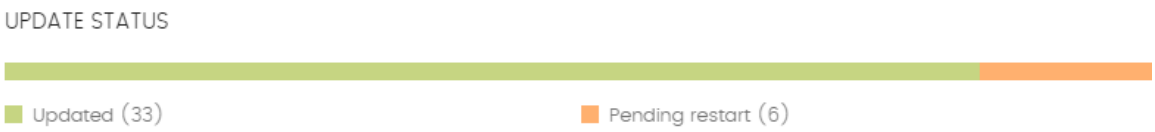


Figura 14.7: panel Estado de la actualización

- **Significado de las series**

Serie	Descripción
Actualizados	Número de equipos con el motor Cytomic Data Watch actualizado.
Desactualizados	Número de equipos con el motor Cytomic Data Watch desactualizado.
Pendientes de reinicio	Número de equipos que han descargado el motor Cytomic Data Watch pero todavía no se han reiniciado, con lo que todavía no se ha actualizado.

Tabla 14.9: descripción de la serie Estado de la actualización

- **Filtros preestablecidos desde el panel**

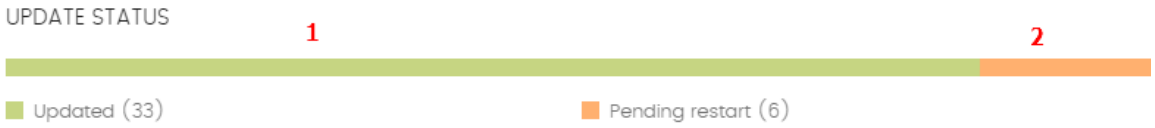


Figura 14.8: zonas activas del panel Estado de la actualización

Al hacer clic en las zonas indicadas en la figura 14.8 se abre el listado **Estado de Data Control** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Protección actualizada = Si.
(2)	Protección actualizada = Pendiente de reinicio.
(3)	Protección actualizada = No.

Tabla 14.10: definición de filtros del listado Estado de Data Control

Estado de la indexación

Muestra el estado de los equipos con respecto al estado de indexación de las unidades de almacenamiento conectadas.

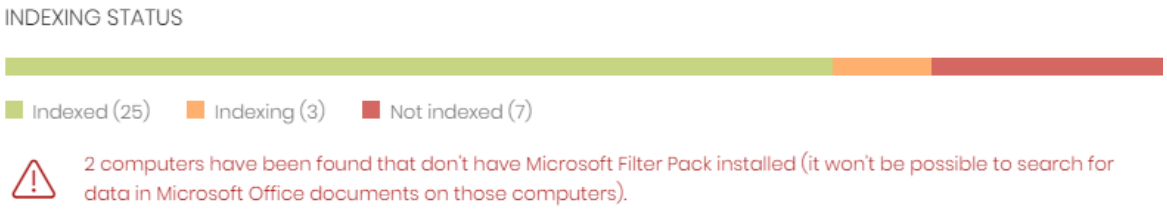


Figura 14.9: panel Estado de la indexación

- **Significado de las series**

Serie	Descripción
Indexado	Número de equipos con los contenidos de las unidades de almacenamiento completamente indexados. Requiere que las búsquedas y/o el inventario estén activados. Consulta el apartado "**Configuración de Data Control**".
No indexado	Número de equipos con los contenidos de las unidades de almacenamiento sin indexar. Requiere que las búsquedas y/o el inventario estén activados. Consulta el apartado "**Configuración de Data Control**".
Indexando	Número de equipos con contenidos en proceso de indexación. Requiere que las búsquedas y/o el inventario estén activados. Consulta el apartado "**Configuración de Data Control**".

Tabla 14.11: descripción de la serie Estado de la indexación

- **Filtros preestablecidos desde el panel**

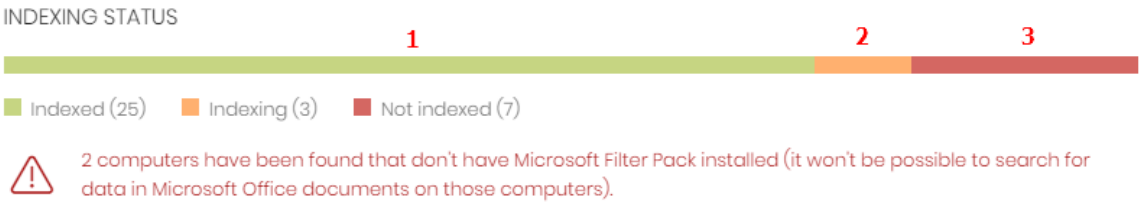


Figura 14.10: zonas activas del panel Estado de la indexación

Al hacer clic en las zonas indicadas en la figura **14.10** se abre el listado **Estado de Data Control** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de indexación = Indexado.
(2)	Estado de indexación = Indexando.
(3)	Estado de indexación = No indexado.

Tabla 14.12: definición de filtros del listado Estado de Data Control

Características activadas en los equipos

Refleja el número total de equipos en la red que tienen instalado y correctamente licenciado Cytomic Data Watch, y que han reportado el estado **Activado** para cada una de las tres funcionalidades.

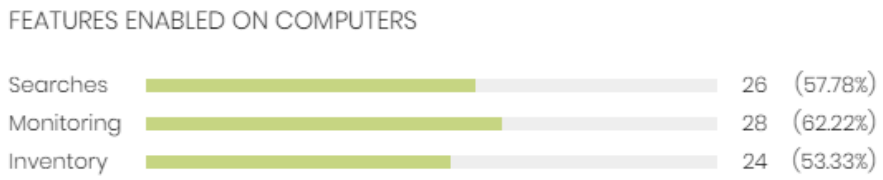


Figura 14.11: panel Características activadas en los equipos

- **Significado de las series**

Serie	Descripción
Búsquedas	Muestra el número de equipos que reportan como activada la funcionalidad de búsqueda por contenido de ficheros PII.
Seguimiento	Muestra el número de equipos que reportan como activada la funcionalidad de monitorización de ficheros PII.
Inventario	Muestra el número de equipos que reportan como activada la funcionalidad de inventario de ficheros PII.

Tabla 14.13: descripción de la serie Características activadas en los equipos

- **Filtros preestablecidos desde el panel**

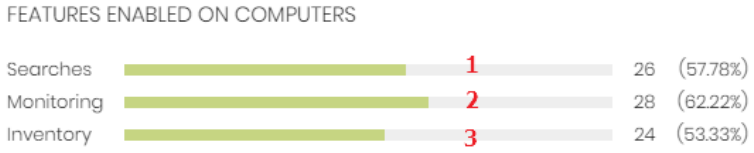


Figura 14.12: zonas activas del panel Características activadas en los equipos

Al hacer clic en las zonas indicadas en la figura **14.12** se abre el listado **Estado de Data Control** con los filtros preestablecidos mostrados a continuación.

Zona activa	Filtro
(1)	Búsqueda de información en los equipos activada = Si.
(2)	Seguimiento de información personal activada = Si.
(3)	Inventario de información personal activado= Si.

Tabla 14.14: definición de filtros del listado Estado de Data Control

Archivos eliminados por el administrador

Muestra los distintos estados por los que pasan los ficheros eliminados por el administrador.

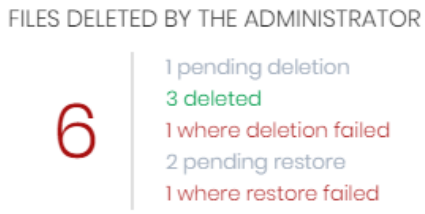


Figura 14.13: panel Archivos eliminados por el administrador

- **Significado de las series**

Serie	Descripción
Pendientes de eliminar	Archivos marcados para borrar pero que todavía no se ha ejecutado la tarea.
Eliminados	Archivos borrados que permanecen en el área de backup.
Con error al eliminar	Archivos sobre los que no fue posible ejecutar la tarea de borrado.
Pendientes de restaurar	Archivos marcados para restaurar pero que todavía no se ha ejecutado la tarea.
Restaurados	Archivos que han sido movidos desde el área de backup a su ubicación original.

Tabla 14.15: descripción de la serie Archivos eliminados por el administrador

- **Filtros preestablecidos desde el panel**

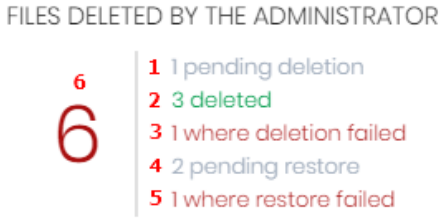


Figura 14.14: zonas activas del panel Archivos eliminados por el administrador

Al hacer clic en las zonas indicadas en la figura **14.14** se abre un listado con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(1)	Archivos con información personal.	Pendiente de eliminar.
(2)	Archivos eliminados por el administrador.	Estado = Eliminado.

Tabla 14.16: definición de filtros del listado Archivos eliminados por el administrador

Zona activa	Listado	Filtro
(3)	Archivos con información personal.	Error eliminando.
(4)	Archivos eliminados por el administrador.	Estado = Pendiente de restaurar.
(5)	Archivos eliminados por el administrador.	Estado = Error restaurando.
(6)	Archivos eliminados por el administrador.	Estado = todos.

Tabla 14.16: definición de filtros del listado Archivos eliminados por el administrador

Archivos con información personal

Muestra el número de ficheros con información personal encontrados en la red y el total de ficheros encontrados en el último inventario diario generado.

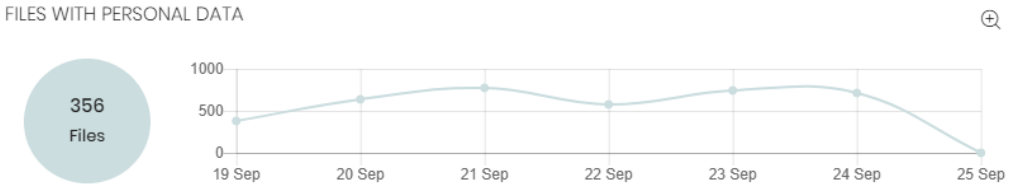


Figura 14.15: panel Archivos con información personal

- **Significado de las series**

Serie	Descripción
Burbuja	Número total de ficheros PII encontrados según el último inventario enviado por cada equipo.
Linea	Número de ficheros PII encontrados en los inventarios diarios generados en las fechas indicadas en el eje de las Xs, y en todos los equipos de la red.

Tabla 14.17: descripción de la serie Archivos con información personal

- **Filtros preestablecidos desde el panel**

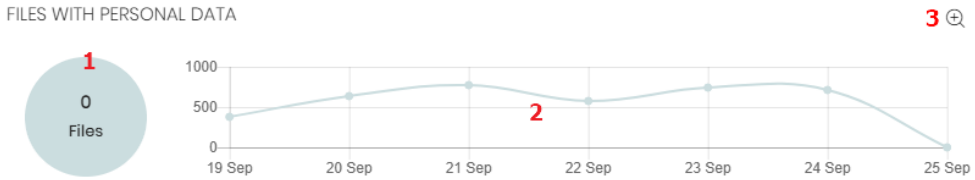


Figura 14.16: zonas activas del panel Archivos con información personal

Al hacer clic en las zonas indicadas en la figura 14.16 se abre el listado **Archivos con información personal** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtros.
(2)	Fecha 1 = fecha elegida y Fecha 2 = fecha actual.
(3)	Se abre una nueva ventana con una ampliación del widget.

Tabla 14.18: definición de filtros del listado Archivos con información personal

- **Ampliación de la gráfica Archivos con información personal**

Al hacer clic sobre el icono se abre una ventana con una ampliación del widget **Archivos con información personal** representando mediante una serie independiente el número de ficheros PII que contienen cada una de las entidades soportadas.

Para configurar el widget:

- Haz clic en la leyenda para activar o desactivar una serie.
- Haz clic en el link **Ocultar todos los datos** para mostrar el número de ficheros PII que contienen cualquier tipo de entidad.
- Haz clic en **Mostrar todos los datos** para mostrar el número de ficheros PII que contienen cada tipo de entidad por separado.

Equipos con información personal

Muestra el número de equipos de usuario y servidores que contienen ficheros con información personal en el último inventario diario generado.

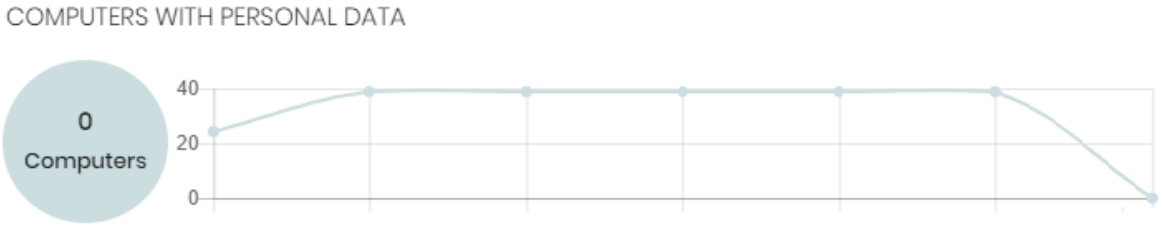


Figura 14.17: panel Archivos con información personal

- **Significado de las series**

Serie	Descripción
Burbuja	Número de equipos con ficheros PII encontrados según los últimos datos enviados por cada equipo.
Linea	Número total de equipos con ficheros PII encontrados en los inventarios diarios generados en las fechas indicadas en el eje de las Xs.

Tabla 14.19: descripción de la serie Equipos con información personal

- **Filtros preestablecidos desde el panel**

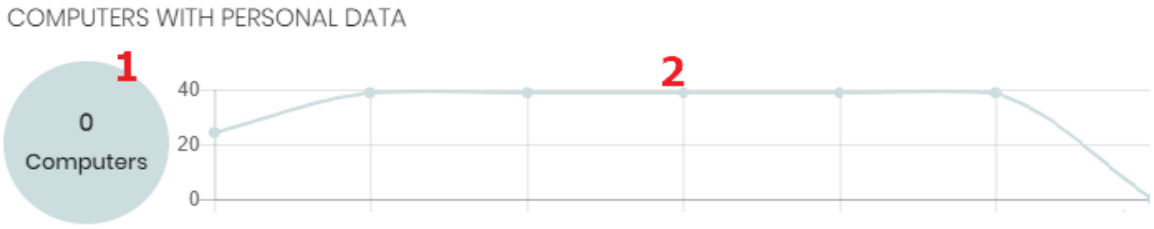


Figura 14.18: zonas activas del panel Archivos con información personal

Al hacer clic en las zonas indicadas en la figura 14.18 se abre el listado **Archivos con información personal** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtros.
(2)	Fecha 1 = fecha elegida y Fecha 2 = fecha actual.

Tabla 14.20: definición de filtros del listado Archivos con información personal

Archivos por tipo de información personal

Muestra el número de archivos PII encontrados por cada tipo de entidad soportada en el último inventario diario generado.

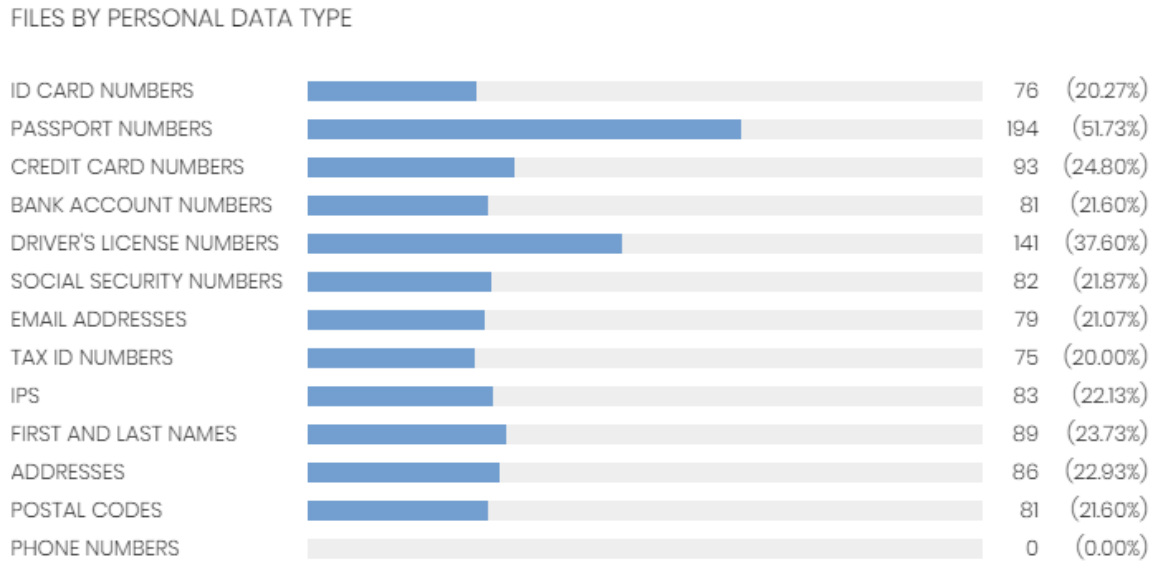


Figura 14.19: panel Archivos por tipo de información personal

- **Significado de las series**

Serie	Descripción
Serie	Número total de ficheros PII encontrados en el último inventario diario generado por cada tipo de entidad soportada, y porcentaje de ficheros sobre el total de ficheros PII detectados.

Tabla 14.21: descripción de la serie Archivos por tipo de información personal

- **Filtros preestablecidos desde el panel**

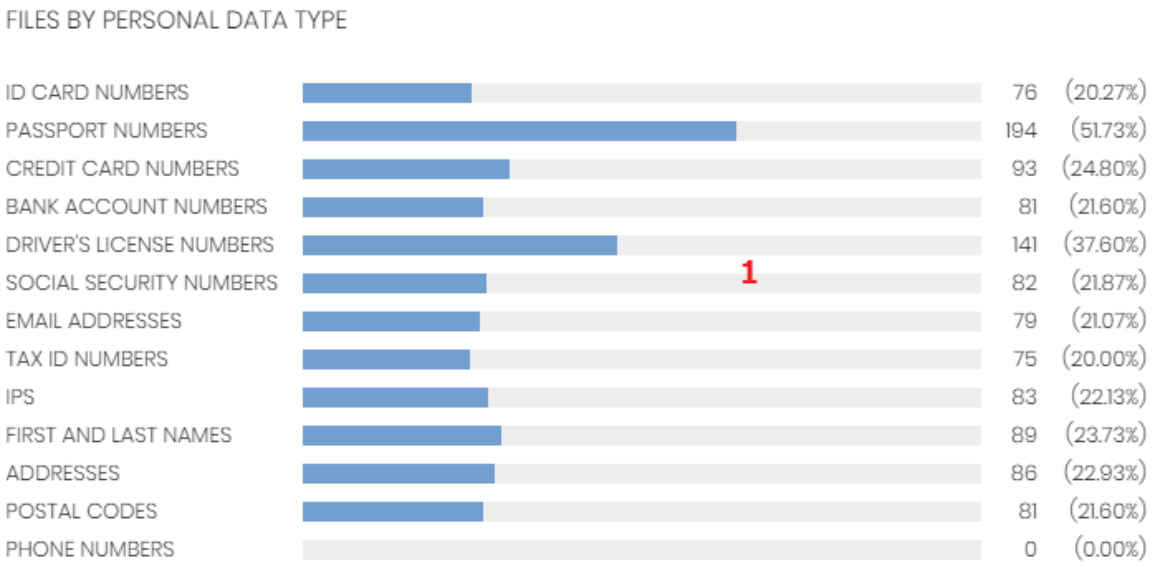


Figura 14.20: zonas activas del panel Archivos por tipo de información personal

Haz clic en el widget para abrir el listado **Archivos con información personal** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Información personal = tipo de entidad seleccionada.

Tabla 14.22: definición de filtros del listado Archivos con información personal

Listados en Cytomic Data Watch

Listado Estado de Data Control

Este listado muestra todos los equipos de la red e incorpora filtros relativos al estado del módulo Cytomic Data Watch para localizar aquellos puestos de trabajo o dispositivos móviles que cumplen los criterios establecidos en el panel.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres

Tabla 14.23: campos del listado Estado de Data Control

Campo	Comentario	Valores
Seguimiento de información personal	Indica si Cytomic Data Watch puede realizar un seguimiento de los ficheros con información personal en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	• Error instalando y Error • Desactivado • Activado • Sin licencia • Sin información
Inventario	Indica si Cytomic Data Watch puede generar un inventario de los ficheros con información personal en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	• Error instalando y Error • Desactivado • Activado • Sin licencia • Sin información
Búsquedas	Indica si Cytomic Data Watch puede buscar ficheros en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	• Error instalando y Error • Desactivado • Instalando • Activado • Sin licencia • Sin información
Actualizado	Indica si el módulo de Cytomic Data Watch instalado en el equipo coincide con la última versión publicada o no. Al pasar el puntero del ratón por encima del campo se indica la versión de la protección instalada.	• Actualizado • Pendiente de reinicio • No actualizado
Microsoft Filter Pack	Indica si todos los componentes necesarios del paquete Microsoft Filter Pack están instalados o no en el equipo.	• Instalado • No instalado • Información no disponible
Estado de indexación	Indica el estado del proceso de indexación de ficheros.	• Indexando • Indexado (Solo texto o Todo el contenido • No indexado • No disponible
Última conexión	Fecha del último envío del estado de Cytomic EPDR a la nube de Cytomic.	Fecha

Tabla 14.23: campos del listado Estado de Data Control

- **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Versión del agente		Cadena de caracteres
Fecha instalación	Fecha en la que el Software Cytomic EPDR se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha del último envío del estado del equipo a la nube de Cytomic.	Fecha
Fecha de la última actualización	Fecha de la última actualización del agente.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS • Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección actualizada	Indica si el módulo de la protección instalado en el equipo es la última versión publicada.	Binario
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Conocimiento actualizado	Indica si el fichero de firmas descargado en el equipo es la última versión publicada.	Binario
Fecha de última actualización	Fecha de la descarga del fichero de firmas.	Fecha

Tabla 14.24: campos del fichero exportado Estado de Data Control

Campo	Comentario	Valores
Seguimiento de información personal	Indica si Cytomic Data Watch puede realizar un seguimiento de los ficheros con información personal en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	• Error instalando • Error • Desactivado • Correcto • Sin licencia • Sin información
Inventario de información	Indica si Cytomic Data Watch puede generar un inventario de los ficheros con información personal en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	• Error instalando • Error • Desactivado • Correcto • Sin licencia • Sin información
Búsquedas	Indica si Cytomic Data Watch puede buscar ficheros en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	• Error instalando • Error • Desactivado • Correcto • Sin licencia • Sin información
Microsoft Filter Pack	Indica si todos los componentes necesarios del paquete Microsoft Filter Pack están instalados o no en el equipo.	• Instalado • No instalado • No disponible
Estado de indexación	Indica el estado del proceso de indexación de ficheros.	• Indexando • Indexado • No indexado • No disponible
Tipo de indexación	Muestra el tipo de indexación configurado en el equipo.	• Solo el texto • Todo el contenido
Estado de aislamiento	Indica si el equipo ha sido aislado de la red o se comunica con sus equipos vecinos de forma normal.	• Aislado • No aislado
Fecha error instalación	Fecha en la que se intentó la instalación del módulo Cytomic Data Watch y se produjo el error.	Fecha
Error instalación	Motivo del error de instalación.	Cadena de caracteres

Tabla 14.24: campos del fichero exportado Estado de Data Control

- **Herramienta de filtrado**

Campo	Comentario	Valores
Tipo de equipo	Filtra los equipos según su clase.	• Estación • Portátil • Dispositivo móvil • Servidor
Buscar equipo	Filtra los equipos según su nombre.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Cytomic Data Watch a la nube de Cytomic.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días • Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Protección actualizada	Filtra los equipos según la versión de la protección instalada.	• Todos • Si • No • Pendiente de reinicio
Estado de indexación	Filtra los equipos según el estado del proceso de indexación de ficheros.	• Todos • Indexando • Indexado • No indexado • No disponible
Tipo de indexación	Muestra los equipos que tienen configurado un tipo concreto de indexación.	• Todos • Solo el texto • Todo el contenido
Microsoft Filter Pack	Filtra los equipos si tienen o no instalados todos los componentes necesarios del paquete Microsoft Filter Pack.	• Todos • Falso • Verdadero
Estado de Data Control	Filtra los equipos según el estado del módulo Cytomic Data Watch.	• Instalando… • Sin información • Correcto • Seguimiento de información personal desactivado

Tabla 14.25: campos de filtrado para el listado Estado de Data Control

Campo	Comentario	Valores
		• Búsqueda de información en el equipo desactivado • Error • Error Instalando • Sin licencia • Seguimiento de información personal activada • Búsqueda de información en los equipos activada • Inventario de información personal activado • Inventario de información personal desactivado

Tabla 14.25: campos de filtrado para el listado Estado de Data Control

Listado Archivos con información personal

Este listado muestra todos los ficheros PII encontrados, así como su tipo, localización y otra información relevante.

Dado que Cytomic Data Watch solo retiene el último inventario completo de cada equipo, aquellos que estuvieran apagados en el momento de su generación solo mostraran información en el listado **Archivos con información personal** si el campo **Última vez visto** abarca la fecha en la que se generó el inventario de esos equipos.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Cadena de caracteres
Ruta	Ruta completa de la carpeta donde se almacena el fichero dentro del equipo.	Cadena de caracteres

Tabla 14.26: campos del listado Archivos con información personal

Campo	Comentario	Valores
Información personal	Tipo de información personal contenida en el fichero.	• Entidad documento de identidad • Entidad Pasaporte • Entidad Tarjeta de crédito • Entidad Cuenta bancaria • Entidad Número de la seguridad social • Entidad Permiso de conducir • Entidad Dirección de correo electrónico • Entidad Dirección IP • Entidad Nombre y Apellido • Entidad Direcciones • Entidad Teléfono móvil
Última vez visto	Fecha en la que se tomó la última fotografía del sistema de ficheros del equipo.	Fecha

Tabla 14.26: campos del listado Archivos con información personal

- **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Cadena de caracteres
Ruta	Ruta completa de la carpeta donde se almacena el fichero dentro del equipo.	Cadena de caracteres
DNIs	Entidad Documento de identidad.	Booelano
Pasaportes	Entidad Número de pasaporte.	Booelano
Tarjetas de crédito	Entidad Número de tarjeta de crédito.	Booelano
Cuentas bancarias	Entidad Numero de cuenta bancaria.	Booelano
Permisos de conducir	Entidad Permiso de conducir.	Booelano

Tabla 14.27: campos del fichero exportado Archivos con información personal

Campo	Comentario	Valores
Números de la Seguridad Social	Entidad Número de la seguridad social.	Booelano
Direcciones de correo electrónico	Entidad Dirección de correo electrónico.	Booelano
IPs	Entidad Dirección IP.	Booelano
Nombres y apellidos	Entidad Nombre y apellidos.	Booelano
Direcciones	Entidad Dirección física.	Booelano
Números de teléfono	Entidad Número de teléfono.	Booelano
Última vez visto	Fecha en la que el fichero fue incluido por última vez en el inventario diario.	Fecha
Estado	Estado del fichero.	• Eliminado • Pendiente de eliminar • Restaurado • Pendiente de restaurar • Error restaurando
Error	• El fichero está en uso. • El contenido del fichero ha cambiado con respecto al almacenado en el inventario. • El fichero ha sido borrado por el usuario desde que se generó el inventario y la acción de borrado por parte del administrador. • Error al intentar eliminar el fichero.	Cadena de caracteres

Tabla 14.27: campos del fichero exportado Archivos con información personal

- **Herramienta de filtrado**

Campo	Comentario	Valores
Tipo de equipo	Filtra los equipos según su clase.	• Estación • Portátil • Servidor
Última vez visto	Muestra el inventario de los equipos que fueron vistos por última vez dentro del rango de fechas especificado.	• Todos • Últimas 24 horas • Últimos 7 días • Último mes • Último año

Tabla 14.28: campos de filtrado para el listado Archivos con información personal

Campo	Comentario	Valores
Información personal	Especifica el tipo de entidad que se buscará en el fichero PII.	• DNIs • Tarjetas de crédito • Permisos de conducir • Direcciones de correo electrónico • IPs • Direcciones • Números de teléfonos • Pasaportes • Cuentas bancarias • Números de la seguridad social • NIFs • Nombres y apellidos

Tabla 14.28: campos de filtrado para el listado Archivos con información personal

Listado Equipos con información personal

Este listado muestra el número de ficheros PII encontrados en cada uno de los equipos de la red. Dependiendo de la configuración de los filtros **Fecha 1** y **Fecha 2** el listado puede utilizarse para mostrar información de varios tipos:

- Si los campos **Fecha 1** y **Fecha 2** están establecidos, el listado muestra la variación en el número de ficheros PII encontrados en cada uno de los equipos de la red entre las dos fechas. Por lo tanto, el listado presenta una evolución en el número de ficheros PII encontrados en cada equipo de la red.
- Si los campos **Fecha 1** y **Fecha 2** están vacíos, el listado muestra los ficheros PII encontrados en cada equipo de la red, según haya sido el resultado del último inventario completo generado.
- Si el campo **Fecha 1** está establecido, el listado muestra los ficheros PII encontrados en cada equipo de la red, según haya sido el resultado del inventario completo creado en la fecha indicada.

Para ver el listado de ficheros PII encontrado en un equipo haz clic en el nombre del equipo. Se abrirá el listado **Archivos con información personal** filtrado por el nombre del equipo elegido.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres

Tabla 14.29: campos del listado Equipos con información personal

Campo	Comentario	Valores
Archivos (fecha)	Nombre del archivo.	Cadena de caracteres
Variación	Muestra la diferencia en el número de ficheros PII encontrados entre las fechas establecidas en Fecha 1 y Fecha 2. Si el número es positivo se mostrará el icono ↑. Si el número es negativo se muestra el icono ↓.	Numérico

Tabla 14.29: campos del listado Equipos con información personal

- **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Fecha 1	Fecha inicial utilizada en la evolución de ficheros PII.	Fecha
Fecha de inventario	Fecha en la que se generó el inventario completo del equipo.	Fecha
Archivos con información personal	Número de ficheros PII encontrados en la fecha indicada en Fecha 1.	Numérico
Pasaportes	Número de ficheros PII que contienen la entidad Pasaporte encontrada en la fecha indicada en Fecha 1.	Numérico
Tarjetas de crédito	Número de ficheros que contienen la entidad Tarjeta de crédito encontrada en la fecha indicada en Fecha 1.	Numérico
Cuentas bancarias	Número de ficheros que contienen la entidad Cuentas bancarias encontrada en la fecha indicada en Fecha 1.	Numérico
Permisos de conducir	Número de ficheros que contienen la entidad Permisos de conducir encontrada en la fecha indicada en Fecha 1.	Booelano
Números de la Seguridad Social	Número de ficheros que contienen la entidad Números de la Seguridad social encontrada en la fecha indicada en Fecha 1.	Numérico
Direcciones de correo electrónico	Número de ficheros que contienen la entidad Direcciones de correo electrónico encontrada en la fecha indicada en Fecha 1.	Numérico

Tabla 14.30: campos del fichero exportado Equipos con información personal

Campo	Comentario	Valores
NIFs	Número de ficheros que contienen la entidad NIF encontrada en la fecha indicada en Fecha 1.	Numérico
IPs	Número de ficheros que contienen la entidad IP encontrada en la fecha indicada en Fecha 1.	Numérico
Nombres y apellidos	Número de ficheros que contienen la entidad Nombre y apellidos encontrada en la fecha indicada en Fecha 1.	Numérico
Direcciones	Número de ficheros que contienen la entidad Dirección encontrada en la fecha indicada en Fecha 1.	Numérico
Números de teléfono	Número de ficheros que contienen la entidad Número de teléfono encontrada en la fecha indicada en Fecha 1.	Numérico
Fecha 2	Fecha inicial utilizada en la evolución de ficheros PII.	Fecha
Fecha de inventario	Fecha en la que se generó el inventario completo del equipo.	Fecha
Archivos con información personal	Número de ficheros PII encontrados en la fecha indicada en Fecha 2.	Numérico
Pasaportes	Número de ficheros que contienen la entidad Pasaporte encontrada en la fecha indicada en Fecha 2.	Numérico
Tarjetas de crédito	Número de ficheros que contienen la entidad Tarjeta de crédito encontrada en la fecha indicada en Fecha 2.	Numérico
Cuentas bancarias	Número de ficheros que contienen la entidad Cuentas bancarias encontrada en la fecha indicada en Fecha 2.	Numérico
Permisos de conducir	Número de ficheros que contienen la entidad Permisos de conducir encontrada en la fecha indicada en Fecha 2.	Booelano
Números de la Seguridad Social	Número de ficheros que contienen la entidad Números de la Seguridad social encontrada en la fecha indicada en Fecha 2.	Numérico
Direcciones de correo electrónico	Número de ficheros que contienen la entidad Direcciones de correo electrónico encontrada en la fecha indicada en Fecha 2.	Numérico
NIFs	Número de ficheros que contienen la entidad NIF encontrada en la fecha indicada en Fecha 2.	Numérico
IPs	Número de ficheros que contienen la entidad IP encontrada en la fecha indicada en Fecha 2.	Numérico

Tabla 14.30: campos del fichero exportado Equipos con información personal

Campo	Comentario	Valores
Nombres y apellidos	Número de ficheros que contienen la entidad Nombre y apellidos encontrada en la fecha indicada en Fecha 2.	Numérico
Direcciones	Número de ficheros que contienen la entidad Dirección encontrada en la fecha indicada en Fecha 2.	Numérico
Números de teléfono	Número de ficheros que contienen la entidad Número de teléfono encontrada en la fecha indicada en Fecha 2.	Numérico

Tabla 14.30: campos del fichero exportado Equipos con información personal

- **Herramienta de filtrado**

Campo	Comentario	Valores
Buscar	Filtra el listado por el nombre del equipo.	Cadena de caracteres
Fecha 1	Primera fecha a comparar.	Fecha
Fecha 2	Segunda fecha comparar.	Fecha
Tipo de equipo	Filtra los equipos según su clase.	• Estación • Portátil • Servidor
Información personal	Especifica el tipo de entidad que se buscará en el fichero PII.	• DNIs • Tarjetas de crédito • Permisos de conducir • Direcciones de correo electrónico • IPs • Direcciones • Números de teléfonos • Pasaportes • Cuentas bancarias • Números de la seguridad social • NIFs • Nombres y apellidos
Variación	Muestra los equipos cuya variación en el número de ficheros es positiva o negativa.	• **Positivo**: el número de ficheros encontrados en Fecha 2 es superior a Fecha 1. • **Negativo**: el número de ficheros encontrados en Fecha 2 es inferior a Fecha 1. • **Todos**

Tabla 14.31: campos de filtrado para el listado Equipos con información personal

- **Ventana detalle del equipo**

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta el apartado "**Información de equipo**" en la página **177** para obtener más información.

Listado Archivos eliminados por el administrador

Este listado muestra el estado de los ficheros que han recibido en el pasado tareas de borrado o restauración y que todavía permanecen en los equipos de la red, de forma accesible o en la zona de backup.

Campo	Comentario	Valores
Fecha	Fecha en la que el fichero cambió de estado.	Fecha
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Archivos con información personal
Ruta	Localización del archivo dentro del sistema de ficheros del equipo.	Cadena de caracteres
Efectuado por	Cuenta de la consola de administración que originó el cambio de estado del fichero.	Cadena de caracteres
Estado	Estado del fichero.	• Todos • Eliminado • Pendiente de eliminar • Restaurado • Pendiente de restaurar • Error restaurando

Tabla 14.32: campos del listado Archivos eliminados por el administrador

- **Campos mostrados en fichero exportado (historial)**

Este listado incluye las acciones de borrado y restauración que el administrador ejecutó sobre los ficheros de la red.

Campo	Comentario	Valores
Fecha	Fecha en la que el fichero cambió de estado.	Fecha
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Archivos con información personal
Ruta	Localización del archivo dentro del sistema de ficheros del equipo.	Cadena de caracteres
Efectuado por	Cuenta de la consola de administración que originó el cambio de estado del fichero.	Cadena de caracteres
Estado	Estado del fichero.	• Todos • Eliminado • Pendiente de eliminar • Restaurado • Pendiente de restaurar • Error restaurando

Tabla 14.33: campos del listado Archivos eliminados por el administrador

- **Campos mostrados en fichero exportado (historial detallado)**

Este listado incluye todas las acciones de borrado y restauración que el administrador ejecutó sobre los ficheros de la red a lo largo del tiempo.

Campo	Comentario	Valores
Fecha	Fecha en la que el fichero cambió de estado.	Fecha
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Archivos con información personal

Tabla 14.34: campos del listado Archivos eliminados por el administrador

Campo	Comentario	Valores
Ruta	Localización del archivo dentro del sistema de ficheros del equipo.	Cadena de caracteres
Efectuado por	Cuenta de la consola de administración que originó el cambio de estado del fichero.	Cadena de caracteres
Estado	Estado del fichero.	• Todos • Eliminado • Pendiente de eliminar
		• Restaurado • Pendiente de restaurar • Error restaurando

Tabla 14.34: campos del listado Archivos eliminados por el administrador

- **Herramienta de filtrado**

Campo	Comentario	Valores
Estado	Estado del fichero.	• Todos • Eliminado • Pendiente de eliminar • Restaurado • Pendiente de restaurar • Error restaurando

Tabla 14.35: campos de filtrado para el listado Archivos eliminados por el administrador

Extensiones de programas soportadas

Nombre de la suite	Producto	Extensiones
Office	Word	• DOC • DOT • DOCX • DOCM • RTF
	Excel	• XLS • XLSM • XLSX • XLSB • CSV
	PowerPoint	• PPT • PPS • PPSX • PPSM • SLDX • SLDM • POTX • PPTM • PPTX • POTM
OpenOffice	Writer	• ODM • ODT • OTT • OXT • STW • SXG • SXW
	Draw	• ODG • OTG • STD
	Math	• ODF • SXM
	Base	• ODB
	Impress	• OTP • ODP • STI • SXI

Tabla 14.36: listado de extensiones de programas soportadas

Nombre de la suite	Producto	Extensiones
	Calc	• OTS • ODS • SXC
Texto plano		TXT
Navegadores web	• Internet Explorer • Chrome • Opera • Otros	• HTM • HTML • MHT • OTH
Cliente de correo	• Outlook • Outlook Express	EML
Otros	Adobe Acrobat Reader	PDF
	Extensible Markup Language	XML
	Contribute	STC
	ArcGIS Desktop	SXD

Tabla 14.36: listado de extensiones de programas soportadas

Empaquetadores y algoritmos de compresión soportados

Nombre del compresor / empaquetador / algoritmo	Extensiones
7-ZIP	7Z
bzip2	BZ2
gzip	GZ
Binhex	HQX
LHARC	• LHA • LZH
Lempel-Ziv & Haruyasu	LZH
Lempel–Ziv–Oberhumer / lzop	LZO
Multi-Purpose Internet Mail	MME
Lotus Notes Traveler	NTS
Winrar	RAR
Tar	TAR
Tar & Gzip	TGZ
Uuencode	• UU • UUE
XXEncoding	• XX • XXE
PkZip / PKWare	ZIP

Tabla 14.37: listado de extensiones de empaquetadores / compresores soportados

Entidades y países soportados

Cytomic Data Watch soporta las entidades mostradas a continuación:

- Cuentas bancarias.
- Tarjetas de crédito.
- Número de identidad personal.
- Direcciones IP.
- Direcciones de correo electrónico.
- Números de teléfono.
- Números de carnet de conducir.
- Números de pasaporte.

- Números de la seguridad social.
- Nombres y apellidos.
- Direcciones físicas.

Países soportados

El formato de las distintas entidades reconocidas varía dependiendo del país. Cytomic Data Watch soporta la detección de entidades de los países mostrados a continuación:

- Alemania
- Austria
- Bélgica
- Dinamarca
- España
- Finlandia
- Francia
- Hungría
- Irlanda
- Italia
- Noruega
- Países Bajos
- Portugal
- Suecia
- Suiza
- Reino Unido

Capítulo 15

Cytomic Patch (Actualización de programas vulnerables)

Cytomic Patch es un módulo integrado en la plataforma Cytomic que localiza los equipos de la red que contienen software con vulnerabilidades conocidas, y los actualiza de forma automática y centralizada. De esta forma minimiza la superficie de ataque, evitando que el malware aproveche fallos del software instalado en los equipos de los usuarios y servidores para infectarlos.

Cytomic Patch es compatible con sistemas operativos Windows y detecta aplicaciones de terceros pendientes de actualizar o en EoL (End of Life), así como los parches y actualizaciones publicados por Microsoft para todos sus productos (sistemas operativos, bases de datos, suites ofimáticas, etc.).

> *Los equipos Windows XP SP3 y Windows Server 2003 SP2 requieren un equipo con el rol de caché / repositorio instalado en el mismo segmento de red para poder reportar y e instalar los parches pendientes. Un equipo Windows XP SP3 o Windows Server 2003 SP2 con el rol de caché / repositorio asignado tampoco podrá descargar parches.*

CONTENIDO DEL CAPÍTULO

Funcionalidades de Cytomic Patch

Toda la funcionalidad de Cytomic Patch se concentra en los puntos de la consola de administración mostrados a continuación:

- **Configuración del descubrimiento de parches a aplicar**: a través del perfil de configuración **Gestión de parches**, accesible desde el panel lateral en el menú superior **Configuración.** Consulta el apartado "**Configuración del descubrimiento de parches sin aplicar**".
- **Configuración de las exclusiones de parches**: desde el listado **Parches disponibles**. Consulta el apartado "**Excluir parches en todos o en algunos equipos**".
- **Visibilidad del estado de actualización del parque IT**: mediante widgets en un panel de control independiente, accesible desde el menú superior **Estado**, panel lateral **Gestión de parches**. Consulta el apartado "**Listado Estado de gestión de parches**".
- **Listados de parches pendientes de aplicar**: desde los listados **Estado de gestión de parches**, **Parches disponibles** y **Programas "End of Life"** accesibles desde el menú superior **Estado**, panel lateral **Mis listados, Añadir**. Consulta el apartado "**Listados en Cytomic Patch**".
- **Histórico de parches instalados**: desde el listado **Historial de instalaciones**, accesible desde el menú superior **Estado**, panel lateral **Mis listados, Añadir.** Consulta el apartado "**Listado Historial de instalaciones**".
- **Parcheo de equipos**: desde el menú superior **Tareas** y creando una tarea programada de tipo **Instalar parches**. También se pueden parchear los equipos desde los menús de contexto del árbol de grupos en el menú superior **Equipos,** de los listados y desde **Detalle de equipo**. Consulta el

apartado "**Descargar e instalar los parches**".

- **Desinstalación de parches**: elige una de las opciones siguientes:
  - Desde el widget **Últimas tareas de instalación de parches**, haz clic en el link **Ver historial de instalaciones**. Consulta el apartado "**Últimas tareas de instalación de parches**".
  - Desde el menú superior **Estado** haz clic en el panel lateral **Mis listados Añadir** y selecciona el listado **Historial de instalaciones**. Consulta el apartado "**Listado Historial de instalaciones**".
  - Desde en el menú superior **Tareas**, selecciona la tarea que instaló el parche a desinstalar y haz clic en **Ver parches instalados**.
- Al hacer clic en el parche se muestra su información asociada y el botón **Desinstalar** si es compatible con su desinstalación. Consulta el apartado "**Desinstalar los parches defectuosos**".

Flujo general de trabajo

Cytomic Patch es una herramienta integral que gestiona el parcheo y actualización de los sistemas operativos y programas instalados en los equipos de la red. Para conseguir reducir de forma eficiente la superficie de ataque de los equipos, es necesario seguir los pasos mostrados a continuación:

- Comprobar que Cytomic Patch funciona correctamente en los equipos instalados.
- Comprobar que los parches publicados están instalados.
- Aislar los equipos con vulnerabilidades conocidas sin parchear.
- Instalar los parches seleccionados.
- Desinstalación (Rollback) de los parches que muestran un mal funcionamiento.
- Excluir parches en todos o en algunos equipos.
- Comprobar que los programas instalados en los equipos no han entrado en EoL.
- Comprobar puntualmente el histórico de instalaciones de parches y actualizaciones.
- Comprobar puntualmente el estado del parcheo de equipos con incidencias.

Comprobar que Cytomic Patch funciona correctamente

Sigue los pasos mostrados a continuación:

- Comprueba que los equipos de la red tienen una licencia asignada de Cytomic Patch y que el módulo está instalado y en funcionamiento. Utiliza el widget "**Estado de gestión de parches**".
- Comprueba que los equipos con una licencia de Cytomic Patch asignada se comunican con la nube de Cytomic. Utiliza el widget **"Tiempo desde la última comprobación".**
- Comprueba que los equipos donde se instalarán los parches tienen el servicio Windows Update en

ejecución con las actualizaciones automáticas desactivadas.

> *Activa la configuración **Desactivar Windows Update en los equipos** en el perfil de configuración de cifrado para que Cytomic EPDR pueda gestionar correctamente el servicio. Consulta el apartado "**Configuración general**".*

Comprobar que los parches publicados están instalados

Los parches y actualizaciones se publican de forma constante según los proveedores del software instalado en la red detectan vulnerabilidades y las corrigen. Estos parches tienen asociada una criticidad y un tipo.

- Para obtener una visión general de los parches pendientes de instalar según su tipo y criticidad utiliza el widget "**Criticidad de los parches**".
- Para ver los parches pendientes de instalación en un equipo o grupo de equipos:
  - En el árbol de equipos (menú superior **Equipos**, pestaña **Carpeta** en el panel lateral) haz clic en el menú de contexto de un grupo que contenga equipos Windows y selecciona **Visualizar parches disponibles**. Se mostrará el listado "**Listado Parches disponibles**" filtrado por el grupo.

ó

  - En el panel de equipos (menú superior **Equipos**, panel derecho) haz clic en el menú de contexto de un equipo y selecciona **Visualizar parches disponibles**. Se mostrará el listado "**Listado Parches disponibles**" filtrado por el equipo.
- Para obtener una visión global detallada de los parches pendientes de instalar:
  - En el menú superior **Estado** haz clic en el panel lateral **Mis listados**, **Añadir** y selecciona el listado "**Listado Parches disponibles**".
  - Utiliza la herramienta de filtrado para acotar la búsqueda.
- Para buscar los equipos que no tienen instalado un parche concreto:
  - En el menú superior **Estado** haz clic en el panel lateral **Mis listados**, **Añadir** y selecciona el listado "**Listado Parches disponibles**".
  - Utiliza la herramienta de filtrado para acotar la búsqueda.
  - Haz clic en el menú de contexto del equipo – parche a buscar y selecciona el menú **Visualizar equipos** con el parche disponible para su instalación.

Aíslar los equipos con vulnerabilidades conocidas sin parchear

Para aislar un equipo que todavía no ha recibido un parche ya publicado que corrige una vulnerabilidad conocida:

- En el menú superior **Estado** haz clic en el link **Añadir** del panel lateral y selecciona el listado "**Parches disponibles**".
- Haz clic en el menú de contexto de un parche y elige en el menú desplegable la opción **Aislar**

equipo.

Descargar e instalar los parches

Para instalar los parches y actualizaciones Cytomic Patch utiliza la infraestructura de tareas implementada en Cytomic EPDR.

> *La instalación de parches publicados por Microsoft no se completará con éxito si el servicio Windows Update está deshabilitado en el equipo del usuario o servidor.*

Los parches y actualizaciones se instalan mediante tareas rápidas o programadas. Las tareas rápidas instalan el parche en tiempo real pero no reinician el equipo del usuario, aunque sea requisito para completar la instalación. Las tareas programadas permiten configurar los parámetros de la actualización de parches. Consulta el capítulo "**Tareas**" en la página **503** para obtener información general sobre las Tareas en Cytomic EPDR.

- **Descarga de parches y ahorro de ancho de banda**

Antes de la instalación de un parche es necesaria su descarga desde los servidores del proveedor de software. Esta descarga se produce de forma transparente e independiente en cada equipo cuando se lanza la tarea de instalación. Para minimizar el ancho de banda consumido se puede aprovechar la infraestructura de nodos caché / repositorios instalada en la red del cliente.

> *No es posible descargar parches ni actualizaciones a través de un nodo con el rol proxy asignado. Consulta la sección "***Configuración de los roles del agente Cytomic***" en la página* **212** *para obtener más información sobre los roles de* Cytomic EPDR.

Los nodos caché / repositorio almacenan los parches durante un periodo máximo de 30 días, transcurrido el cual se eliminarán. Si un equipo solicita a un nodo caché la descarga de un parche y éste no lo tiene en su repositorio, el equipo dará un tiempo al nodo caché para que lo descargue. Este tiempo depende del tamaño del parche a descargar. Si no es posible la descarga, el equipo la iniciará de forma directa.

Una vez aplicados los parches en los equipos, éstos se borrarán del medio de almacenamiento donde residen.

- **Secuencia de tareas de instalación**

Las tareas de instalación de parches pueden requerir la descarga de parches desde los servidores del proveedor si los nodos con el rol de caché / repositorio no los tienen previamente almacenados. En este escenario, las tareas inmediatas inician la descarga de los parches necesarios en el momento en que éstas se crean, de forma que puede darse un alto consumo de ancho de banda si afectan a muchos equipos, o el volumen de la descarga es alto.

Las tareas programadas de instalación de parches comienzan la descarga de parches en el momento en que se indica en su configuración, pero si varias tareas coinciden en el punto de inicio se introduce un retardo aleatorio de hasta un máximo de 2 minutos para evitar el solapamiento de descargas y minimizar hasta cierto punto el consumo de ancho de banda.

- **Estrategias de instalación de parches**

La consola de administración es una herramienta muy flexible que permite instalar los parches de múltiples maneras. De forma general se siguen las estrategias siguientes:

- Para instalar uno o varios parches concretos utiliza el listado "**Listado Parches disponibles**" y configura la herramienta de filtrado.
- Para instalar todos los parches de una criticidad concreta o asociados a un programa o fabricante, utiliza las tareas inmediatas o programadas.
- Para instalar parches en equipos concretos o en un grupo utiliza el Árbol de grupos.

A continuación, se indican las combinaciones posibles de parches y destinos, y se describen los pasos a ejecutar en cada una de ellas.

Destino / parche	Uno o varios parches específicos	Uno, varios o todos los tipos de parches
Uno o varios equipos	Caso I: desde el listado Parches disponibles	Caso II: desde el árbol de equipos
Un grupo	Caso III: desde el listado Parches disponibles	Caso IV: desde el árbol de equipos
Varios o todos los grupos	Caso V: desde el listado Parches disponibles	Caso VI: desde el menú superior Tareas

Tabla 15.1: instalación de parches según el destino y el conjunto de parches instalado

Caso I: desde el listado Parches disponibles

Para instalar uno o más parches concretos en uno o varios equipos:

- En el menú superior **Estado** haz clic en el panel lateral **Mis listados Añadir** y selecciona el listado "**Listado Parches disponibles**".
- Utiliza la herramienta de filtrado para acotar la búsqueda.
- Haz clic en las casillas de selección de los equipos – parches a instalar y selecciona **Instalar** en la barra de acciones para crear una tarea rápida o **Programar instalación** para crear una tarea programada.

Caso II: desde el árbol de equipos

Para instalar uno varios o todos los tipos de parches en uno o varios equipos:

- En el menú superior **Equipos**, pestaña **Carpetas** del árbol de equipos (panel izquierdo) haz clic en el grupo al que pertenecen los equipos. Si los equipos pertenecen a varios grupos haz clic en el grupo

raíz Todos.

- Haz clic en las casillas de selección de los equipos que recibirán el grupo de parches.
- En la barra de acciones haz clic en **Programar la instalación de parches.**
- Configura la tarea, haz clic en el botón **Guardar** y publícala.

Caso III: desde el listado Parches disponibles

Para instalar un parche concreto en un grupo de equipos:

- En el menú superior **Equipos**, pestaña **Carpetas** del árbol de equipos (panel izquierdo) haz clic en el menú de contexto del grupo.
- Haz clic en el menú **Visualizar parches disponibles**. Se mostrará el listado "**Listado Parches disponibles**" filtrado por el grupo.
- Utiliza el campo **Parche** de la herramienta de filtrado para listar únicamente el parche a instalar.
- Selecciona todos los equipos del listado con las casillas de selección.
- Haz clic en **Instalar** en la barra de acciones para crear una tarea rápida o **Programar instalación** para crear una tarea programada.

Para instalar varios parches concretos en un grupo de equipos repite el punto anterior tantas veces como parches se quieran instalar.

Caso IV: desde el árbol de equipos

Para instalar uno, varios o todos los tipos de parches en un grupo de equipos:

- En el menú superior **Equipos**, pestaña **Carpetas** del árbol de equipos (panel izquierdo) haz clic en el menú de contexto del grupo.
- Haz clic en el menú **Programar instalación de parches**. Se mostrará la ventana de la tarea.
- Configura la tarea con el tipo o tipos de parches que se instalarán en el grupo, haz clic en el botón **Guardar** y publícala.

Caso V: desde el listado Parches disponibles

Para instalar un parche concreto en varios grupos de equipos:

- En el menú superior **Estado** haz clic en el panel lateral **Mis listados Añadir** y selecciona el listado "**Listado Parches disponibles**".
- Utiliza la herramienta de filtrado para acotar la búsqueda del parche.
- Haz clic en la casilla del parche a instalar y selecciona **Programar instalación** para crear una tarea.
- Haz clic en el menú superior **Tareas** y edita la tarea creada en el punto anterior.
- En el campo **Destinatarios** añade los grupos que recibirán el parche en **Grupos de equipos** y elimina los **Equipos Adicionales**.
- Haz clic en **Atrás**, configura la tarea y haz clic en **Guardar**.

- Publica la tarea.

Para instalar varios parches concretos en varios grupos de equipos repite el apartado anterior tantas veces como parches tengas que instalar.

Caso VI: desde el menú superior Tareas

Para instalar uno, varios o todos los tipos de parches en varios o todos los grupos de equipos:

- En el menú superior haz clic en **Tareas**, haz clic en **Añadir tarea** y selecciona **Instalar parches**.
- Establece el campo **Destinatarios** para determinar los equipos y grupos que recibirán la tarea de instalación.
- Indica la programación horaria de la tarea. Consulta el apartado "**Programación horaria y repetición de la tarea**" en la página **505** para obtener más información.
- Indica el nivel de criticidad de los parches a instalar.
- Indica qué productos recibirán parches utilizando las casillas de selección en el árbol de productos. Dado que el árbol de productos es un recurso vivo que cambia a lo largo del tiempo, ten en cuenta las siguientes reglas al seleccionar los elementos del árbol:
  - Al seleccionar un nodo se marcarán todos sus nodos hijos y sus descendientes. Por ejemplo, al seleccionar Adobe se seleccionarán todos los nodos que quedan por debajo de este nodo.
  - Si seleccionas un nodo y posteriormente Cytomic EPDR agrega de forma automática un nuevo nodo hijo en la rama seleccionada, este nodo también quedará seleccionado de forma automática. Por ejemplo, si seleccionas el nodo Adobe se seleccionarán todos sus nodos hijos, y si posteriormente dentro de Adobe Cytomic EPDR agrega un nuevo nodo (un nuevo programa o familia de programas), éste quedará seleccionado de forma automática. Por el contrario, si se seleccionan manualmente algunos nodos hijo individuales de Adobe y Cytomic EPDR añade un nuevo nodo hijo, éste no se seleccionará de forma automática.
  - Los programas a parchear se evalúan en el momento en que se ejecuta la tarea, no en el momento de su creación o configuración. Esto implica que si Cytomic EPDR agrega una nueva entrada en el árbol después de que el administrador haya configurado una tarea de parcheo, y esta entrada es seleccionada de forma automática según la regla del punto anterior, se instalarán los parches asociados a ese nuevo programa en el momento en que se ejecute la tarea.
- Establece las opciones de reinicio en el caso de que sea un requisito reiniciar el puesto de trabajo o servidor para completar la instalación del parche:
  - **No reiniciar automáticamente**: al terminar la tarea de instalación de parches se le muestra al usuario del equipo una ventana con las opciones **Reiniciar ahora** y **Recordar más tarde**. En caso de elegir ésta última, se volverá a mostrar a las 24 horas siguientes.
  - **Reiniciar automáticamente solo las estaciones de trabajo**: al terminar la tarea de instalación de parches se muestra al usuario del equipo una ventana con las opciones **Reiniciar ahora**, **Botón de minimizar** y **Cuenta atrás de 4 horas**. Cada 30 minutos se maximizará la pantalla como recordatorio de la proximidad del reinicio. Cuando falte menos de una hora para el reinicio el botón de minimizar se deshabilitará. Cuando la cuenta atrás se haya completado el equipo se

reiniciará automáticamente.

- **Reiniciar automáticamente solo los servidores**: el comportamiento es idéntico a la opción **Reiniciar automáticamente solo las estaciones de trabajo** pero aplica solo a equipos de tipo servidor.
- **Reiniciar automáticamente tanto las estaciones de trabajo como los servidores**: el comportamiento es idéntico a la opción **Reiniciar automáticamente solo las estaciones de trabajo** pero aplica tanto a estaciones de trabajo como a servidores**.**

- Haz clic en **Guardar** y publica la tarea.

Descargar los parches de forma manual

En algunos casos Cytomic EPDR no puede obtener una URL de descarga para iniciar la instalación del parche de forma automática. El motivo de este escenario es diverso: puede ser debido a que el parche es de pago, o porque no es un parche público y requiere un registro previo del usuario a la descarga, entre otras razones. Debido a los EULAs que protegen a muchos parches, éstos no pueden ser descargados por Cytomic para su redistribución, de forma que será el propio administrador el encargado de descargar de forma manual el parche y compartirlo en la red para que los equipos se actualicen.

Cytomic EPDR implementa un mecanismo mediante el cual integra estas descargas manuales en la consola web para que el administrador pueda añadir los parches descargados manualmente.

Para añadir un parche de forma manual al respositorio sigue los pasos mostrados a continuación:

- Identifica los parches que requieren una descarga manual.
- Obtén la URL de descarga.
- Integra el parche descargado en el repositorio de parches.
- Habilita el parche descargado para su instalación.
- Opcional: deshabilita un parche ya habilitado para su instalación

Identifica los parches que requieren una descarga manual

- Desde el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una lista con todos los listados disponibles.
- Elige el listado **Parches disponibles** y configura los siguientes filtros:
  - **Instalación**: Requiere descarga manual.
  - **Mostrar parches no descargables**: Si.
- Haz clic en el botón **Filtrar**. El listado mostrará todos los parches reportados por Cytomic EPDR como necesarios para actualizar los equipos de la red y que no son descargables de forma automática.

Obtén la URL de descarga

- Con el listado de parches no descargables del apartado "**Identifica los parches que requieren una descarga manual**" haz clic en un parche concreto. Se mostrarán los detalles del parche.
- Haz clic en el campo **URL de descarga** para iniciar la descarga del parche y guarda el nombre del fichero que aparece en el campo **Nombre del archivo**.

Integra el parche descargado en el repositorio de parches

- Localiza en la red un equipo con Cytomic EPDR instalado y el rol de caché asignado y copia el fichero descargado en la ruta siguiente:

```
c:\Programdata\Panda Security\Panda Aether Agent\Repository\ManuallyDeploy.
```

> *Si la unidad de almacenamiento del equipo ha cambiado a otra diferente de la establecida por defecto en el proceso de instalación del software Cytomic EPDR, accede a la siguiente ruta:*
>
> `x:\Panda Security\Panda Aether Agent\Repository\ManuallyDeploy`
>
> *Siendo x la unidad donde reside el repositorio del equipo. Consulta el apartado "**Establecer la unidad de almacenamiento**" en la página 214 para mas información.*

- Si la carpeta **ManuallyDeploy** no existe, créala con permisos de administrador para lectura y escritura.
- Si es necesario, renombra el parche recién copiado con el nombre obtenido en el campo **Nombre de archivo** del apartado "**Obtén la URL de descarga**".

Habilita el parche descargado para su instalación

- Una vez copiado el parche en el repositorio vuelve al listado **Parches disponibles** y haz clic en el menú de contexto asociado al parche descargado manualmente.
- Elige la opción **Marcar como descargado manualmente** del menú desplegable. A partir de este momento el parche pasará del estado previo **Requiere descarga manual** al estado **Pendiente (descargado manualmente)** para todos los equipos que requieran su instalación. Una vez en estado **Pendiente (descargado manualmente)** se habilitarán todas las opciones necesarias en el menú de contexto del parche para poder instalarse de la misma forma que un parche

descargado automáticamente. Consulta el apartado "**Descargar e instalar los parches**".

> *Cytomic EPDR no comprueba que un parche en estado Pendiente (descargado manualmente) realmente exista en algún equipo con el rol de caché asignado. De igual manera, tampoco comprueba que todos los equipos de la red que deberían recibir el parche tienen asignado un equipo caché con el parche copiado en su repositorio. Es responsabilidad del administrador asegurarse de que los equipos caché que se utilizarán en la descarga de parches tienen en la carpeta ManuallyDeploy los parches necesarios descargables de forma manual.*

Deshabilita un parche para su instalación

Para retirar del repositorio un parche previamente integrado sigue los pasos mostrados a continuación:

- En el listado **Parches disponibles** configura un filtro de las siguientes características:
  - **Instalación**: Pendiente (descargado manualmente).
  - **Mostrar parches no descargables**: Si.
- Haz clic en el botón **Filtrar**. El listado mostrará todos los parches descargados de forma manual y habilitados para su instalación.
- Haz clic en el menú de contexto asociado al parche habilitado para su instalación y elige la opción **Marcar como "Requiere descarga manual"** . A partir de este momento el parche dejará de pertenecer al repositorio de parche instalables y perderá las opciones de su menú de contexto.

Desinstalar los parches defectuosos

En alguna ocasión puede suceder que los parches publicados por los proveedores del software no funcionen correctamente. Aunque se recomienda seleccionar un reducido grupo de equipos de prueba previo al despliegue en toda la red, Cytomic EPDR también soporta la desinstalación de parches (Rollback).

Requisitos para desinstalar un parche instalado

- El rol del administrador tiene el permiso **Instalar / desinstalar** parche habilitado. Consulta el apartado "**Instalar / desinstalar y excluir parches**" en la página **80** para obtener más información.
- La instalación del parche a desinstalar finalizó completamente.
- El parche se puede desinstalar. No todos los parches soportan esta funcionalidad.

Desinstalar un parche ya instalado

- Accede a la pantalla de desinstalación del parche:
  - En el menú superior **Estado** haz clic en el panel lateral **Mis listados Añadir** y selecciona **"Listado Historial de instalaciones".**

- Accede al listado de parches instalados en el menú superior **Tareas**, selecciona la tarea que instaló el parche a desinstalar y haz clic en el link **Ver parches instalados**, situado en la parte superior derecha de la ventana de la tarea.
- Accede al widget "**Últimas tareas de instalación de parches**" en el menú superior **Estado**, menú lateral **Gestión de parches** y haz clic en el link **Historial de instalaciones**.

- Selecciona de la lista el parche a desinstalar.
- Si el parche se puede desinstalar, se mostrará el botón **Desinstalar el parche**. Haz clic en el botón para mostrar la ventana de selección de equipos:
  - Selecciona **Desinstalar en todos los equipos** para eliminar el parche de todos los equipos de la red.
  - Selecciona **Desinstalar solo en…** para eliminar el parche del equipo indicado.
- Cytomic EPDR creará una tarea de ejecución inmediata que desinstalará el parche.
- Si el parche requiere el reinicio del equipo de usuario para completar su desinstalación, se esperará a que el usuario lo reinicie de forma manual.

> *Un parche desinstalado volverá a mostrarse en los listados de parches disponibles a no ser que haya sido excluido. Si has configurado una tarea programada de instalación de parches y el parche no ha sido excluido, éste se volverá a instalar en su próxima ejecución. Si el parche ha sido retirado por el proveedor, no se volverá a mostrar ni a instalar. Consulta el apartado "***Excluir parches en todos o en algunos equipos***".*

Excluir parches en todos o en algunos equipos

Para evitar la instalación de los parches que han tenido un mal funcionamiento o que cambian de forma importante las características del programa que los recibe, el administrador de la red puede excluirlos a discreción. Para ello sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Estado** y en el panel lateral **Añadir** en la zona **Mis listados**. Elige el listado **Parches disponibles**. Este listado muestra una linea por cada par equipo - parche disponible. Un parche disponible es aquel que no ha sido instalado en algún equipo de la red o que ha sido desinstalado.
- Para excluir un único parche haz clic en el menú de contexto asociado al parche ⋮ y elige la opción **Excluir** ⃠. Se mostrará una ventana emergente para seleccionar el tipo de exclusión.
  - **Excluir solo para el equipo X**: excluye el parche elegido en el equipo indicado en el listado.
  - **Excluir para todos los equipos**: el parche elegido se excluirá de todos los equipos de la red.
- Para excluir varios parches y/o un único parche de varios equipos selecciónalos con las casillas de selección, haz clic en la barra de acciones y elige la opción **Excluir** ⃠. Se mostrará una ventana emergente para seleccionar el tipo de exclusión:
  - **Excluir solo para los equipos seleccionados**: excluye los parches elegidos en los equipos

indicados en el listado.

- **Excluir para todos los equipos**: los parches elegidos se excluirán de todos los equipos de la red.

> *Los parches excluidos hacen referencia a una versión concreta del parche, de forma que si se excluye un determinado parche y posteriormente el proveedor del software publica otro posterior, éste último no se excluirá automáticamente.*

Comprueba que los programas no han entrado en EoL

Los programas que han entrado en EoL no reciben ningún tipo de actualización por parte de los proveedores de software, de forma que se recomienda sustituirlos por alternativas equivalentes o por versiones más avanzadas.

Para localizar los programas actualmente en EOL o que entrarán en EOL en breve:

- Haz clic en el menú superior **Estado**, panel lateral **Gestión de parches:**
- En el widget "**Programas "End of life"**" se muestra la información dividida en tres series:
  - **Actualmente en EOL**: programas instalados en la red que ya no reciben actualizaciones de sus respectivos proveedores.
  - **Actualmente o en 1 año en EOL**: programas instalados en la red que ya están en EOL o que entrarán en EOL en el plazo de un año.
  - **Con fecha EOL conocida**: programas instalados en la red que tienen fecha EOL conocida.

Para localizar todos los programas con información de EOL conocida:

- Haz clic en el menú superior **Estado**, panel lateral **Mis listados, Añadir.**
- Selecciona el **"Listado Programas End of Life". .**

El listado contiene una entrada por cada par equipo – programa en EoL.

Comprueba el histórico de instalaciones de parches y actualizaciones

Para determinar si un parche concreto está instalado en los equipos de la red:

- Haz clic en el menú superior **Estado**, panel lateral **Mis listados, Añadir.**
- Selecciona "**Listado Historial de instalaciones**".

El listado contiene una entrada por cada par equipo – parche instalado, junto con información sobre su nombre, versión, programa o sistema operativo al que afecta y criticidad / tipo del parche.

Comprueba el nivel de parcheo de los equipos con incidencias

Cytomic EPDR relaciona los equipos que tienen incidencias detectadas con su nivel de parcheo, de forma que es posible determinar si un equipo infectado o con amenazas detectadas tiene o no aplicados todos los parches que se han publicado.

Para ver si un equipo con una incidencia detectada tiene parches pendientes de instalación:

- En el menú superior **Estado**, widgets **Amenazas detectadas por el antivirus, Actividad del malware, Actividad de PUPs, Actividad de Exploits** y **Programas actualmente bloqueados en clasificación** haz clic en una amenaza - equipo. Se mostrará la información de la amenaza detectada en el equipo.
- En la sección **Equipo afectado** haz clic en el botón **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles** filtrado por el equipo.
- Selecciona todos los parches disponibles para este equipo y haz clic en la barra de acciones **Instalar** para crear una tarea inmediata que parcheará el equipo.

*Debido a que este proceso puede implicar descargas de parches desde los servidores del proveedor del software a parchear, y por lo tanto retrasar su aplicación en el tiempo, se recomienda aislar el equipo de la red si el equipo ha sido infectado y muestra tráfico de red en su ciclo de vida. De esta forma se minimiza el riesgo de propagación de la infección en la red del cliente mientras el proceso de parcheo se completa. Consulta el capítulo "***Análisis forense***" en la página **449** para obtener más información acerca del ciclo de vida del malware y el apartado "**Aislar uno o varios equipos de la red de la organización**".*

Configuración del descubrimiento de parches sin aplicar

Cytomic Patch mantiene un inventario de los parches y actualizaciones pendientes de instalación de todos los equipos de la red que tienen una licencia del módulo asignada y en funcionamiento.

Para configurar el descubrimiento de parches y actualizaciones:

- Haz clic en el menú superior **Configuración**, panel lateral **Gestión de parches.**
- Haz clic en el botón **Añadir** y completa la configuración con la información mostrada a continuación.
- Asigna la nueva configuración a los equipos de la red con una licencia Cytomic Patch activada.

Configuración general

- Haz clic en **Desactivar Windows Update en los equipos** para que Cytomic Patch gestione las actualizaciones de forma exclusiva y sin interferencias con la configuración local de Windows Update.
- Haz clic en el selector **Buscar parches automáticamente** para activar la búsqueda de parches. Si el selector no está activado los parches pendientes de instalación no se mostrarán en los listados, aunque las tareas de instalación de parches podrán aplicarlos de forma independiente.

Frecuencia de la búsqueda

Buscar parches con la siguiente frecuencia establece cada cuanto tiempo Cytomic Patch consulta los parches instalados en los equipos y los compara con las bases de datos de parches disponibles.

Criticidad de los parches

Establece la criticidad de los parches que Cytomic Patch busca en las bases de datos de parches disponibles.

> ⚠ *La criticidad de cada parche está establecida por cada proveedor del software afectado por la vulnerabilidad. Este criterio de clasificación no es uniforme y se recomienda comprobar previamente la descripción del parche para aquellos que no estén clasificados como "críticos", con el objetivo de evitar su instalación si no se padecen los síntomas descritos.*

Paneles / widgets en Cytomic Patch

A continuación, se detallan los distintos widgets implementados en el panel de control **Gestión de parches,** sus distintas áreas y zonas activas incorporadas y los tooltips y su significado.

Estado de gestión de parches

Muestra los equipos donde Cytomic Patch está funcionando correctamente y aquellos con errores o problemas en la instalación o en la ejecución del módulo. El estado del módulo se representa mediante un círculo con distintos colores y contadores asociados. El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

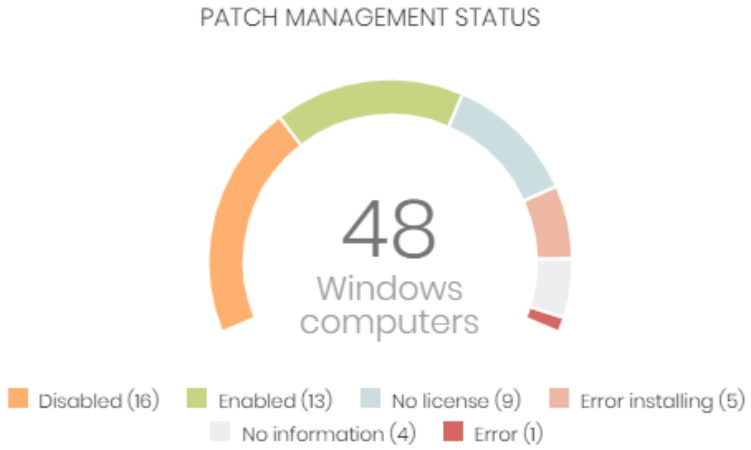


Figura 15.1: panel de Estado de gestión de parches

- **Significado de las series**

Serie	Descripción
Activado	Indica el porcentaje de equipos en los que Cytomic Patch se instaló sin errores, su ejecución no presenta problemas y la configuración asignada permite buscar parches automáticamente.
Desactivado	Indica el porcentaje de equipos en los que Cytomic Patch se instaló sin errores, su ejecución no presenta problemas y la configuración asignada no permite buscar parches automáticamente.
Sin licencia	Equipos sin servicio de gestión de parches debido a que no se dispone de licencias suficientes, o no se les ha asignado una licencia disponible.
Error instalando	Indica los equipos donde el módulo no se pudo instalar.
Sin información	Equipos con licencia recientemente asignada y que todavía no han reportado su estado al servidor, o equipo con el agente sin actualizar.
Error	El módulo Cytomic Patch no responde a las peticiones del servidor y su configuración difiere de la establecida en la consola web.
Parte central	Refleja el número de total de equipos compatibles con el módulo Cytomic Patch.

Tabla 15.2: descripción de la serie Estado de gestión de parches

- **Filtros preestablecidos desde el panel**

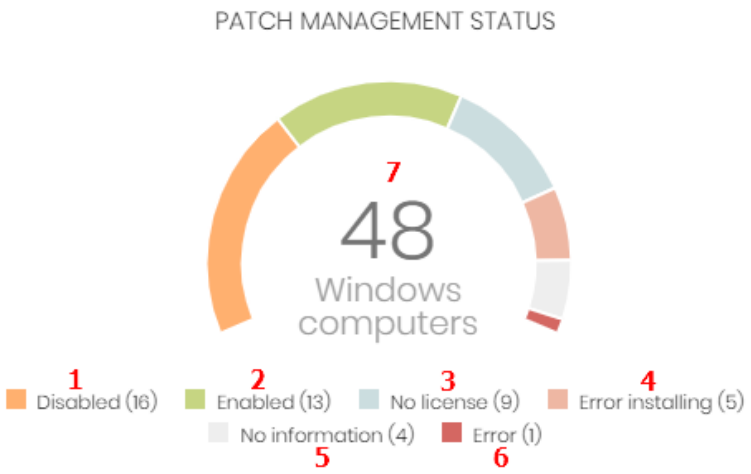


Figura 15.2: zonas activas del panel Estado de gestión de parches

Al hacer clic en las zonas indicadas en la figura 15.2 se abre el listado **Estado de gestión de parches** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de gestión de parches = Desactivado.
(2)	Estado de gestión de parches = Activado.

Tabla 15.3: definición de filtros del listado Estado de gestión de parches

Zona activa	Filtro
(3)	Estado de gestión de parches = Sin licencia.
(4)	Estado de gestión de parches = Error instalando.
(5)	Estado de gestión de parches = Sin información.
(6)	Estado de gestión de parches = Error.
(7)	Sin filtro.

Tabla 15.3: definición de filtros del listado Estado de gestión de parches

Tiempo desde la última comprobación

Muestra los equipos de la red que no han conectado con la nube de Cytomic en un determinado periodo de tiempo para comprobar su estado de parcheo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.

Figura 15.3: panel Tiempo desde la última comprobación

- **Significado de las series**

Serie	Descripción
72 horas	Número de equipos que no comprobaron su estado de parcheo en las últimas 72 horas.
7 días	Número de equipos que no comprobaron su estado de parcheo en las últimas 7 días.
30 días	Número de equipos que no comprobaron su estado de parcheo en los últimas 30 días.

Tabla 15.4: descripción de la serie Tiempo desde la última comprobación

- **Filtros preestablecidos desde el panel**

Figura 15.4: zonas activas del panel Tiempo desde la ultima comprobación

Al hacer clic en las zonas indicadas en la figura **15.4** se abre el listado **Estado de gestión de parches** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 3 días y Estado de gestión de parches = Activado o Desactivado o Sin información o Error.
(2)	Última conexión = Hace más de 7 días y Estado de gestión de parches = Activado o Desactivado o Sin información o Error.
(3)	Última conexión = Hace más de 30 días y Estado de gestión de parches = Activado o Desactivado o Sin información o Error.

Tabla 15.5: definición de filtros del listado Estado de gestión de parches

Programas "End of life"

Muestra la información relativa al "end of life" de los programas instalados en los equipos de la red, agrupados según el plazo restante.

Figura 15.5: panel Programas "End of life"

- **Significado de las series**

Serie	Descripción
Actualmente en EOL	Programas instalados en el parque informático que ya entraron en EOL.
Actualmente o en 1 año en EOL	Programas instalados en el parque informático que ya han entrado en EOL o entrarán dentro de un año.

Tabla 15.6: descripción de la serie Programas "End of life"

Serie	Descripción
Con fecha EOL conocida	Programas instalados en el parque informático cuya fecha de EOL es conocida.

Tabla 15.6: descripción de la serie Programas "End of life"

- **Filtros preestablecidos desde el panel**

Figura 15.6: zonas activas del panel Programas "End of life"

Al hacer clic en las zonas indicadas en la figura 15.6 se abre el listado **Programas "End Of Life'** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Fecha de inventario = Actualmente en "End Of Life".
(2)	Fecha de inventario = Actualmente o en 1 año en "End Of Life".
(3)	Fecha de inventario = Todos.

Tabla 15.7: definición de filtros del listado Programas "End Of Life'

Últimas tareas de instalación de parches

*Consulta el apartado "**Gestionar tareas**" en la página **506** para obtener más información sobre como modificar una tarea ya creada.*

Muestra un listado de las últimas tareas de instalación de parches y actualizaciones creadas. Este widget está formado por varios enlaces que permiten gestionar las tareas de instalación de parches:

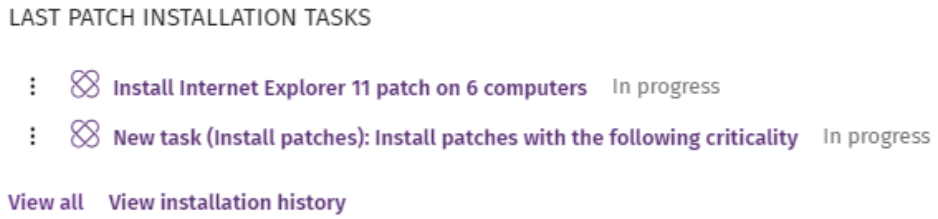


Figura 15.7: panel de Últimas tareas de instalación de parches

- Haz clic en una tarea para editar su configuración.
- Haz clic en el link **Ver todas** para acceder directamente al menú superior **Tareas** donde se muestran todas las tareas creadas.
- Haz clic en el link **Ver historial de instalaciones** para acceder al listado **Historial de instalaciones** con todas las tareas de instalación de parches terminadas con éxito o con error.
- Haz clic en el menú de contexto asociado a una tarea para mostrar una lista desplegable con las opciones siguientes:
  - **Cancelar**: interrumpe la tarea si estaba en curso.
  - **Ver resultados**: muestra los resultados de la tarea.

Parches disponibles

Muestra un recuento de parejas parche - equipo sin aplicar, distribuido por la categoría del parche. Cada parche no aplicado se contabiliza tantas veces como equipos no lo tengan instalado.

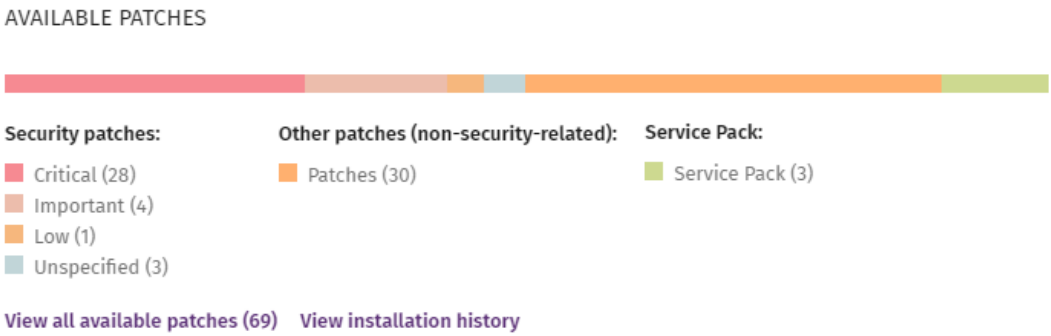


Figura 15.8: panel Parches disponibles

- **Significado de las series**

Serie	Descripción
Parches de seguridad - Críticos	Número de parches clasificados como de importancia crítica relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos seguridad - Importantes	Número de parches clasificados de importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad - Baja	Número de parches clasificados como de importancia baja relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad – No clasificados	Número de parches sin determinar su importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Otros parches (no de seguridad)	Número de parches no relativos a la seguridad del sistema y que no han sido aplicados todavía.

Tabla 15.8: descripción de la serie Parches disponibles

Serie	Descripción
Service Packs	Número de paquetes de parches y actualizaciones que no han sido aplicados todavía.
Ver todos los parches disponibles	Número de parches de cualquier importancia relativos o no a la seguridad del sistema y que no han sido aplicados todavía.
Ver parches excluidos	Número de parches excluidos de su instalación.

Tabla 15.8: descripción de la serie Parches disponibles

- **Filtros preestablecidos desde el panel**

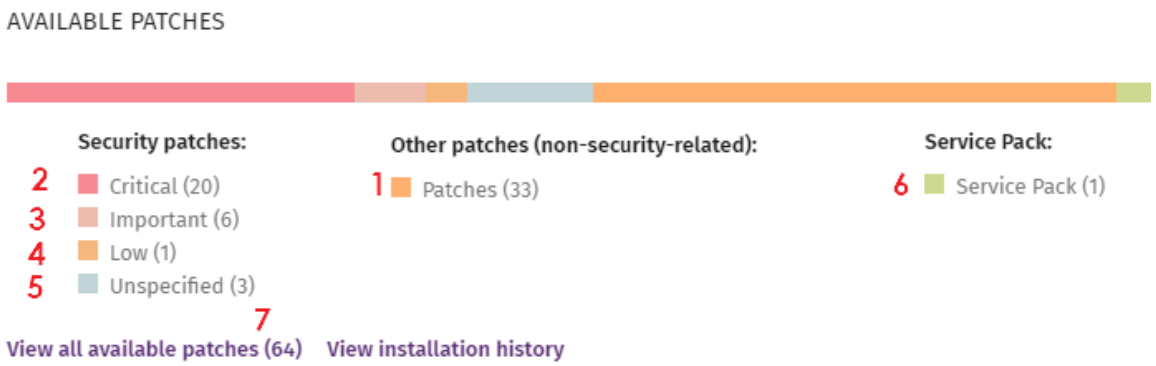


Figura 15.9: zonas activas del panel Parches disponibles

Al hacer clic en las zonas indicadas en la figura 15.9 se abre un listado con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(1)	Parches disponibles	Criticidad = Critica (de seguridad).
(2)	Parches disponibles	Criticidad = Importante (de seguridad).
(3)	Parches disponibles	Criticidad = Baja (de seguridad).
(4)	Parches disponibles	Criticidad = No clasificado (de seguridad).
(5)	Parches disponibles	Criticidad = Otros parches (no de seguridad).
(6)	Parches disponibles	Criticidad = Service Pack.
(7)	Parches disponibles	Sin filtros.
(8)	Historial de instalaciones	Sin filtros.
(9)	Parches excluidos	Sin filtros.

Tabla 15.9: definición de filtros del listado Parches disponibles

Listados en Cytomic Patch

Listado Estado de gestión de parches

Este listado muestra en detalle todos los equipos de la red compatibles con Cytomic Patch, incorporando filtros que permiten localizar aquellos puestos de trabajo y servidores que no estén recibiendo el servicio por alguno de los conceptos mostrados en el panel asociado.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Gestión de parches	Estado del módulo.	• Activado • Desactivado • Error instalando (motivo del error) • Sin licencia • Sin información • Error
Última comprobación	Fecha en la que Cytomic Patch consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Última conexión	Fecha del último envío del estado de Cytomic EPDR a la nube de Cytomic.	Fecha

Tabla 15.10: campos del listado Estado de gestión de parches

- **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres

Tabla 15.11: campos del fichero exportado Estado de gestión de parches

Campo	Comentario	Valores
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Versión del agente		Cadena de caracteres
Fecha instalación	Fecha en la que el módulo Cytomic Patch se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha de la última vez que el agente se conectó con la nube de Cytomic.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS • Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Servidor Exchange	Versión del servidor de correo instalada en el servidor.	Cadena de caracteres
Protección actualizada	Indica si el módulo de la protección instalado en el equipo es la última versión publicada.	Booleano
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Fecha de última actualización	Fecha de la descarga del fichero de firmas.	Fecha
Estado de gestión de parches	Estado del módulo.	• Activado • Desactivado • Error instalando • Sin licencia • Sin información • Error
Requiere reinicio	El equipo no se ha reiniciado para completar la instalación de uno o más parches descargados.	Booleano
Fecha de la última comprobación	Fecha en la que Cytomic Patch consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Estado de aislamiento	Indica si el equipo ha sido aislado de la red o se comunica con sus equipos vecinos de forma normal.	• Aislado • No aislado

Tabla 15.11: campos del fichero exportado Estado de gestión de parches

Campo	Comentario	Valores
Fecha error instalación	Fecha en la que se intentó la instalación del módulo Cytomic Patch y se produjo el error.	Fecha
Error instalación	Motivo del error de instalación.	• Error en la descarga • Error en la ejecución

Tabla 15.11: campos del fichero exportado Estado de gestión de parches

- **Herramienta de filtrado**

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Última comprobación	Fecha en la que Cytomic Patch consultó a la nube para comprobar si se han publicado nuevos parches.	• Todos • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Última conexión	Fecha de la última vez que el agente se conectó con la nube de Cytomic.	Fecha
Pendiente de reinicio para completar instalación de parches	El equipo no se ha reiniciado para completar la instalación de uno o más descargados.	Booleano
Estado de gestión de parches	Estado del módulo.	• Activado • Desactivado • Error instalando • Sin licencia • Sin información • Error

Tabla 15.12: campos de filtrado para el listado Estado de gestión de parches

- **Ventana detalle del equipo**

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta el apartado "**Información de equipo**" en la página **177** para obtener más información.

Listado Parches disponibles

Muestra el detalle de todos los parches sin instalar en los equipos de la red y publicados por Cytomic. Cada línea del listado refleja un par parche – equipo de la red.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Instalación	Indica el estado de la instalación del parche: • **Pendiente**: el parche está disponible para el equipo y no ha completado su instalación. • **Requiere descarga manual**: el parche requiere que el administrador descargue de forma manual el parche y lo copie en un equipo con el rol de cache asignado. Consulta el apartado "**Descargar los parches de forma manual**". • **Pendiente (descargado manualmente)**: el parche ya fue descargado de forma manual y forma parte del repositorio de parches. Consulta el apartado "**Descargar los parches de forma manual**".	

Tabla 15.13: campos del listado Parches disponibles

Campo	Comentario	Valores
Menú de contexto	Despliega un menú de acciones: • **Instalar**: crea una tarea inmediata de instalación del parche en el equipo elegido. • **Programar instalación**: crea una tarea configurable de instalación del parche elegido. • **Aislar equipo**: aísla el equipo de la red. • **Visualizar parches disponibles del equipo**: filtra el listado por el equipo elegido para mostrar todos los parches disponibles que aun no se han instalado. • **Visualizar equipos con el parche disponible**: muestra todos los equipos que tienen disponible el parche elegido para su aplicación.	

Tabla 15.13: campos del listado Parches disponibles

- **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres

Tabla 15.14: campos del fichero exportado Parches disponibles

Campo	Comentario	Valores
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y sus requisitos si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha
Es descargable	Indica si el parche está disponible para su descarga o requiere un contrato adicional con el proveedor del software para acceder a aquel.	Booleano
Tamaño de la descarga (KB)	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico
Estado	Indica el estado de la instalación del parche: • **Pendiente**: el parche está disponible para el equipo y no ha completado su instalación. • **Pendiente (descargado manualmente)**: el parche ya fue descargado de forma manual y forma parte del repositorio de parches. Consulta el apartado "**Descargar los parches de forma manual**".	Cadena de caracteres

Tabla 15.14: campos del fichero exportado Parches disponibles

Campo	Comentario	Valores
	• **Requiere descarga manual**: el parche requiere que el administrador descargue de forma manual el parche y lo copie en un equipo con el rol de cache asignado. Consulta el apartado "**Descargar los parches de forma manual**".	
Nombre del archivo	Nombre del archivo que contiene el parche.	Cadena de caracteres
URL de descarga	Recurso HTTP en la infraestructura del proveedor del software para descargar el parche.	Cadena de caracteres

Tabla 15.14: campos del fichero exportado Parches disponibles

- **Herramienta de filtrado**

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack

Tabla 15.15: campos de filtrado para el listado Parches disponibles

Campo	Comentario	Valores
Mostrar parches no descargables	Indica los parches que no son descargables directamente por Cytomic Patch debido a requisitos adicionales del proveedor (aceptación de EULA, introducción de credenciales, captchas etc.).	Booleano

Tabla 15.15: campos de filtrado para el listado Parches disponibles

- **Ventana Parche detectado**

Al hacer clic en una de las filas del listado se mostrará la ventana Parche detectado con información sobre el parche disponible y el botón Instalar parche, que creará una tarea de instalación del parche en el equipo seleccionado.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base, etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Equipo	Nombre del equipo con software desactualizado.	• Cadena de caracteres
Estado de instalación	Indica si el parche ya forma parte del respositorio de parches aplicables a los equipos o si requiere la descarga e integración manual por parte del administrador en el respositorio de parches.	• Pendiente • Requiere descarga manual • Pendiente (descargado manualmente)
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha

Tabla 15.16: campos de la ventana Parche detectado

Campo	Comentario	Valores
Tamaño de la descarga	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres
URL de la descarga	URL para descargar el parche de forma individual.	Cadena de caracteres
Nombre del archivo	Nombre del archivo que contiene el parche.	Cadena de caracteres

Tabla 15.16: campos de la ventana Parche detectado

Listado Programas End of Life

Muestra los programas que ya no tienen soporte por parte de sus proveedores y que por tanto son un objetivo especialmente vulnerable para el malware y las amenazas.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software en EoL.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL	Cadena de caracteres
EOL	Fecha en la que el programa entró en EoL.	Fecha (en rojo si el equipo entró en EOL)

Tabla 15.17: campos del listado Programas EoL

- **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres

Tabla 15.18: campos del fichero exportado Programas EoL

Campo	Comentario	Valores
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL.	Cadena de caracteres
EoL	Fecha en la que el programa entró en EoL.	Fecha
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha

Tabla 15.18: campos del fichero exportado Programas EoL

- **Herramienta de filtrado**

Campo	Comentario	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Fecha inventario	Fecha en la que el programa entrará en EOL.	• Todos • Actualmente en "End of life" • Actualmente o en "End of life" en 1 año

Tabla 15.19: campos de filtrado para el listado Programas EoL

- **Ventana Detalles del programa**

Al hacer clic en una de las filas del listado se mostrará la ventana Parche detectado con información sobre el parche disponible y el botón Instalar parche, que creará una tarea de instalación del parche en el equipo seleccionado.

Campo	Comentario	Valores
Programa	Nombre del programa o versión del sistema operativo Windows que recibió el parche.	Cadena de caracteres
Familia	Bundle, suit o grupo de programas al que pertenece el software.	Cadena de caracteres
Editor/Empresa	Empresa que diseñó o publicó el programa.	Cadena de caracteres
Versión	Versión del programa.	Cadena de caracteres
EOL	Fecha en la que el programa entró en EoL.	Fecha

Tabla 15.20: campos de la ventana Detalles del programa

Listado Historial de instalaciones

Muestra los parches que Cytomic EPDR intentó instalar y los equipos que los recibieron en un intervalo determinado.

Campo	Comentario	Valores
Fecha	Fecha en la que se instaló el parche o actualización.	Fecha
Equipo	Nombre del equipo que recibió el parche o actualización.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa o versión del sistema operativo Windows que recibió el parche.	Cadena de caracteres
Versión	Versión del programa o sistema operativo que recibió el parche.	Cadena de caracteres
Parche	Nombre del parche instalado.	Cadena de caracteres
Criticidad	Importancia del parche instalado.	• Otros parches • Crítica • Importante • Moderada • Baja • No clasificado • Service Pack
Instalación	Estado de la instalación del parche o actualización.	• Instalado • Requiere reinicio • Error • Desinstalado • El parche ya no es requerido
Menú de contexto ⋮	Muestra un desplegable con opciones.	• **Ver tarea**: muestra la configuración de la tarea asociada a la instalación o desinstalación del parche seleccionado.

Tabla 15.21: campos del listado Historial de instalaciones

- **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Fecha	Última fecha de intento de instalación.	Fecha
Programa	Nombre del programa o versión del sistema operativo Windows que recibió el parche.	Cadena de caracteres
Versión	Versión del programa o sistema operativo que recibió el parche.	Cadena de caracteres
Parche	Nombre del parche instalado.	Cadena de caracteres
Criticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador de KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y sus requisitos si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha

Tabla 15.22: campos del fichero exportado Historial de instalaciones

Campo	Comentario	Valores
Instalación	Estado de la instalación del parche o actualización.	• Instalado • Requiere reinicio • Error • El parche ya no es requerido • Desinstalado
Error de instalación	El módulo de Cytomic Patch no se instaló correctamente.	• **Imposible realizar la descarga**: instalador no disponible • **Imposible realizar la descarga**: fichero corrupto • **Espacio insuficiente en disco**
URL de descarga	URL para descargar el parche de forma individual.	Cadena de caracteres
Código de resultado	Código resultado de la instalación del parche. Puede indicar el éxito o el motivo del fracaso de la operación. Consulta la documentación del proveedor para interpretar el código de resultado.	Numérico

Tabla 15.22: campos del fichero exportado Historial de instalaciones

- **Herramienta de filtrado**

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Desde	Fecha de inicio para el intervalo de búsqueda.	Fecha
Hasta	Fecha de finalización para el intervalo de búsqueda.	Fecha
Criticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad)

Tabla 15.23: campos de filtrado para el listado Historial de instalaciones

Campo	Comentario	Valores
		• Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Instalación	Estado de la instalación del parche o actualización.	• Instalado • Requiere reinicio • Error • El parche ya no es requerido • Desinstalado
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres

Tabla 15.23: campos de filtrado para el listado Historial de instalaciones

- **Ventana Parche instalado**

Al hacer clic en una de las filas del listado se mostrará la ventana Parche instalado con información detallada del parche.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack

Tabla 15.24: campos de la ventana Parche instalado

Campo	Comentario	Valores
CVEs	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Fecha de instalación	Fecha en la que el parche se instaló con éxito en el equipo.	Fecha
Resultado	Estado de la instalación del parche o actualización.	• Instalado • Requiere reinicio • Error • El parche ya no es requerido • Desinstalado
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Tamaño de la descarga	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres
Descripción	Notas que incluye el fabricante sobre los efectos que produce aplicar el parche, condiciones especiales y problemas solucionados.	Cadena de caracteres

Tabla 15.24: campos de la ventana Parche instalado

Listado Parches excluidos

Este listado muestra los parches que el administrador ha marcado como excluidos para evitar su instalación en los equipos de la red. Se muestra una linea por cada par parche - equipo excluido,

excepto en el caso de exclusiones para todos los equipos de la red, que se mostrarán en una única linea.

Campo	Comentario	Valores
Equipo	Dependiendo del destino de la exclusión el contenido de este campo varía: • Si el parche se ha excluido para un único equipo se incluye el nombre del equipo. • Si el parche se ha excluido para todos los equipos de la cuenta se incluye el literal "(Todos)".	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa al que pertenece el parche excluido.	Cadena de caracteres
Versión	Versión del programa al que pertenece el parche excluido.	Cadena de caracteres
Parche	Nombre del parche excluido.	Cadena de caracteres
Criticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Excluido por	Cuenta de usuario de la consola de administración que excluyó el parche.	Cadena de caracteres
Excluido desde	Fecha en la que se excluyó el parche.	Cadena de caracteres

Tabla 15.25: campos del listado Parches excluidos

- **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres

Tabla 15.26: campos del fichero exportado Parches excluidos

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Dependiendo del destino de la exclusión el contenido de este campo varía: • Si el parche se ha excluido para un único equipo indica el nombre del equipo. • Si el parche se ha excluido para todos los equipos de la cuenta indica el literal "(Todos)".	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción del equipo asignada por el administrador de la red.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa al que pertenece el parche excluido.	Cadena de caracteres
Versión	Versión del programa al que pertenece el parche excluido.	Cadena de caracteres
Parche	Nombre del parche excluido.	Cadena de caracteres
Criticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres

Tabla 15.26: campos del fichero exportado Parches excluidos

Campo	Comentario	Valores
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Tamaño de la descarga (KB)	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico
Excluido por	Cuenta de usuario de la consola de administración que excluyó el parche.	Cadena de caracteres
Excluido desde	Fecha en la que se excluyó el parche.	Cadena de caracteres

Tabla 15.26: campos del fichero exportado Parches excluidos

- **Herramienta de filtrado**

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo con un parche excluido.	Cadena de caracteres
Programa	Nombre del programa al que pertenece el parche excluido.	Cadena de caracteres
Parche	Nombre del parche excluido.	Cadena de caracteres
Mostrar parches no descargables	Indica los parches que no son descargables directamente por Cytomic Patch debido a requisitos adicionales del proveedor (aceptación de EULA, introducción de credenciales, captchas etc.).	Booleano
CVEs	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Criticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad)

Tabla 15.27: campos de filtrado para el listado Parches excluidos

Campo	Comentario	Valores
		• Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack

Tabla 15.27: campos de filtrado para el listado Parches excluidos

- **Ventana Parche excluido**

Al hacer clic en una de las filas del listado se mostrará la ventana Parche excluido con información detallada del parche marcado para no instalarse en los equipos de la red.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Tamaño de la descarga	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico

Tabla 15.28: campos de la ventana Parche instalado

Campo	Comentario	Valores
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres
Descripción	Notas que incluye el fabricante sobre los efectos que produce aplicar el parche, condiciones especiales y problemas solucionados.	Cadena de caracteres

Tabla 15.28: campos de la ventana Parche instalado

Capítulo 16

Cytomic Encryption (Cifrado de dispositivos)

Cytomic Encryption es un módulo integrado en la plataforma Cytomic que cifra el contenido de los medios de almacenamiento conectados a los equipos administrados por Cytomic EPDR. Su objetivo es minimizar la exposición de la información de las empresas, tanto en casos de pérdida o robo de los equipos como al descartar sistemas de almacenamiento en uso sin borrar previamente su contenido.

Cytomic Encryption es compatible con ciertas versiones de sistemas operativos Windows 7 en adelante (consulta el apartado "**Versiones del sistema operativo compatibles**" en la página **354**) y permite controlar el estado del cifrado de los equipos de la red, gestionando de forma centralizada sus claves de recuperación. Además, aprovecha recursos hardware como los chips TPM, ofreciendo una gran flexibilidad a la hora de elegir el sistema de autenticación más adecuado en cada caso.

CONTENIDO DEL CAPÍTULO

Introducción a los conceptos de cifrado

Cytomic Encryption utiliza las herramientas integradas en los sistemas operativos Windows para gestionar el cifrado en los equipos de la red gestionados con Cytomic EPDR.

Para una correcta comprensión de los procesos involucrados en el cifrado y descifrado de la información, es necesario presentar algunos conceptos relativos a la tecnología de cifrado utilizada.

TPM

TPM (Trusted Platform Module, módulo de plataforma segura) es un chip que se incluye en algunas placas base de equipos de sobremesa, portátiles y servidores. Su principal objetivo es proteger la información sensible de los usuarios, almacenando claves y otra información utilizada en el proceso de autenticación.

Ademas, el TPM es el responsable de detectar los cambios en la cadena de inicio del equipo, impidiendo por ejemplo el acceso a un disco duro desde un equipo distinto al que se utilizó para su cifrado.

La versión mínima de TPM soportada por Cytomic Encryption es la 1.2. y Cytomic recomienda su uso en combinación con otros sistemas de autenticación soportados. En algunos escenarios es posible que el TPM esté deshabilitado en la BIOS del equipo y sea necesario su activación manual.

PIN y PIN extendido / mejorado

PIN (Personal Identification Number, número de identificación personal) es una secuencia de 4 a 20 números (6 a 20 en equipos Windows 10 versión 1709 y posteriores) que actúa como contraseña simple y es requerida en el inicio de un equipo que tenga un volumen cifrado. Sin el PIN la secuencia de arranque no se completa y el acceso al equipo no es posible.

Si el hardware es compatible, Cytomic EPDR utilizará un PIN extendido o PIN mejorado compuesto por letras y números para incrementar la complejidad de la contraseña.

Debido a que el PIN Extendido se pide en el proceso de inicio del equipo previo a la carga del sistema operativo, las limitaciones de la BIOS pueden restringir la entrada de teclado a la tabla ASCII de 7 bits. Adicionalmente, los teclados que utilizan una distribución distinta a la dispuesta en el mapa de caracteres EN-US, tales como teclados QWERTZ o AZERTY, pueden provocar el fallo en la introducción del PIN Extendido. Por esta razón Cytomic EPDR controla que los caracteres introducidos por el usuario pertenecen al mapa EN-US antes de establecer el PIN Extendido en el proceso de cifrado del equipo.

Passphrase

Es una contraseña de 8 a 255 caracteres alfanuméricos equivalente al PIN Extendido.

Llave USB

Permite almacenar la clave de acceso en un dispositivo USB formateado con NTFS, FAT o FAT32. De esta forma, no se requiere introducir ninguna contraseña en el proceso de inicio del equipo, aunque es necesario que el dispositivo USB que almacena la contraseña esté conectado en el equipo.

Algunos PCs antiguos no son capaces de acceder a las unidades USB en el proceso de arranque, comprueba que los equipos de tu organización tienen acceso a las unidades USB desde la BIOS.

Clave de recuperación

Cuando se detecta una situación anómala en un equipo protegido con Cytomic Encryption o en el caso de que hayamos olvidado la contraseña de desbloqueo, el sistema pedirá una clave de recuperación de 48 dígitos. Esta clave se gestiona desde la consola de administración y debe ser introducida para completar el inicio del equipo. Cada volumen cifrado tendrá su propia clave de recuperación independiente.

Cytomic Encryption únicamente almacena las claves de recuperación de los equipos que gestiona. La consola de administración no mostrará las claves de recuperación de los equipos cifrados por el usuario y no gestionados por Cytomic.

La clave de recuperación se solicita en los escenarios mostrados a continuación:

- Cuando se introduce errónea y repetidamente el PIN o la passphrase en el proceso de inicio del equipo.
- Cuando un equipo protegido con TPM detecta un cambio en la secuencia de arranque (disco duro protegido por TPM y conectado en otro equipo).
- Cuando se ha cambiado la placa base del equipo y por lo tanto el TPM.
- Al desactivar, deshabilitar o borrar el contenido del TPM.

- Al cambiar los valores de configuración de arranque del equipo.
- Al cambiar el proceso de arranque del equipo:
  - Actualización de la BIOS.
  - Actualización del firmware.
  - Actualización de la UEFI.
  - Modificación del sector de arranque.
  - Modificación del registro maestro de arranque (master boot record).
  - Modificación del gestor de arranque (boot manager).
  - Cambio del firmware implementado en ciertos componentes que forman parte del proceso de arranque del equipo (tarjetas de vídeo, controladores de discos etc.) conocido como Option ROM.
  - Cambio de otros componentes que intervienen en las fases iniciales del arranque del sistema.

BitLocker

Es el software instalado en algunas versiones de los equipos Windows 7 y superiores encargado de gestionar el cifrado y descifrado de los datos almacenados en los volúmenes del equipo. Cytomic Encryption instala BitLocker automáticamente en aquellas versiones de servidor que no lo incluyan pero sean compatibles.

Partición de sistema

Es una zona pequeña del disco duro de 1.5 gigabytes aproximadamente que permanece sin cifrar y que es necesaria para que el equipo complete correctamente el proceso de inicio. Cytomic Encryption crea automáticamente esta partición de sistema si no existiera previamente.

Algoritmo de cifrado

El algoritmo de cifrado elegido en Cytomic Encryption es el AES-256 aunque los equipos con volúmenes cifrados por el usuario que utilicen otro algoritmo de cifrado también son compatibles.

Visión general del servicio de cifrado

El proceso general de cifrado abarca varios apartados que el administrador deberá conocer para gestionar correctamente los recursos de la red susceptibles de contener información delicada o comprometedora en caso de robo, pérdida o descarte del volumen sin borrar:

- **Cumplimiento de los requisitos mínimos de hardware y software:** consulta el apartado "**Requisitos mínimos de Cytomic Encryption**" para ver las limitaciones y particularidades del cifrado en cada plataforma compatible.
- **Estado previo del cifrado en el equipo del usuario**: dependiendo de si BitLocker estaba siendo usado previamente en el equipo del usuario, el proceso de integración en Cytomic EPDR puede

variar ligeramente.

- **Asignación de configuraciones de cifrado**: establece el estado (cifrado o no cifrado) de los equipos de la red y el o los métodos de autenticación.
- **Interacción del proceso de cifrado con el usuario del equipo:** el proceso de cifrado inicial requiere de la colaboración del usuario para completarse de forma correcta. Consulta el apartado "**Cifrado de volúmenes sin cifrado previo**".
- **Visualización del estado de cifrado del parque informático**: mediante los widgets / paneles incluidos en el menú superior **Estado**, panel lateral **Cifrado**. Consulta el apartado "**Paneles / widgets en Cytomic Encryption**" para una descripción completa de los widgets incluidos en Cytomic Encryption. También se soportan filtros para localizar equipos en los listados según su estado. Consulta el apartado "**Filtros disponibles**".
- **Restricción de los permisos de cifrado a los administradores de la seguridad**: el sistema de roles mostrado en el apartado "**Descripción de los permisos implementados**" en la página **75** abarca la funcionalidad de cifrado y visualización del estado de los equipos de la red.
- **Obtención de la clave de recuperación**: en los casos en que el usuario haya olvidado el PIN / passpharse o el TPM haya detectado una situación anómala el administrador de la red podrá obtener de forma centralizada la clave de recuperación y enviársela al usuario. Consulta el apartado "**Obtención de la clave de recuperación**".

Características generales de Cytomic Encryption

Tipos de autenticación soportados

Dependiendo de la existencia o no de TPM y de la versión del sistema operativo, PCytomic Encryption admite distintas combinaciones de métodos de autenticación, mostrados a continuación de forma ordenada según la recomendación de Cytomic:

- **TPM + PIN**: compatible con todas las versiones de Windows soportadas, requiere el chip TPM habilitado en la BIOS y el establecimiento de un PIN.
- **Solo TPM**: compatible con todas las versiones de Windows soportadas, requiere el chip TPM habilitado en la BIOS excepto en Windows 10, donde se habilita de forma automática.
- **Dispositivo USB**: requiere una llave USB y un equipo que pueda acceder a dispositivos USBs en el arranque. Necesario en equipos Windows 7 sin TPM.
- **Passprhase**: solo disponible en equipos Windows 8 y posteriores sin TPM.

Cytomic Encryption utiliza por defecto un método de autenticación que incluya el uso de TPM si se encuentra disponible. Si se elige una combinación de autenticación no incluida en el listado anterior, la consola de administración mostrará una ventana de advertencia indicando que el equipo permanecerá sin cifrar.

Tipo de dispositivos de almacenamiento compatibles

Cytomic Encryption cifra todos los dispositivos internos de almacenamiento masivo:

- Unidades de almacenamiento fijas del equipo (sistema y datos).
- Discos duros virtuales (VHD) pero unicamente el espacio utilizado independientemente de lo indicado en la consola de administración.

No se cifrarán:

- Discos duros internos dinámicos.
- Discos duros extraibles.
- Llaves USB.
- Particiones de tamaño muy reducido.
- Otros dispositivos de almacenamiento externo.

Requisitos mínimos de Cytomic Encryption

Los requisitos mínimos se dividen en:

- Versiones del sistema operativo Windows y familias compatibles.
- Requisitos de hardware.

Versiones del sistema operativo compatibles

- Windows 7 (Ultimate, Enterprise)
- Windows 8/8.1 (Pro, Enterprise)
- Windows 10 (Pro, Enterprise, Education)
- Windows Server 2008 R2 y superiores (incluyendo a las ediciones Server Core)

Requisitos hardware

- TPM 1.2 y superiores si se utiliza este método de autenticación.
- Llave USB y equipo compatible con la lectura de dispositivos USB desde la BIOS en sistemas Windows 7 sin TPM.

Gestión de equipos según su estado de cifrado previo

Administración de equipos por Cytomic Encryption

Para que un equipo de la red se considere gestionado por Cytomic Encryption es necesario que se cumplan las condiciones siguientes:

- El equipo cumple con los requisitos mínimos descritos en el apartado "**Requisitos mínimos de Cytomic Encryption**".
- El equipo ha recibido al menos una vez una configuración desde la consola de administración que

establezca el cifrado de los volúmenes y éste se ha completado con éxito.

Los equipos que previamente tenían cifrado alguno de sus volúmenes y no han recibido una configuración que cifre sus unidades no serán gestionados por Cytomic Encryption y por lo tanto el administrador no tendrá acceso a la clave de recuperación ni al estado del equipo.

Por el contrario, los equipos que han recibido una configuración que cifre sus unidades, independientemente de su estado anterior (cifrado o no) serán administrados por Cytomic Encryption.

Desinstalación del agente Cytomic EPDR

Independientemente de si el equipo estaba siendo administrado por Cytomic Encryption o no, si los dispositivos de almacenamiento estaban cifrados, al desinstalar Cytomic EPDR se dejaran tal y como están. No obstante, se perderá el acceso centralizado a la clave de recuperación.

Si posteriormente el equipo se reintegra en Cytomic EPDR se mostrará la última clave de recuperación almacenada.

Proceso de cifrado y descifrado

Cifrado de volúmenes sin cifrado previo

El proceso de cifrado se inicia cuando el agente Cytomic EPDR instalado en el equipo de usuario se descarga una configuración de tipo Cifrado. En ese momento se le mostrará al usuario una ventana informativa que le guiará en todo el proceso.

El número de pasos total varía dependiendo del tipo de autenticación elegida por el administrador y del estado previo del equipo. Si cualquiera de los pasos termina en un error, el agente lo reportará a la consola de administración y el proceso se detendrá.

No se permitirá el cifrado de equipos desde una sesión de escritorio remoto ya que es necesario el reinicio del equipo y la introducción de una clave antes de la carga del sistema operativo, operaciones que no son posibles con un sistema de escritorio remoto estándar.

El proceso de cifrado se iniciará cuando la instalación o desinstalación en curso de parches gestionados por el módulo Cytomic Encryption haya finalizado.

A continuación se muestra el proceso completo de cifrado y se indica si se muestra feedback al usuario del equipo y si es necesario el reinicio de la máquina:

Paso	Proceso en el equipo	Interacción con el usuario
1	El agente recibe una configuración del módulo de cifrado que pide cifrar el contenido de los dispositivos de almacenamiento instalados.	Ninguno
2	Si el equipo es de tipo servidor y no tiene las herramientas de BitLocker instaladas éstas se descargan y se instalan.	Se muestra una ventana pidiendo permiso para reiniciar el equipo y completar la instalación de BitLocker o posponer. Si se elige posponer el proceso se detiene y se volverá a preguntar en el siguiente inicio de sesión. **Requiere reinicio.**
3	Si el equipo no estaba cifrado previamente se crea la partición de sistema.	Se muestra una ventana pidiendo permiso para reiniciar el equipo y completar la creación de la partición de sistema o posponer. Si se elige posponer el proceso se detiene y se volverá a preguntar en el siguiente inicio de sesión. **Requiere reinicio.**
4	Si existe una directiva de grupo definida previamente por el administrador de la red que colisione con las establecidas por Cytomic Encryption se mostrará un error y el proceso terminará. Las directivas de grupo configuradas por Cytomic Encryption son: En el Editor de Directivas de grupo local, navega la ruta siguiente: Directiva equipo local > Configuración del equipo > Plantillas administrativas > Componentes de Windows > Cifrado de unidad BitLocker > Unidades del sistema operativo. Marca a Sin definir las políticas de grupo indicadas para evitar este error.	Si el administrador no ha definido directivas de grupo globales que entren en colisión con las directivas locales definidas por Cytomic Encryption no se mostrará ningún mensaje.

Tabla 16.1: pasos para el cifrado de volúmenes sin cifrar previamente

Paso	Proceso en el equipo	Interacción con el usuario
5	Preparación del TPM si existe y si el método de autenticación elegido involucra a éste componente y no estaba habilitado previamente desde la BIOS.	Requiere confirmar un reinicio para que el usuario pueda entrar en la BIOS del equipo y habilitar el TPM. En sistemas operativos Windows 10 no es necesario modificar la BIOS pero se requiere el reinicio igualmente. El reinicio del paso 3, en caso de haberlo, se juntará con el actual.
6	Preparación del dispositivo USB si el método de autenticación elegido involucra a este componente.	Se requiere al usuario introducir un dispositivo USB para almacenar la contraseña de inicio de equipo.
7	Almacenamiento del PIN si el método de autenticación elegido involucra a este componente.	Se requiere al usuario introducir el PIN. Si se utilizan caracteres alfanuméricos y el hardware no es compatible se mostrará el error "-2144272180". En este caso introduce un PIN numérico.
8	Almacenamiento de la passphrase si el método de autenticación elegido involucra a este componente.	Se requiere al usuario introducir la passphrase.
9	Se genera la clave de recuperación y se envía a la nube de Cytomic. Una vez que la clave se ha recibido, el proceso continúa en el equipo del usuario.	Ninguno.
10	Comprobación de que el hardware del equipo es compatible con la tecnología de cifrado, e inicio del cifrado.	Se requiere confirmar un reinicio para hacer el chequeo del hardware utilizado en los distintos métodos de autenticación elegidos. **Requiere reinicio.**
11	Cifrado de volúmenes.	Comienza el proceso de cifrado en segundo plano sin ocasionar molestias al usuario del equipo. La duración depende del volumen de datos a cifrar. Una duración media del tiempo de cifrado se sitúa en torno a las 2-3 horas. El usuario puede utilizar y apagar el equipo normalmente. El proceso de cifrado se reanudará en el siguiente encendido del equipo.
12	El proceso de cifrado se completa de forma silenciosa y a partir de ese momento el proceso de cifrado y descifrado es transparente para el usuario.	Dependiendo del método de autenticación elegido el usuario puede necesitar introducir una llave USB, un PIN, una passphrase o nada en el inicio del equipo.

Tabla 16.1: pasos para el cifrado de volúmenes sin cifrar previamente

Cifrado de volúmenes ya cifrados previamente

En el caso de que algún volumen del equipo ya estuviera cifrado, Cytomic Encryption modifica algunos parámetros para habilitar su gestión centralizada. A continuación se indican las acciones realizadas:

- Si el método de autenticación elegido por el usuario no coincide con el especificado en la configuración, éste se cambiará, solicitándole al usuario las claves o recursos hardware necesarios. Si no es posible asignar un método de autenticación compatible con la plataforma y con la configuración especificada por el administrador, el equipo quedará cifrado por el usuario y no será gestionado por Cytomic Encryption.
- Si el algoritmo de cifrado utilizado no está soportado (distinto de AES-256) se dejará sin cambios para evitar el descifrado y cifrado completo el volumen pero el equipo será administrador por Cytomic Encryption.
- Si existen tanto volúmenes cifrados como sin cifrar, se cifrarán todos los volúmenes aplicando el mismo método de autenticación.
  - Si el método de autenticación elegido previamente involucra la introducción de una contraseña y es compatible con los métodos soportados por Cytomic Encryption, se volverá a pedir la contraseña al usuario para unificar el método de autenticación en todos los volúmenes.
- Si el usuario eligió una configuración de cifrado distinta a la establecida por el administrador (cifrado unicamente de los sectores ocupados frente al cifrado completo del volumen) el volumen se dejará sin cambios para minimizar el proceso de cifrado.

Cifrado de nuevos volúmenes

Si una vez completado el proceso de cifrado el usuario del equipo crea un nuevo volumen, Cytomic Encryption lo cifrará inmediatamente respetando la configuración asignada por el administrador de la red.

Descifrado de volúmenes

Se distinguen tres casos:

- Si Cytomic Encryption cifra un equipo, a partir de ese momento el administrador podrá asignar una configuración para descifrarlo.
- Si un equipo ya estaba cifrado por el usuario antes de la instalación de Cytomic Encryption y se le asigna una configuración de cifrado se considerará cifrado por Cytomic EPDR y se podrá descifrar asignando una configuración desde la consola de administración.
- Si un equipo ya estaba cifrado por el usuario antes de la instalación de Cytomic Encryption y nunca se le ha asignado una configuración de cifrado no se considerará cifrado por Cytomic EPDR y no se podrá descifrar asignando una configuración desde la consola de administración.

Modificación local de la configuración de BitLocker

El usuario del equipo tiene acceso a la configuración local de BitLocker desde las herramientas de Windows pero los cambios que efectúe serán revertidos de forma inmediata a la configuración

establecida por el administrador de la red a través de la consola de administración. El comportamiento de Cytomic Encryption ante un cambio de esta naturaleza se muestra a continuación:

- **Desactivar el desbloqueo automático de una unidad**: se revierte a la configuración de bloqueo automático.
- **Quitar la contraseña de un volumen**: se pedirá la nueva contraseña.
- **Descifrar un volumen previamente cifrado por Cytomic Encryption**: se cifrará automáticamente el volumen.
- **Cifrar una unidad descifrada**: si la configuración de Cytomic Encryptionimplica descifrar las unidades la acción del usuario prevalece y no se descifrará la unidad.

Comportamiento de Cytomic Encryption ante errores

- **Errores en el test de hardware**: el test de hardware se ejecuta cada vez que se inicia el equipo hasta que sea superado, momento en el que el equipo comenzará el cifrado automáticamente.
- **Error al crear la partición de sistema**: muchos errores al crear la partición de sistema son subsanables por el propio usuario del equipo (por ejemplo la falta de espacio). Periódicamente Cytomic Encryption intentará crear la partición de forma automática.
- **Negativa a activar el chip TPM por parte del usuario**: el equipo mostrará un mensaje en cada proceso de inicio pidiéndole al usuario la activación del chip TPM. Hasta que esta condición no sea resuelta el proceso de cifrado no comenzará.

Obtención de la clave de recuperación

En los casos en que el usuario haya perdido el PIN / passphrase / dispositivo USB o el chip TPM haya detectado un cambio en la cadena de inicio del equipo, será necesaria la introducción de la clave de recuperación. Cytomic Encryption mantiene todas las claves de recuperación de los equipos de la red cuyo cifrado gestiona.

Para obtener la clave de recuperación de un equipo sigue los pasos mostrados a continuación:

- En el menú superior **Equipos** haz clic en el equipo cuyas claves quieres recuperar.
- En la pestaña **Detalles**, sección **Protección de datos**, haz clic en el link **Obtener la clave de recuperación**. Se mostrará una ventana con los identificadores de volumen cifrados.
- Haz clic en un identificador de volumen para mostrar su contraseña de recuperación.

Paneles / widgets en Cytomic Encryption

A continuación, se detallan los distintos widgets implementados en el dashboard de **Cifrado,** las distintas áreas y zonas activas incorporadas y los tooltips y su significado. Para acceder haz clic en el menú superior **Estado**, panel lateral **Cifrado.**

Estado del cifrado

Muestra el total de equipos compatibles con Cytomic Encryption así como su estado con respecto a la tecnología de cifrado.

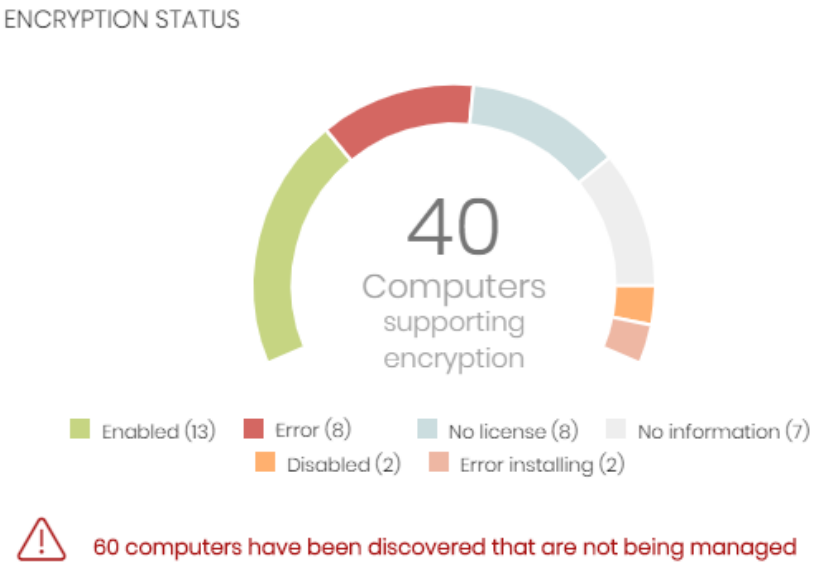


Figura 16.1: panel de Estado del cifrado

- **Significado de las series**

Serie	Descripción
Activado	Equipos con Cytomic Encryption instalado, con una configuración que indica cifrar el equipo y sin reporte de errores de cifrado ni de instalación.
Desactivado	Equipos con Cytomic Encryption instalado, con una configuración que indica no cifrar el equipo y sin reporte de errores de cifrado ni de instalación.
Error	No se ha podido realizar la acción que el administrador ha indicado en la configuración de cifrado o descifrado.
Error instalando	No se ha podido descargar e instalar BitLocker si fue necesario.
Sin licencia	Equipo compatible con Cytomic Encryption pero sin licencia asignada.
Sin información	Equipos con licencia recientemente asignada y que todavía no han reportado su estado al servidor, o equipo con un agente sin actualizar.

Tabla 16.2: descripción de la serie Estado del cifrado

- **Filtros preestablecidos desde el panel**

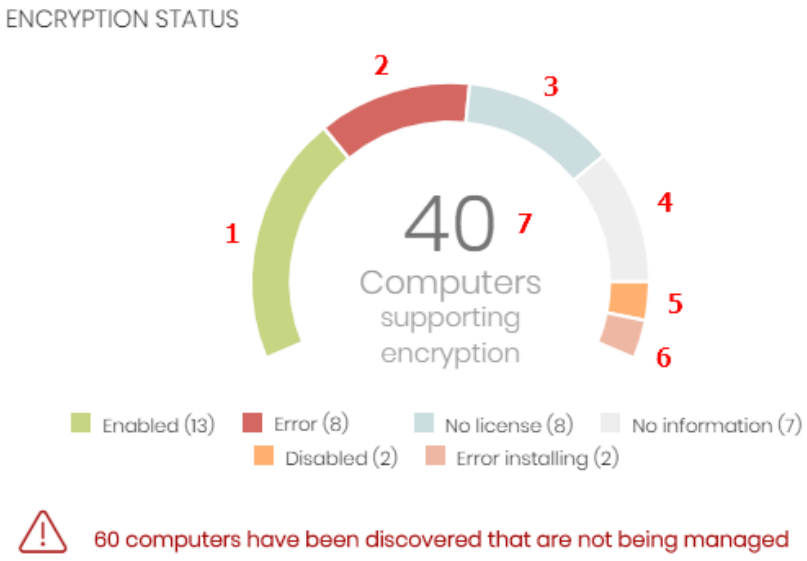


Figura 16.2: zonas activas del panel Estado del cifrado

Al hacer clic en las zonas indicadas en la figura 16.2 se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado del cifrado = Activado.
(2)	Estado del cifrado = Error.
(3)	Estado del cifrado = Sin licencia.
(4)	Estado del cifrado = Sin información.
(5)	Estado del cifrado = Desactivado.
(6)	Estado del cifrado = Error instalando.
(7)	Sin filtros.

Tabla 16.3: definición de filtros del listado Estado del cifrado

Equipos compatibles con cifrado

Muestra los equipos compatibles y no compatibles con la tecnología de filtrado agrupados en series según su tipo.

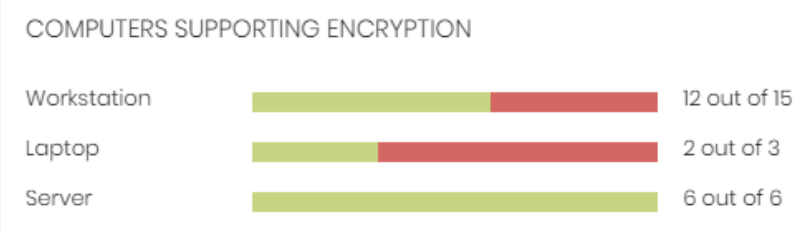


Figura 16.3: panel de Equipos compatibles con cifrado

- **Significado de las series**

Serie	Descripción
Estación - verde	Dispositivos de tipo estación compatibles con cifrado.
Estación - rojo	Dispositivos de tipo estación no compatibles con cifrado.
Portátil - verde	Dispositivos de tipo portátil compatibles con cifrado.
Portátil - rojo	Dispositivos de tipo portátil no compatibles con cifrado.
Servidor - verde	Dispositivos de tipo servidor compatibles con cifrado.
Servidor - rojo	Dispositivos de tipo servidor no compatibles con cifrado.

Tabla 16.4: descripción de la serie Equipos compatibles con cifrado

- **Filtros preestablecidos desde el panel**

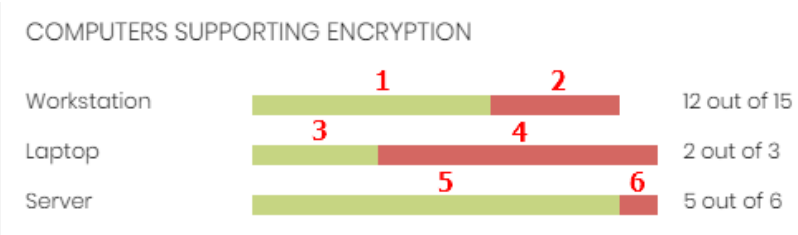


Figura 16.4: zonas activas del panel Estado del cifrado

Al hacer clic en las zonas indicadas en la figura 16.4 se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Tipo de equipo = Estación.
(2)	Listado de equipos con filtro **No compatibles con cifrado.**
(3)	Tipo de equipo = Portátil.

Tabla 16.5: definición de filtros del listado Estado del cifrado

Zona activa	Filtro
(4)	Listado de equipos con filtro **No compatibles con cifrado.**
(5)	Tipo de equipo = Servidor.
(6)	Listado de equipos con filtro **No compatibles con cifrado.**

Tabla 16.5: definición de filtros del listado Estado del cifrado

Equipos cifrados

Muestra el estado del proceso de cifrado en los equipos de la red compatibles con Cytomic Encryption.

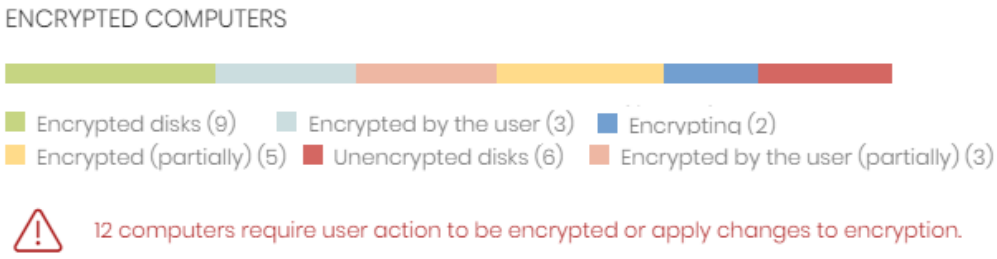


Figura 16.5: panel Equipos cifrados

- **Significado de las series**

Serie	Descripción
Desconocido	Medios de almacenamiento cifrados con un método de autenticación no soportado por Cytomic Encryption.
Discos no cifrados	Ninguno de los medios de almacenamiento del equipo están cifrados ni por el usuario ni por Cytomic Encryption.
Discos cifrados	Todos los medios de almacenamiento del equipo están cifrados por Cytomic Encryption.
Cifrando	Al menos un medio de almacenamiento del equipo está en proceso de cifrado.
Descifrando	Al menos un medio de almacenamiento del equipo está en proceso de descifrado.
Cifrado por el usuario	Todos los medios de almacenamiento se encuentran cifrados pero alguno de ellos o todos fueron cifrados por el usuario.
Cifrado por el usuario (parcialmente)	Alguno de los medios de almacenamiento se encuentran cifrados por el usuario y el resto permanece sin cifrar o está cifrado por Cytomic Encryption.
Cifrado (parcialmente)	Al menos uno de los medios de almacenamiento del equipo está cifrado por Cytomic Encryption pero el resto permanece sin cifrar.

Tabla 16.6: descripción de la serie Equipos cifrados

- **Filtros preestablecidos desde el panel**

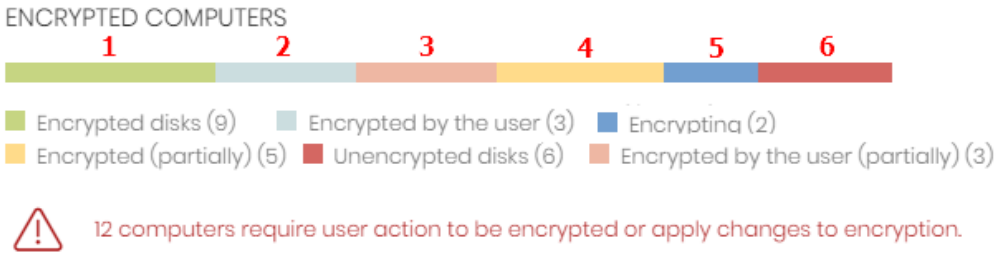


Figura 16.6: zonas activas del panel Equipos Cifrados

Al hacer clic en las zonas indicadas en la figura 16.6 se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Cifrado de discos = Discos cifrados.
(2)	Cifrado de discos = Cifrado por el usuario.
(3)	Cifrado de discos = Cifrado por el usuario (parcialmente).
(4)	Cifrado de discos = Cifrado (parcialmente).
(5)	Cifrado de discos = Cifrando.
(6)	Cifrado de discos = Discos no cifrados.
(7)	Cifrado de discos = Descifrando.
(8)	Cifrado de discos = Desconocido.

Tabla 16.7: definición de filtros del listado Estado del cifrado

Métodos de autenticación aplicados

Muestra los equipos con el cifrado configurado en la red agrupados por el tipo de autenticación elegido.

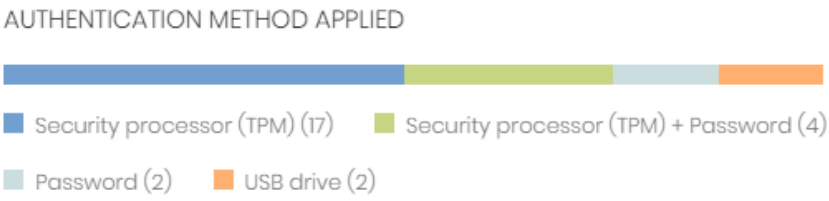


Figura 16.7: panel Métodos de autenticación

- **Significado de las series**

Serie	Descripción
Desconocido	El método de autenticación elegido por el usuario del equipo no está soportado por Cytomic Encryption.
Procesador de seguridad (TPM)	El método de autenticación utilizado es TPM.
Procesador de seguridad (TPM) + Contraseña	El método de autenticación utilizado es TPM y PIN o passphrase solicitado en el inicio del equipo.
Contraseña	El método de autenticación elegido es PIN o passphrase solicitado en el inicio del equipo.
USB	El método de autenticación elegido es dispositivo USB conectado en el arranque del equipo.
Sin cifrar	Ninguno de los dispositivos de almacenamiento del equipo está cifrado.

Tabla 16.8: descripción de la serie Métodos de autenticación aplicado

- **Filtros preestablecidos desde el panel**

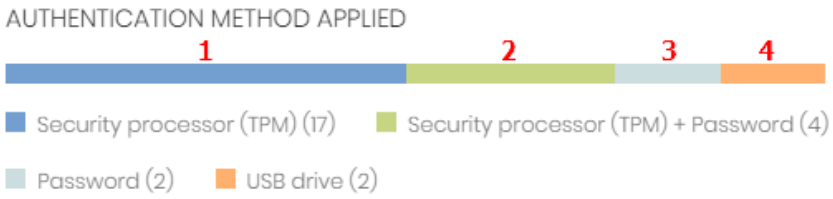


Figura 16.8: zonas activas del panel Métodos de autenticación aplicado

Al hacer clic en las zonas indicadas en la figura 16.8 se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Método de autenticación = Procesador de seguridad (TPM)
(2)	Método de autenticación= Procesador de seguridad (TPM) + Contraseña
(3)	Método de autenticación = Contraseña
(4)	Método de autenticación = USB
(5)	Método de autenticación = Desconocido
(6)	Método de autenticación = Sin cifrar

Tabla 16.9: definición de filtros del listado

Listados en Cytomic Encryption

Para acceder a los listados de Cytomic Encryption sigue los pasos mostrados a continuación:

- **Para mostrar listados con filtros preestablecidos**: en el menú superior **Estado**, panel lateral **Cifrado**, haz clic en una serie de los widgets mostrados. Se abrirá el listado asociado al widget con la herramienta de filtrado configurada par mostrar la serie seleccionada.
- **Para mostrar listados sin filtros preestablecidos**: en el menú superior **Estado**, panel **Mis listados** haz clic en el enlace **Añadir** y selecciona un listado.

*Consulta el apartado "**Gestión de listados**" en la página **57** para obtener más información sobre la gestión de listados en Cytomic EPDR.*

Listado Estado del cifrado

Este listado muestra todos los equipos de la red gestionados por Cytomic EPDR y compatibles con Cytomic Encryption. Incorpora filtros relativos al módulo para controlar el estado del cifrado en el parque informático.

Campo	Comentario	Valores
Equipo	Nombre del equipo compatible con la tecnología de cifrado.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo y versión instalada en el equipo de usuario o servidor.	Cadena de caracteres
Estado del cifrado	Estado del módulo Cytomic Encryption.	• Sin información • Activado • Desactivado • Error • Error instalando • Sin licencia
Cifrado de discos	Estado de los medios de almacenamiento del equipo con respecto al cifrado.	• Desconocido • Discos no cifrados • Discos cifrados • Cifrando • Descifrando • Cifrado por el usuario

Tabla 16.10: campos del listado Estado de cifrado

Campo	Comentario	Valores
		• Cifrado por el usuario (parcialmente) • Cifrado (parcialmente)
Método de autenticación	Método de autenticación seleccionado para cifrar los discos.	• Todos • Desconocido • Procesador de seguridad (TPM) • Procesador de seguridad (TPM) + Contraseña • Contraseña • USB • Sin cifrar
Última conexión	Fecha de la última vez que el agente se conectó con la nube de Cytomic.	Fecha

Tabla 16.10: campos del listado Estado de cifrado

- **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo compatible con la tecnología de cifrado.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres¡
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del módulo agente Cytomic.	Cadena de caracteres
Fecha de instalación	Fecha en la que el software Cytomic EPDR se instaló con éxito en el equipo.	Fecha

Tabla 16.11: campos del fichero exportado

Campo	Comentario	Valores
Fecha de la última conexión		Fecha
Plataforma	Sistema operativo instalado en el equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección actualizada	El módulo de la protección instalado en el equipo es la última versión publicada.	Booleano
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Conocimiento actualizado	El fichero de firmas descargado en el equipo es la última versión publicada.	Booleano
Fecha de la ultima actualización	Fecha de la descarga del fichero de firmas.	Fecha
Estado del cifrado	Estado del módulo Cytomic Encryption.	• Sin información • Activado • Desactivado • Error • Error instalando • Sin licencia
Cifrado de discos	Estado de los medios de almacenamiento del equipo con respecto al cifrado.	• Desconocido • Discos no cifrados • Discos cifrados
		• Cifrando • Descifrando • Cifrado por el usuario • Cifrado (parcialmente) • Cifrado por el usuario (parcialmente)
Acciones de cifrado pendientes del usuario	El usuario tiene pendiente introducir información o reiniciar el equipo para completar el proceso de cifrado de los volúmenes.	Booleano
Métodos de autenticación	Método de autenticación seleccionado para cifrar los discos.	• Todos • Desconocido • Procesador de seguridad (TPM)

Tabla 16.11: campos del fichero exportado

Campo	Comentario	Valores
		• Procesador de seguridad (TPM) + Contraseña • Contraseña • USB • Sin cifrar
Fecha de cifrado	Fecha del volumen más antiguo cifrado dentro de la primera que vez se consideró al equipo como completamente cifrado (se cifraron todos sus volúmenes compatibles).	Fecha
Versión de especificación del TPM	Versión de las especificaciones TPM soportadas por el chip incluido en el equipo.	Cadena de caracteres
Fecha error instalación cifrado	Fecha del último error de instalación reportado.	Fecha
Error instalación cifrado	Se ha producido un error al instalar el módulo Cytomic Encryption en el equipo.	Cadena de caracteres
Fecha error cifrado	Última fecha en la que se reportó un error de cifrado en el equipo.	
Error cifrado	El proceso de cifrado devolvió un error.	Cadena de caracteres

Tabla 16.11: campos del fichero exportado

- **Herramienta de filtrado**

Campo	Comentario	Valores
Fecha de cifrado desde	Limite inferior del rango de fechas en la que se consideró al equipo como completamente cifrado.	Fecha
Fecha de cifrado hasta	Limite superior del rango de fechas en la que se consideró al equipo como completamente cifrado.	Fecha
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Cifrado de discos	Estado de los medios de almacenamiento del equipo con respecto al cifrado.	• Desconocido • Discos no cifrados • Discos cifrados

Tabla 16.12: campos de filtrado para el listado

Campo	Comentario	Valores
		• Cifrando • Descifrando • Cifrado por el usuario • Cifrado (parcialmente) • Cifrado por el usuario (parcialmente)
Estado del cifrado	Estado del módulo Cytomic Encryption.	• Sin información • Activado • Desactivado • Error • Error Instalando • Sin licencia
Método de autenticación	Método de autenticación seleccionado para cifrar los discos.	• Todos • Desconocido • Procesador de seguridad (TPM) • Procesador de seguridad (TPM) + Contraseña • Contraseña • USB • Sin cifrar
Última conexión	Fecha del último envío del estado de Cytomic EPDR a la nube de Cytomic.	Fecha

Tabla 16.12: campos de filtrado para el listado

- **Ventana detalle del equipo**

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta el apartado "**Información de equipo** en la página **177** para obtener más información.

Configuración del cifrado

Cytomic Encryption permite establecer de forma centralizada la configuración del cifrado de los equipos de la red.

Para configurar el cifrado de los equipos:

- Haz clic en el menú superior **Configuración**, panel lateral **Cifrado.**
- Haz clic en el botón **Añadir** y completa la configuración con la información mostrada en el apartado "**Opciones de configuración de Cytomic Encryption**".

Opciones de configuración de Cytomic Encryption

Cifrar todos los discos duros de los equipos

Indica si los dispositivos de almacenamiento interno del equipo serán cifrados o no. Dependiendo del estado anterior del equipo, el comportamiento de Cytomic Encryptionserá diferente:

- Si el equipo está cifrado por Cytomic Encryption y se deshabilita **Cifrar todos los discos duros de los equipos**, se descifrarán todos los volúmenes cifrados.
- Si el equipo está cifrado pero no por Cytomic Encryption y se deshabilita **Cifrar todos los discos duros de los equipos** los volúmenes no sufren ningún cambio.
- Si el equipo está cifrado pero no por Cytomic Encryption y se habilita **Cifrar todos los discos duros de los equipos** se adecuará la configuración interna de cifrado para que coincida con los métodos soportados en Cytomic EPDR evitando volver a cifrar el volumen. Consulta el apartado "**Cifrado de volúmenes ya cifrados previamente**".
- Si el equipo no está cifrado y se habilita **Cifrar todos los discos duros de los equipos** se cifrarán todos los volúmenes según el proceso mostrado en el apartado "**Cifrado de volúmenes sin cifrado previo**".

Solicitar una contraseña para acceder al equipo

Habilita la autenticación por contraseña en el arranque del equipo. Dependiendo de la plataforma y de la existencia de hardware TPM se permitirá el uso de dos tipos de contraseña:

- **Equipos con TPM**: se pedirá una contraseña de tipo PIN.
- **Equipos sin TPM**: se pedirá una contraseña de tipo passhrase.

> ⚠ *Si estableces esta configuración a No y el equipo no tiene acceso a un procesador de seguridad TPM compatible, sus medios de almacenamiento no se cifrarán.*

No cifrar los equipos que requieren un USB para autenticarse

Para evitar la utilización de dispositivos USB soportados por Cytomic Encryption en la autenticación, el administrador puede deshabilitar su uso.

> ⚠ *Solo los equipos Windows 7 sin TPM están en posición de utilizar el método de autenticación por USB. Si el administrador deshabilita el uso de USBs, estos equipos no serán cifrados.*

Cifrar sólo el espacio utilizado

El administrador puede minimizar el tiempo de cifrado empleado restringiendo la protección a los sectores del disco duro que están siendo utilizados. Los sectores liberados tras borrar un fichero continuarán cifrados pero el espacio libre previo al cifrado del disco duro permanecerá sin cifrar, siendo accesible por terceros mediante herramientas de recuperación de ficheros borrados.

Filtros disponibles

Para localizar los equipos de la red que coincidan con alguno de los estados de cifrado definidos en Cytomic EPDR utiliza los recursos del árbol de filtros mostrados en el apartado "**Árbol de filtros**" en la página **152** con los campos mostrados a continuación:

- Cifrado:
  - Acciones de cifrado pendientes del usuario.
  - Cifrado de discos.
  - Fecha de cifrado.
  - Método de autenticación.
  - Tiene acciones pendientes de cifrado del usuario.
- Configuración:
  - Cifrado.
- Equipo:
  - Tiene TPM.
- Hardware:
  - TPM - Activado.
  - TPM - Fabricante.
  - TPM - Propietario.
  - TPM - Versión.
  - TPM - Versión de especificación.
- Módulos:
  - Cifrado.

Capítulo 17

Configuración del bloqueo de programas

Para incrementar la seguridad de base en los equipos Windows de la red, el administrador puede bloquear la ejecución de los programas que considere peligrosos o no compatibles con la actividad desarrollada en la empresa. Las causas que pueden llevar a un administrador a prohibir la ejecución de un determinado programa pueden ser:

- Programas que por sus altos requisitos consumen mucho ancho de banda o establecen un número de conexiones desproporcionadamente grande, poniendo en peligro el rendimiento de la conectividad de la empresa si son ejecutados por muchos usuarios simultáneos.
- Programas que permiten acceder a contenidos susceptibles de contener amenazas de seguridad o que están protegidos por licencias que la empresa no ha adquirido previamente.
- Programas que permiten acceder a contenidos no relacionados con la actividad de la empresa y que pueden afectar al ritmo de trabajo de los usuarios.

CONTENIDO DEL CAPÍTULO

Acceso a la configuración Bloqueo de programas

Para crear una nueva configuración de bloqueo de programas o asignar una ya existente a grupos de equipos de la red, sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Configuración**, panel lateral **Bloqueo de programas**. Se mostrará un listado de las configuraciones ya creadas.
- Para crear una nueva configuración haz clic en el botón **Añadir** situado en la parte superior

derecha de la ventana. Para conocer en detalle las opciones de configuración consulta el apartado "**Configuración Bloqueo de programas**".

Las configuraciones de bloqueo de programas solo se pueden asignar a puestos de trabajo o servidores Windows.

Configuración Bloqueo de programas

Para crear una nueva configuración o modificar una existente introduce la información mostrada a continuación:

Campo	Descripción
Nombre	Nombre de la política de configuración.
Descripción	Descripción de la política de configuración.
Destinatarios	Grupos y equipos que recibirán la política de configuración
Nombres de los programas a bloquear	Nombres de los ficheros que Cytomic EPDR impedirá su ejecución. En esta caja de texto acepta listas de nombres de ficheros copiadas / pegadas y separados por retorno de carro. No se admiten comodines para evitar configuraciones demasiado amplias que comprometan el buen funcionamiento del equipo.
Código MD5 de los programas a bloquear	MD5 de los ficheros que Cytomic EPDR impedirá su ejecución. En esta caja de texto acepta listas de MD5s copiadas / pegadas y separados por retorno de carro.
Informar	Muestra al usuario del equipo la razón del bloqueo del programa que intentó ejecutar.

Tabla 17.1: configuración de una política de seguridad Bloqueo de programas

No bloquees programas del sistema operativo o componentes que sean necesarios para poder ejecutar correctamente los programas de usuario.

Cytomic EPDR no bloqueará ninguno de sus programas o módulos para garantizar el correcto funcionamiento de la solución de seguridad instalada.

Listados de bloqueo de programas

Listado de Programas bloqueados por el administrador

Muestra el detalle de los programas bloqueados por Cytomic EPDR en los equipos de usuario y servidores.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Ruta	Ruta y nombre del programa bloqueado por el administrador en el equipo del usuario.	Cadena de caracteres
Fecha	Fecha en la que Cytomic EPDR bloqueó el programa.	Fecha

Tabla 17.2: campos del listado Programas bloqueados por el administrador

- **Campos mostrados en fichero exportado**

Campo	Descripción	Valores
Ruta	Ruta y nombre del programa bloqueado por el administrador en el equipo del usuario.	Cadena de caracteres
Hash	MD5 del programa bloqueado por el administrador.	Cadena de caracteres
Fecha	Fecha en la que Cytomic EPDR bloqueó el programa.	Fecha
Usuario logeado	Cuenta de usuario del sistema operativo que lanza el programa bloqueado.	Cadena de caracteres
Acción	Acción ejecutada por Cytomic EPDR.	Cadena de caracteres "Bloquear"

Tabla 17.3: campos del fichero exportado Programas bloqueados por el administrador

- **Herramienta de filtrado**

Campo	Descripción	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Fechas	Intervalo de fechas en el que se ha producido el bloqueo del programa.	• Últimas 24 horas • Últimos 7 días • Último mes

Tabla 17.4: campos de filtrado para el listado Programas bloqueados por el administrador

Paneles / widgets de bloqueo de programas

Para acceder al panel de widgets haz clic en el menú superior **Estado**, panel lateral **Seguridad.**

Programas bloqueados por el administrador

Muestra el número de intentos de ejecución registrados en el parque informático y bloqueados por Cytomic EPDR según la configuración establecida por el administrador de la red.

Figura 17.1: Panel Programas bloqueados por el administrador

- **Significado de las series**

Serie	Descripción
Bloqueados	Número de intentos de ejecución registrados en el parque informático y bloqueados por Cytomic EPDR en el intervalo configurado.

Tabla 17.5: descripción de la serie Programas bloqueados por el administrador

- **Filtros preestablecidos desde el panel**

Figura 17.2: zonas activas del panel Programas bloqueados por el administrador

Al hacer clic en las zonas indicadas en la figura 17.2 se abre el listado **Programas bloqueados por el administrador** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtros.

Tabla 17.6: definición de filtros del listado Programas bloqueados por el administrador

Parte 6

Visibilidad y gestión de las amenazas

Capítulo 18: Visibilidad del malware y del parque informático

Capítulo 19: Gestión de amenazas, elementos en clasificación y cuarentena

Capítulo 20: Análisis forense

Capítulo 21: Alertas

Capítulo 22: Envío programado de informes y listados

Capítulo 18

Visibilidad del malware y del parque informático

Cytomic EPDR ofrece al administrador tres grandes grupos de herramientas para visualizar el estado de la seguridad y del parque informático que gestiona:

- El panel de control, con información actualizada en tiempo real.
- Listados personalizables de incidencias, malware detectado y dispositivos gestionados junto a su estado.
- Informes con información del estado del parque informático, recogida y consolidada a lo largo del tiempo.

*Los informes consolidados se tratan en el capítulo "**Envío programado de informes y listados**" en la página **479**.*

Las herramientas de visualización y monitorización determinan en tiempo real el estado de la seguridad de la red y el impacto de las brechas de seguridad que se puedan producir para facilitar la adopción de las medidas de seguridad apropiadas.

CONTENIDO DEL CAPÍTULO

Paneles / Widgets de seguridad

Para acceder a los paneles que muestran el estado de la seguridad y a sus listados asociados haz clic en el menú superior Estado y en el menú lateral Seguridad  .

A continuación, se detallan los distintos widgets implementados en el dashboard de Cytomic EPDR, las distintas áreas y zonas activas incorporadas y los tooltips y su significado.

Estado de protección

Muestra los equipos donde Cytomic EPDR funciona correctamente y aquellos con errores y problemas en la instalación o en la ejecución del módulo de protección. El estado de los equipos es representado mediante un círculo con distintos colores y contadores asociados.

La suma de los porcentajes de las diferentes series puede resultar más de un 100% debido a que los estados no son mutuamente excluyentes y un mismo equipo puede encontrarse en varias series a la vez.

El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

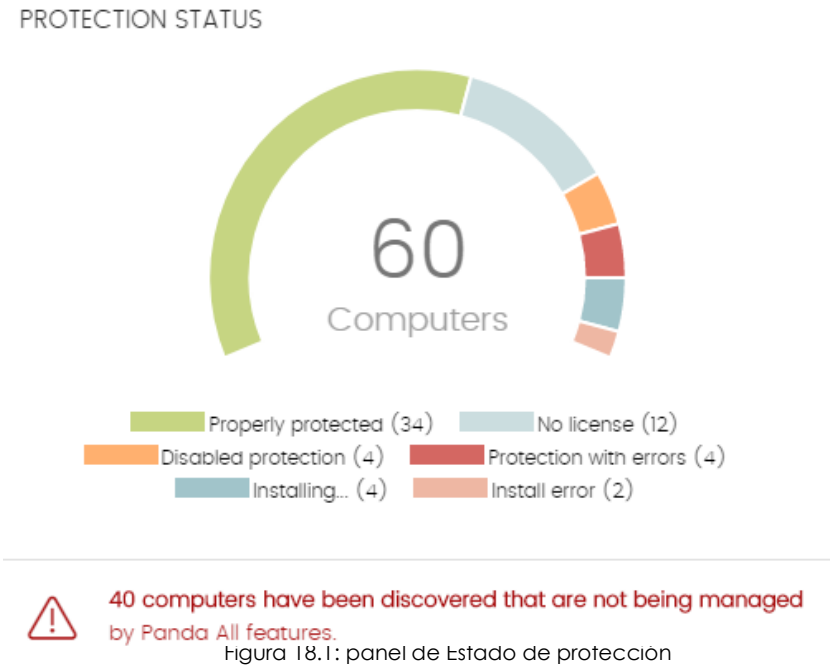


Figura 18.1: panel de Estado de protección

- **Descripción de las series**

Serie	Descripción
Correctamente protegido	Porcentaje de equipos en los que Cytomic EPDR se instaló sin errores y su ejecución no presenta problemas.
Instalando...	Porcentaje de equipos en los que Cytomic EPDR se encuentra en proceso de instalación.
Sin licencia	Equipos sin protección por la falta de suficientes licencias, o por no haberse asignado una licencia disponible.
Protección desactivada	Equipos sin activar la protección antivirus ni la protección avanzada, si ésta última se encuentra disponible para el sistema operativo del equipo en particular.
Protección con error	Equipos con Cytomic EPDR instalado cuyo módulo de protección no responde a las peticiones desde los servidores de Cytomic.
Error instalando	Equipos cuya instalación no se pudo completar.
Parte central	Equipos con un agente Cytomic instalado.

Tabla 18.1: descripción de la serie Equipos desprotegidos

- **Filtros preestablecidos desde el panel**

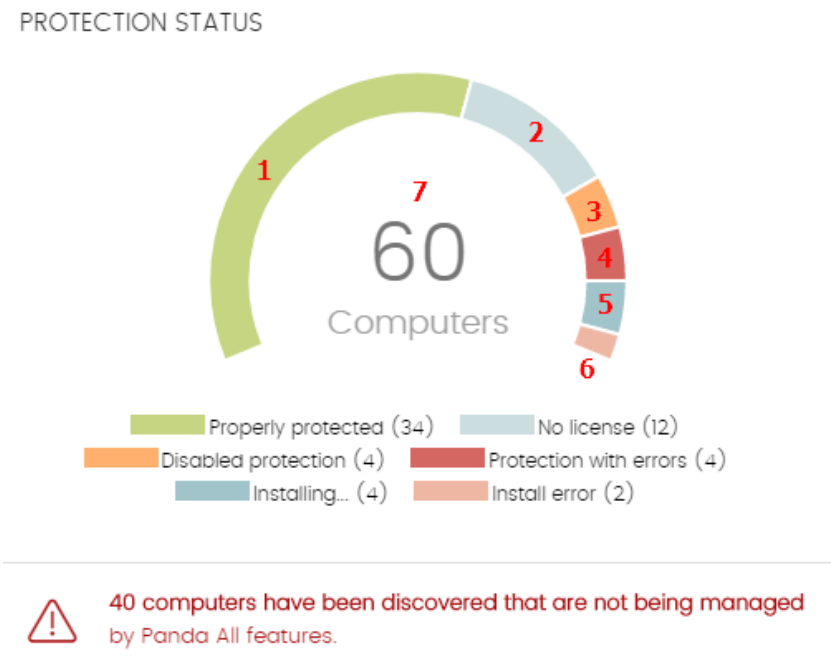


Figura 18.2: zonas activas del panel Estado de protección

Haz clic en las zonas indicadas en la figura 18.2 para abrir el listado **Estado de protección de los equipos** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de protección = Correctamente protegido.
(2)	Estado de protección = Instalando…
(3)	Estado de protección = Protección desactivada.
(4)	Estado de protección = Protección con error.
(5)	Estado de protección = Sin licencia.
(6)	Estado de protección = Error instalando.
(7)	Sin filtro.

Tabla 18.2: definición de filtros del listado Estado de protección de los equipos

Equipos sin conexión

Muestra los equipos de la red que no han conectado con la nube de Cytomic en un determinado periodo de tiempo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.

Figura 18.3: panel Equipos sin conexión

- **Descripción de las series**

Serie	Descripción
72 horas	Número de equipos que no enviaron su estado en las últimas 72 horas.
7 días	Número de equipos que no enviaron su estado en las últimas 7 días.
30 días	Número de equipos que no enviaron su estado en las últimas 30 días.

Tabla 18.3: descripción de la serie Equipos sin conexión

- **Filtros preestablecidos desde el panel**

Figura 18.4: zonas activas del panel Equipos sin conexión

Haz clic en las zonas indicadas en la figura 18.4 para abrir el listado **Equipos sin conexión** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 72 horas.
(2)	Última conexión = Hace más de 7 días.
(3)	Última conexión = Hace más de 30 días.

Tabla 18.4: definición de los filtros del listado Equipos sin conexión

Protección desactualizada

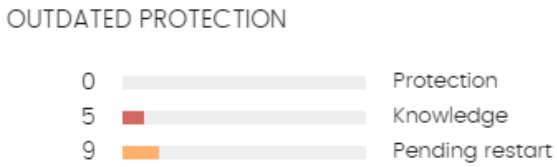


Figura 18.5: Panel Protección desactualizada

Muestra los equipos cuya última versión del fichero de firmas instalada difiere en más de 3 días del fichero publicado por Cytomic. También muestra los equipos cuya versión del motor de protección difiere en más de 7 días del publicado por Cytomic. Por lo tanto, estos equipos pueden ser vulnerables frente a los ataques de amenazas.

- **Descripción de las series**

El panel muestra el porcentaje y el número de equipos vulnerables por estar desactualizados, divididos en tres conceptos:

Serie	Descripción
Protección	Desde hace 7 días el equipo tiene un motor de protección instalado anterior a la última versión publicada por Cytomic.
Conocimiento	Desde hace 3 días el equipo no se actualiza con el fichero de firmas publicado.
Pendiente de reinicio	El equipo requiere un reinicio para completar la actualización.

Tabla 18.5: descripción de la serie Protección desactualizada

- **Filtros preestablecidos desde el panel**

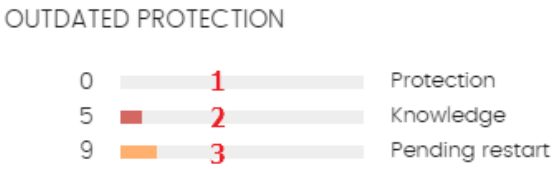


Figura 18.6: Zonas activas del panel Protección desactualizada

Haz clic en las zonas indicadas en la figura 18.6 para abrir el listado **Estado de protección de los equipos** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Protección actualizada = No.
(2)	Conocimiento = No.
(3)	Protección actualizada = Pendiente de reinicio.

Tabla 18.6: definición de los filtros del listado Equipos con protección desactualizada

Programas actualmente bloqueados en clasificación

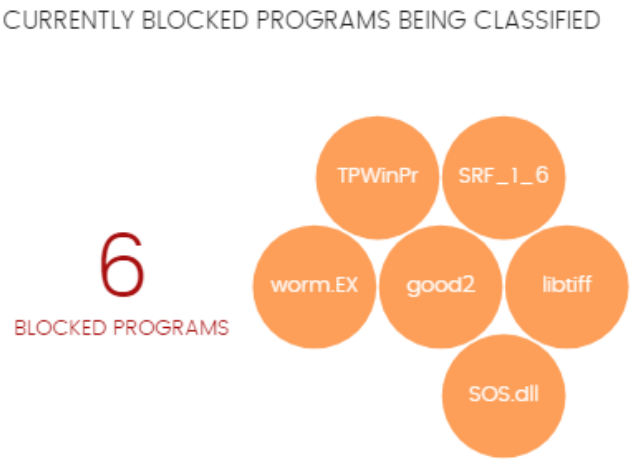


Figura 18.7: panel de Programas actualmente bloqueados en clasificación

Muestra un histórico de los elementos bloqueados que aún no han sido clasificados abarcando desde la puesta en marcha del servicio en el cliente hasta el momento actual. Este widget no se ve afectado por la selección del intervalo de tiempo establecida por el administrador.

En el panel de ejemplo se muestran un total de 6 elementos bloqueados en clasificación. Se trata de 6 aplicaciones que han sido bloqueadas y se están investigando. Cada una de ellas se representa con un círculo.

El número total de elementos bloqueados en clasificación representa las aplicaciones diferentes (con un MD5 diferente) que están siendo bloqueadas. Este número es independiente de la cantidad de intentos de ejecución que cada aplicación bloqueada ha llevado a cabo en cada equipo de la red.

Cada versión encontrada del programa (distinto MD5) se muestra de forma independiente.

El tamaño de las burbujas es una función del número de equipos donde se encontró el programa desconocido que fue bloqueado. De esta forma, un proceso que se ejecuta en muchos equipos tendrá asignada una única burbuja de gran tamaño, frente a un proceso que solo se ha ejecutado en un único equipo, que quedará representado con una burbuja más pequeña.

- **Descripción de las series**

En el panel de control, las aplicaciones bloqueadas se muestran con el código de colores indicado a continuación:

Serie	Descripción
Naranja	Aplicaciones con probabilidad media de ser malware.
Naranja oscuro	Aplicaciones con probabilidad alta de ser malware.

Tabla 18.7: descripción de la serie Programas actualmente bloqueados en clasificación

Serie	Descripción
Rojo	Aplicaciones con probabilidad muy alta de ser malware.

Tabla 18.7: descripción de la serie Programas actualmente bloqueados en clasificación

Al pasar el ratón por encima cada círculo se amplía, mostrando su nombre completo y una serie de iconos que representan acciones clave:

Figura 18.8: representación gráfica de un programa en clasificación

- **Carpeta**: el programa ha leído datos del disco duro del usuario.
- **Bola del mundo**: el programa estableció una conexión con otro equipo.

- **Filtros preestablecidos desde el panel**

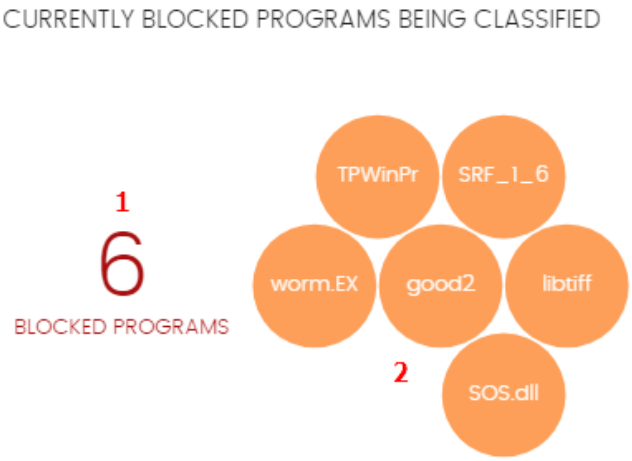


Figura 18.9: zonas activas del panel Programas actualmente bloqueados en clasificación

Haz clic en las zonas indicadas en la figura 18.9 para abrir el listado **Programas actualmente bloqueados en clasificación** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtros.
(2)	Buscar = Hash.

Tabla 18.8: definición de los filtros del listado Programas actualmente bloqueados en clasificación

Programas permitidos por el administrador

Figura 18.10: Panel Programas permitidos por el administrador

Cytomic EPDR impide la ejecución de todos los programas clasificados como malware y, adicionalmente, dependiendo de la configuración de la protección avanzada, también bloqueará los programas no vistos anteriormente hasta que sean analizados y emitida una clasificación sobre su seguridad.

En el caso de que un usuario no pueda esperar a que se emita esta clasificación, o el administrador quiera permitir la ejecución de un elemento ya clasificado como amenaza, Cytomic EPDR implementa recursos para evitar estos bloqueos de ejecución.

> *Cytomic EPDR ejecuta todas las librerías y binarios utilizados en los programas permitidos por el administrador, excepto aquellos ya conocidas y clasificados como amenazas.*

- **Descripción de las series**

El panel representa el número total de elementos que el administrador excluyó del bloqueo, desagregados en tres conceptos:

- Malware
- PUP
- En clasificación

- **Filtros preestablecidos desde el panel**

Figura 18.11: zonas activas del panel Programa permitidos por el administrador

Haz clic en las zonas indicadas en la figura 18.11 para abrir el listado **Programas permitidos por el administrado** con los filtros preestablecidos mostrados a continuación:.

Zona activa	Filtro
(1)	Sin filtros.
(2)	Clasificación actual = malware.
(3)	Clasificación actual = PUP.
(4)	Clasificación actual = En clasificación (bloqueados y sospechosos).

Tabla 18.9: definición de los filtros del listado Programas permitidos por el administrador

Actividad de malware / PUP

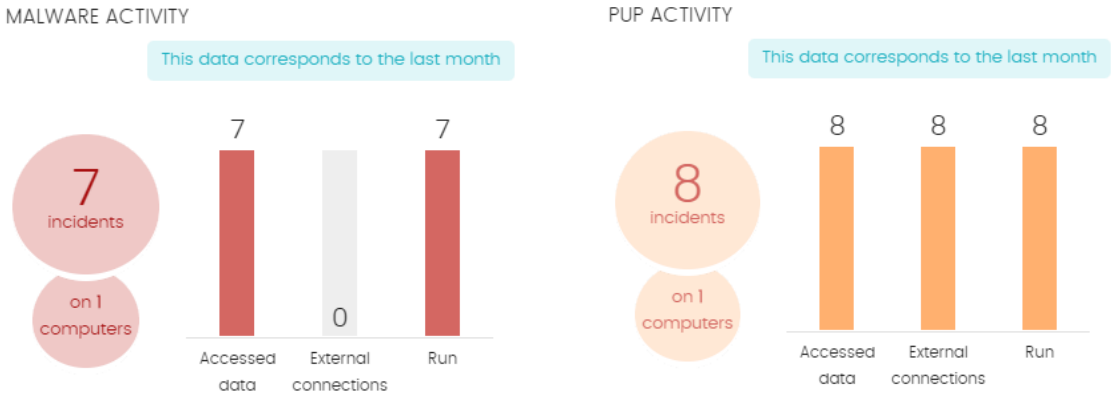


Figura 18.12: panel de Actividad de malware / PUP

Muestra las incidencias detectadas en los procesos ejecutados por los equipos de usuario y servidores Windows, así como en sus sistemas de ficheros. Estas incidencias son reportadas tanto por el análisis en tiempo real como por las tareas de análisis bajo demanda.

Cytomic EPDR genera una incidencia en el panel Actividad de malware / PUP atendiendo a las siguientes reglas:

- Por cada pareja equipo - amenaza - tipo de amenaza distinta encontrada en la red.
- Solo se registra la primera incidencia si se repite varias veces en los primeros 5 minutos.
- Una misma incidencia se registra como máximo 2 veces cada 24 horas.

- **Descripción de las series**

Serie	Descripción
Número de incidencias	Número de incidencias / avisos en Número de equipos detectadas.

Tabla 18.10: descripción de la serie Actividad de malware / PUP

Serie	Descripción
Acceso a datos	Número de avisos que incluyen uno o varios accesos a información del usuario contenida en el disco duro de su equipo.
Conexiones exteriores	Número de avisos que establecieron conexiones con otros equipos.
Ejecutado	Número de muestras malware que se llegaron a ejecutar.

Tabla 18.10: descripción de la serie Actividad de malware / PUP

Actividad de malware, Actividad de PUPs y Actividad de exploits muestran datos con un intervalo máximo de 1 mes. En el caso de que el administrador establezca un periodo de tiempo mayor se mostrará un texto explicativo en la parte superior del panel.

- **Filtros preestablecidos desde el panel**

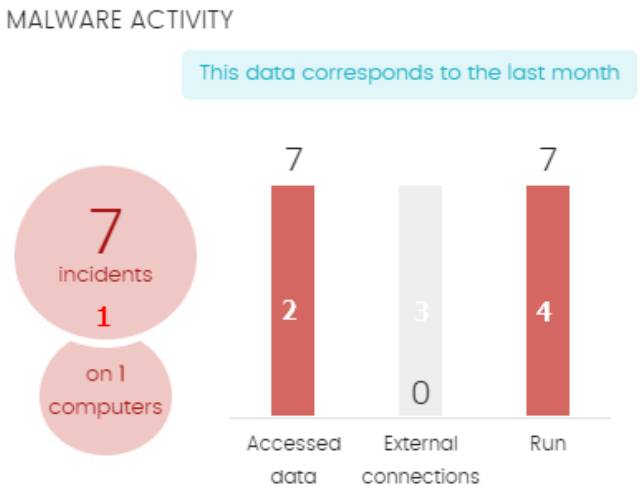


Figura 18.13: zonas activas del panel Actividad de malware / PUP

Haz clic en las zonas indicadas en la figura 18.13 para abrir el listado **Actividad del malware y PUPs** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Tipo de amenaza = (Malware O PUP).
(2)	Acceso a datos = Verdadero.
(3)	Conexiones externas = Verdadero.
(4)	Ejecutado = Verdadero.

Tabla 18.11: definición de los filtros del listado Actividad de malware / PUP

Actividad de exploits

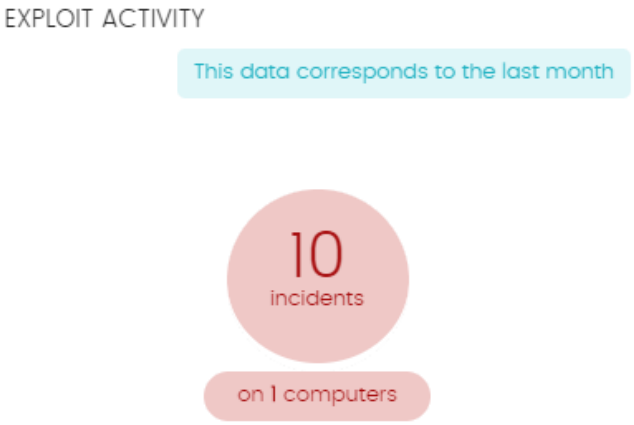


Figura 18.14: panel de Actividad de exploits

Muestra el número de ataques por explotación de vulnerabilidades recibidos en los equipos Windows de la red. Cytomic EPDR genera una incidencia en el panel Actividad de exploits por cada pareja equipo -exploit distinto encontrada en la red. Si el ataque se repite, se generarán un máximo de 10 incidencias cada 24 horas por cada equipo - exploit encontrado.

- **Descripción de las series**

Serie	Descripción
Número de incidencias / ataques	Número de incidencias / ataques en Número de equipos detectadas.

Tabla 18.12: descripción de la serie Actividad de exploits

- **Filtros preestablecidos desde el panel**

Al hacer clic en cualquier zona del widget se mostrará el listado **Actividad de exploits** filtrado por el último mes.

Clasificación de todos los programas ejecutados y analizados

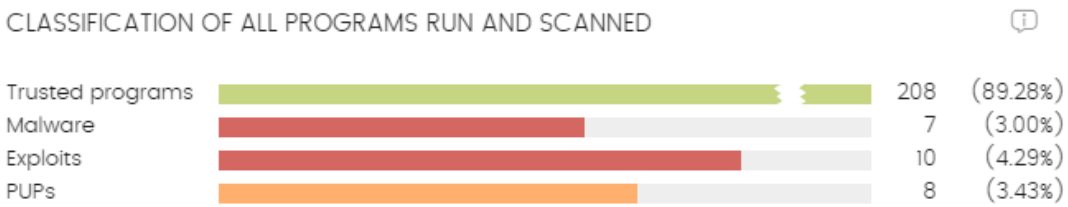


Figura 18.15: panel de Clasificación de todos los programas ejecutados y analizados

Localiza de forma rápida el porcentaje de aplicaciones goodware y malware vistas y clasificadas en la red del cliente, para el intervalo de tiempo establecido por el administrador.

- **Descripción de las series**

El panel consta de cuatro barras horizontales junto al número de eventos asociado y el porcentaje sobre el total.

> *Este panel muestra datos de elementos clasificados para todo el parque informático, y no solo de aquellos equipos sobre los cuales el administrador tenga permisos según sus credenciales de acceso a la consola. Los elementos no clasificados no se muestran en este panel.*

Serie	Descripción
Aplicaciones confiables	Aplicaciones vistas en el parque del cliente que han sido analizadas y su clasificación ha sido goodware.
Aplicaciones maliciosas	Programas que han intentado ejecutarse o han sido analizados en el parque del cliente, y han sido clasificadas como malware o ataques dirigidos.
Exploits	Número de intentos de explotación de aplicaciones detectados en la red.
Aplicaciones potencialmente no deseadas	Programas que han intentado ejecutarse o han sido analizados en el parque del cliente, y han sido clasificadas como malware de tipo PUP.

Tabla 18.13: descripción de la serie Clasificación de todos los programas ejecutados y analizados

- **Filtros preestablecidos desde el panel**

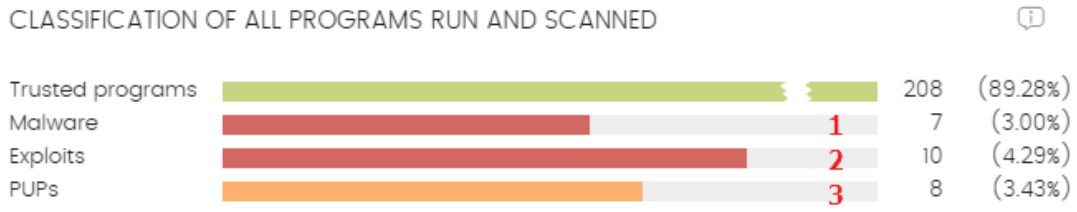


Figura 18.16: zonas activas del panel Clasificación de todos los programas ejecutados y analizados

Haz clic en las zonas indicadas en la figura 18.16para abrir diferentes listados sin filtros preestablecidos:

Zona activa	Filtro
(1)	Listado Actividad del malware.
(2)	Listado Actividad de exploit.
(3)	Listado Actividad de PUPs.

Tabla 18.14: listados accesibles desde el panel Clasificación de todos los programas ejecutados y analizados

Amenazas detectadas por el antivirus

Consolida todos los intentos de intrusión que Cytomic EPDR gestionó en el periodo de tiempo establecido.

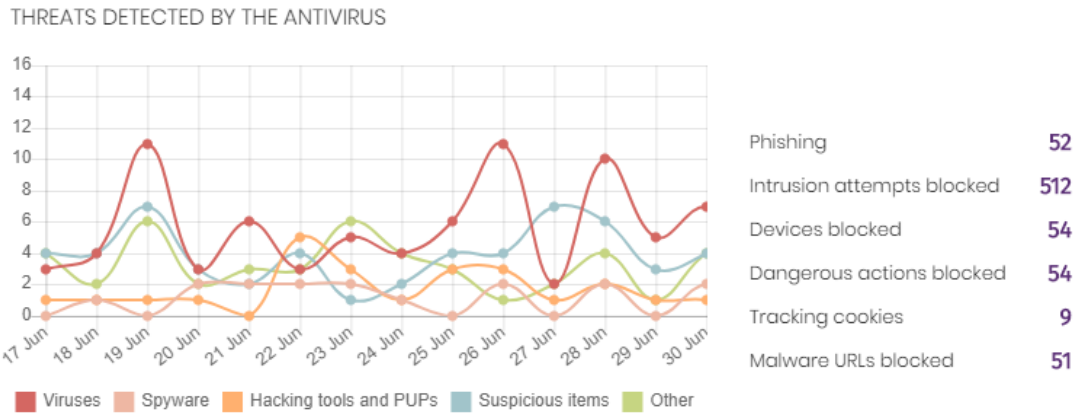


Figura 18.17: panel Amenazas detectadas por el antivirus

Los datos reflejados abarcan todos los vectores de infección y todas las plataformas soportadas, de manera que el administrador pueda disponer de información concreta (volumen, tipo, forma de ataque) relativa a la llegada de malware a la red, durante el intervalo de tiempo determinado.

- **Descripción de las series**

Este panel está formado por dos secciones: un gráfico de líneas y un listado resumen.

El diagrama de líneas representa las detecciones encontradas en el parque informático a lo largo del tiempo separadas por tipo de malware:

Serie	Descripción
Virus y spyware	Programa que se introduce en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.
Herramientas de hacking y PUPs	Programa utilizado por hackers para causar perjuicios a los usuarios de un ordenador, pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc.
Sospechosos	Programa que, tras un análisis de su comportamiento realizado en el equipo del usuario por la protección de Cytomic EPDR, tiene una alta probabilidad de ser considerado malware.
Phishing	Intento de conseguir de forma fraudulenta información confidencial de un usuario mediante el engaño. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito o cuentas bancarias.
Otros	Hoax, Worms, Troyanos y otros tipos de virus.

Tabla 18.15: descripción de la serie Amenazas detectadas por el antivirus

El listado de la derecha muestra los eventos relevantes que requieren una supervisión por parte del administrador en busca de síntomas o situaciones potenciales de peligro.

Serie	Descripción
Acciones peligrosas bloqueadas	Detecciones realizadas por análisis del comportamiento local.
Intentos de intrusión bloqueados	Detección de tráfico de red mal formado cuyo objetivo es provocar un error de ejecución en algún componente del equipo que origine un comportamiento indeseado en el sistema.
Dispositivos bloqueados	Intento de uso por parte del usuario del equipo de un dispositivo restringido según la configuración establecida por el administrador de la red en el módulo Control de dispositivos.
Tracking cookies	Cookies detectadas para registrar la navegación de los usuarios.
URL con malware bloqueadas	Direcciones Web que apuntaban a páginas con malware.

Tabla 18.16: descripción de la serie Amenazas detectadas por el antivirus

- **Filtros preestablecidos desde el panel**

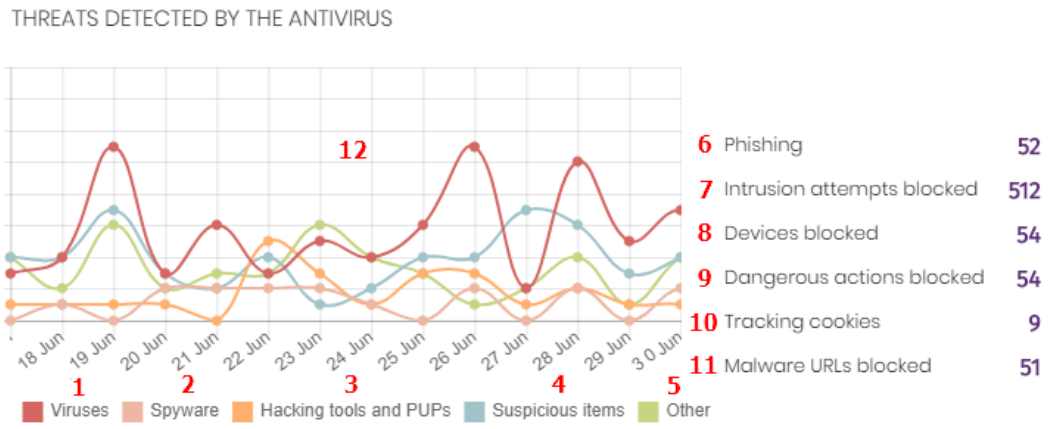


Figura 18.18: zonas activas del paneyl Amenazas detectadas por el antivirus

Haz clic en las zonas indicadas en la figura 18.18 para abrir el listado con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(1)	Amenazas detectadas por el antivirus	Tipo de amenaza = Virus.
(2)	Amenazas detectadas por el antivirus	Tipo de amenaza = Spyware.
(3)	Amenazas detectadas por el antivirus	Tipo de amenaza = Herramientas de hacking y PUPs.

Tabla 18.17: definición de los filtros del listado Amenazas detectadas por el antivirus

Zona activa	Listado	Filtro
(4)	Amenazas detectadas por el antivirus	Tipo de amenaza = Sospechosos.
(5)	Amenazas detectadas por el antivirus	Tipo de amenaza = Otros.
(6)	Amenazas detectadas por el antivirus	Tipo de amenaza = Phishing.
(7)	Intentos de intrusión bloqueados	Sin filtro.
(8)	Dispositivos bloqueados	Sin filtro.
(9)	Amenazas detectadas por el antivirus	Tipo de amenaza = Acciones peligrosas bloqueadas.
(10)	Amenazas detectadas por el antivirus	Tipo de amenaza = Tracking cookies.
(11)	Amenazas detectadas por el antivirus	Tipo de amenaza = URLs con malware.
(12)	Amenazas detectadas por el antivirus	Sin filtro.

Tabla 18.17: definición de los filtros del listado Amenazas detectadas por el antivirus

Filtrado de contenidos en servidores Exchange

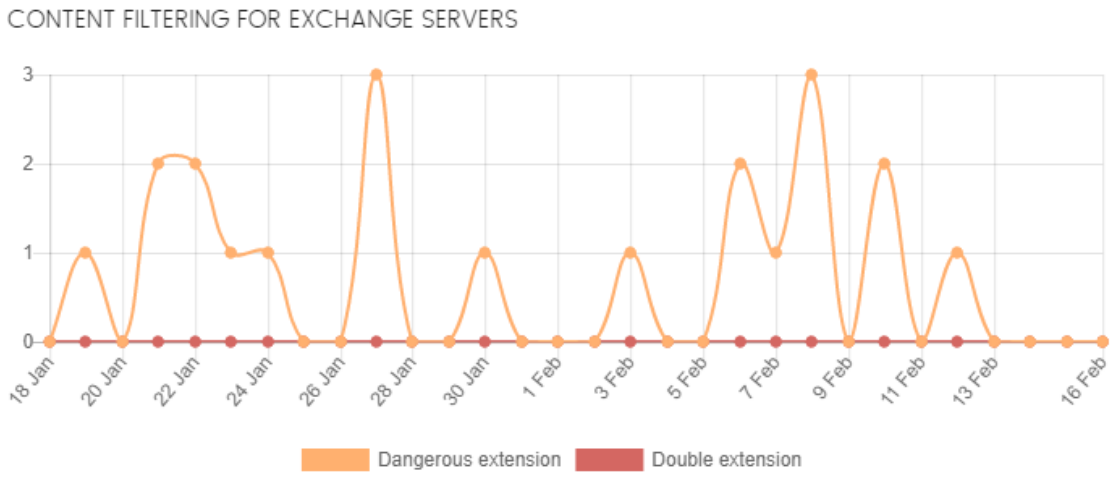


Figura 18.19: panel Filtrado de contenidos en servidores Exchange

Muestra la cantidad de mensajes que fueron bloqueados por el filtro de contenidos del servidor Exchange.

- **Descripción de las series**

Este panel presenta dos series de datos de tipo histórico: el número de mensajes filtrados por contener adjuntos con extensión peligrosa, y por doble extensión.

Al pasar el ratón por las series se muestra un tooltip con la siguiente información:

Serie	Descripción
Extensión peligrosa	Número de mensajes filtrados por contener adjuntos con extensión peligrosa.
Doble extensión	Número de mensajes filtrados por contener adjuntos con doble extensión.

Tabla 18.18: descripción de la serie Filtrado de contenidos en servidores Exchange

Accesos a páginas web

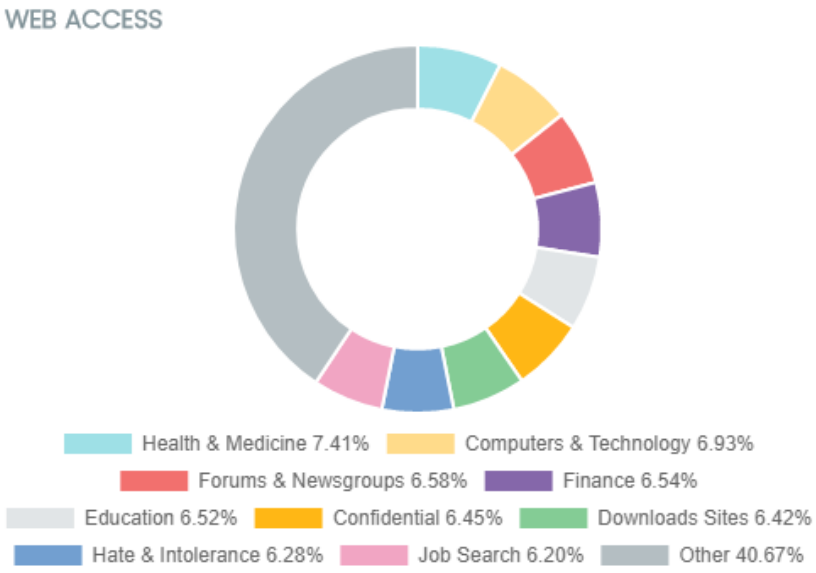


Figura 18.20: panel Accesos a páginas web

Muestra mediante un gráfico de tarta la distribución de categorías Web solicitadas por los usuarios de la red.

- **Descripción de las series**

El panel de tipo tarta muestra los 10 grupos de páginas web más importantes que Cytomic EPDR soporta a la hora de categorizar las páginas web navegadas por los usuarios de la red:

- Odio e intolerancia
- Actividades criminales
- Búsqueda de empleo
- Contactos y anuncios personales
- Finanzas
- Confidencial
- Ocio y espectáculos

- Gobierno
- Drogas ilegales
- Otros

En la zona de la leyenda del panel se muestran los porcentajes de peticiones que encajan con cada categoría.

- **Filtros preestablecidos desde la tabla**

Haz clic en las categorías mostradas en la figura 18.20 para abrir el listado **Accesos a páginas web por equipo** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
Cualquiera	Categoría = Categoría seleccionada.

Tabla 18.19: definición de los filtros Accesos a páginas web por equipo

Categorías más accedidas (top 10)

Detalla en número de accesos y el número de equipos que han accedido a las 10 categorías de páginas más visitadas.

Cada categoría indica el número de accesos totales en el rango de fechas seleccionado, y el número de equipos que han accedido una o más veces a esa categoría.

Figura 18.21: panel Categorías más accedidas

- **Filtros preestablecidos desde el panel**

Se muestra el listado **Accesos a páginas web por equipo** con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro de la tabla.

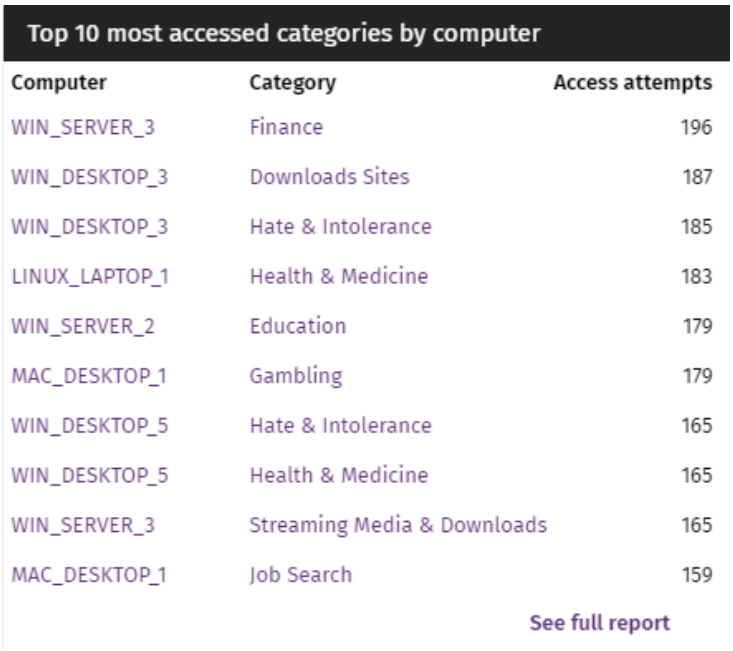
Zona activa	Filtro
Categoría	Categoría = Categoría seleccionada.

Tabla 18.20: definición de los filtros del listado Accesos a páginas web por equipo

Zona activa	Filtro
Ver informe completo	Muestra el listado Accesos a paginas web por categoría sin filtros.

Tabla 18.20: definición de los filtros del listado Accesos a páginas web por equipo

Categorías más accedidas por equipo (top 10)



Top 10 most accessed categories by computer

Computer	Category	Access attempts
WIN_SERVER_3	Finance	196
WIN_DESKTOP_3	Downloads Sites	187
WIN_DESKTOP_3	Hate & Intolerance	185
LINUX_LAPTOP_1	Health & Medicine	183
WIN_SERVER_2	Education	179
MAC_DESKTOP_1	Gambling	179
WIN_DESKTOP_5	Hate & Intolerance	165
WIN_DESKTOP_5	Health & Medicine	165
WIN_SERVER_3	Streaming Media & Downloads	165
MAC_DESKTOP_1	Job Search	159

See full report

Figura 18.22: panel Categorías más accedidas por equipo (Top 10)

En este panel se detallan el número de accesos ordenados por categorías de los 10 equipos que más han visitado la web.

- **Filtros preestablecidos desde el panel**

Haz clic en las distintas zonas de la figura **18.22** para abrir el listado **Accesos a páginas web por equipo** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
Equipo	Equipo = Equipo seleccionado.
Categoría	Categoría = Categoría seleccionada.
Ver listado completo	Sin filtro.

Tabla 18.21: definición de los filtros del listado Accesos a páginas web por equipo

Categorías más bloqueadas (top 10)

Top 10 most blocked categories

Category	Denied access attempts	Computers
Health & Medicine	1,157	11
Criminal Activity	1,123	11
Hate & Intolerance	1,062	11
Finance	1,020	10
Government	999	10
Illegal Drugs	985	11
Computers & Technology	929	11
Gambling	918	11
Entertainment	915	10
Unknown	908	11

See full report

Figura 18.23: zonas activas del panel Categorías más bloqueadas

Indica las 10 categorías de páginas más bloqueadas de la red, junto al número de accesos bloqueados y el número de equipos que realizaron la visita y fueron bloqueados.

- **Filtros preestablecidos desde el panel**

Haz clic en las distintas zonas de la figura 18.23 para abrir el listado **Accesos a páginas web por equipo** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
Categoría	Categoría = Categoría seleccionada.
Ver listado completo	Muestra el listado Accesos a paginas web por categoría sin filtros.

Tabla 18.22: definición de los filtros de Accesos a páginas web por equipo

Categorías más bloqueadas por equipo (Top 10)

Top 10 most blocked categories by computer

Computer	Category	Denied access attempts
LINUX_LAPTOP_1	Health & Medicine	198
WIN_DESKTOP_5	Criminal Activity	184
WIN_SERVER_2	Unknown	181
LINUX_LAPTOP_1	Job Search	181
WIN_DESKTOP_2	Hate & Intolerance	179
WIN_DESKTOP_5	Health & Medicine	179
WIN_SERVER_3	Finance	178
WIN_SERVER_2	Education	173
MAC_DESKTOP_1	Job Search	171
WIN_DESKTOP_3	Hate & Intolerance	165

Figura 18.24: panel categorías más bloqueadas por equipo (Top 10)

Muestra los 10 pares equipo - categoría con mayor número de accesos bloqueados de la red, indicando el nombre del equipo, la categoría y el número de accesos denegados por cada par equipo - categoría.

- **Filtros preestablecidos desde el panel**

Haz clic en las distintas zonas de la figura **18.24** para abrir el listado **Accesos a páginas web por equipo** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
Equipo	Nombre de equipo = Equipo.
Categoría	Categoría = categoría seleccionada.
Ver listado completo	Sin filtro.

Tabla 18.23: definición de los filtros de Accesos a páginas web por equipo

Listados de seguridad

Los listados de seguridad muestran la información de la actividad relativa a la protección de los equipos de la red recogida por Cytomic EPDR, y cuentan con un grado de detalle muy alto al contener la información en bruto utilizada para generar los widgets.

Para acceder a los listados de seguridad elige uno de los dos procedimientos mostrados a continuación:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad** y en widget para abrir su listado asociado. Dependiendo del lugar donde se haga clic dentro del widget se aplicará un filtro distinto asociado al listado.

o

- En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una

ventana donde se muestran todos los listados disponibles en Cytomic EPDR.

- Haz clic en un listado de la sección **Seguridad**. Se mostrara el listado apropiado sin filtros establecidos.

Al hacer clic en una entrada del listado se mostrará la ventana de detalle, que se ajustará al tipo de información mostrada.

Listado de Estado de protección de los equipos

Muestra en detalle todos los equipos de la red, incorporando filtros que permiten localizar aquellos puestos de trabajo o dispositivos móviles que no estén protegidos por alguno de los conceptos mostrados en el panel asociado.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	• Cadena de caracteres • Grupo Todos • Grupo nativo • Grupo Directorio activo
Protección avanzada	Estado de la protección avanzada.	• Instalando • Error. Si es conocido se mostrará su origen, si es desconocido se mostrará el código de error • Activado • Desactivado • Sin licencia
Antivirus	Estado de la protección antivirus	• Instalando • Error. Si es conocido se mostrará su origen, si es desconocido se mostrará el código de error • Activado • Desactivado • Sin licencia

Tabla 18.24: campos del listado Estado de protección de los equipos

Campo	Descripción	Valores
Protección actualizada	El módulo de la protección instalado en el equipo coincide con la última versión publicada o no. Al pasar el puntero del ratón por encima del campo se muestra la versión de la protección instalada.	• Actualizado • No actualizado (7 días sin actualizar desde la publicación) • Pendiente de reinicio.
Conocimiento	El fichero de firmas descargado en el equipo coincide con la última versión publicada o no. Al pasar el puntero del ratón por encima del campo se muestra la fecha de actualización de la versión descargada.	• Actualizado • No actualizado (3 días sin actualizar desde la publicación)
Última conexión	Fecha del último envío del estado de Cytomic EPDR a la nube de Cytomic.	Fecha

Tabla 18.24: campos del listado Estado de protección de los equipos

- **Campos mostrados en fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del módulo agente Cytomic.	Cadena de caracteres
Fecha instalación	Fecha en la que el Software Cytomic EPDR se instaló con éxito en el equipo.	Fecha

Tabla 18.25: campos del fichero exportado Estado de protección de los equipos

Campo	Descripción	Valores
Fecha de la última actualización	Fecha de la última actualización del agente.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS • Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Servidor Exchange	Versión del servidor de correo instalada en el servidor.	Cadena de caracteres
Protección actualizada	El módulo de la protección instalado en el equipo es la última versión publicada.	Binario
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Conocimiento actualizado	El fichero de firmas descargado en el equipo es la última versión publicada.	Binario
Fecha de última actualización	Fecha de la descarga del fichero de firmas.	Fecha
Protección avanzada **Antivirus de archivos** **Antivirus de correo** **Antivirus para navegación web** **Firewall** **Control de dispositivosControl de acceso a páginas web** **Antivirus para servidores Exchange** **Anti-spam para servidors Exchange** **Filtrado de contenidos para servidores Exchange**	Estado de la protección asociada.	• No instalado • Error: si es conocido se mostrará su origen, si es desconocido se mostrará el código de error • Activado • Desactivado • Sin licencia
Estado de aislamiento	El equipo esta aislado de la red.	• Aislado • No aislado

Tabla 18.25: campos del fichero exportado Estado de protección de los equipos

Campo	Descripción	Valores
Fecha de error	Se produjo un error en la instalación de Cytomic EPDR en la fecha y hora indicadas.	Fecha
Error instalación	Descripción del error producido en la instalación de Cytomic EPDR en el equipo.	Cadena de caracteres
Otros productos de seguridad	Nombre del antivirus de terceros fabricantes encontrado en el equipo en el momento de la instalación de Cytomic EPDR.	Cadena de caracteres

Tabla 18.25: campos del fichero exportado Estado de protección de los equipos

- **Herramienta de filtrado**

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Cytomic EPDR a la nube de Cytomic.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días • Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Protección actualizada	La protección instalada coincide con la última versión publicada o no.	• Todos • Si • No • Pendiente de reinicio
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS • Android
Conocimiento	Indica si el fichero de firmas encontrado en el equipo es o no el último publicado.	Binario

Tabla 18.26: campos de filtrado para el listado Estado de protección de los equipos

Campo	Descripción	Valores
Estado de protección	Estado del módulo de protección instalado en el equipo.	• Instalando... • Correctamente protegido • Protección con error • Protección desactivada • Sin licencia • Error instalando
Estado de aislamiento	Configuración del aislamiento del equipo.	• No aislado • Aislado • Aislando • Dejando de aislar

Tabla 18.26: campos de filtrado para el listado Estado de protección de los equipos

- **Ventana detalle del equipo**

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta el apartado "**Información de equipo**" en la página **177** para obtener más información.

Listado de Programas actualmente bloqueados en clasificación

Muestra una tabla con aquellos ficheros que, sin haber sido completada su clasificación, Cytomic EPDR ha detectado de forma preliminar algún riesgo en su ejecución. Estos ficheros son bloqueados durante el tiempo empleado en su clasificación.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido.	Cadena de caracteres
Ruta	Nombre del fichero desconocido y ruta en el equipo del usuario.	Cadena de caracteres
Ha accedido a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Binario
Se ha comunicado con equipos externos	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Binario
Modo de protección	Modo en el que se encontraba la protección avanzada en el momento del descubrimiento del fichero desconocido.	• Audit • Hardening • Lock

Tabla 18.27: campos del listado Programas actualmente bloqueados

Campo	Comentario	Valores
Probabilidad de que sea malicioso	Posibilidad de que finalmente el fichero desconocido sea una amenaza.	• Media • Alta • Muy Alta
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido.	Fecha

Tabla 18.27: campos del listado Programas actualmente bloqueados

- **Campos mostrados en fichero exportado**

*En el menú de contexto de Programas actualmente bloqueados en clasificación se muestra un desplegable con dos entradas: Exportar y Exportar listado y detalles. En este apartado se muestra el contenido de Exportar. Para obtener información sobre Exportar listado y detalles consulta el apartado "***Ficheros exportados Excel***" en la página* **464**.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido.	Cadena de caracteres
Amenaza	Nombre del fichero desconocido.	Cadena de caracteres
Ruta	Nombre del fichero desconocido y ruta en el equipo del usuario.	Cadena de caracteres
Modo de protección	Modo en el que se encontraba la protección en el momento del descubrimiento del fichero desconocido.	• Audit • Hardening • Lock
Acceso a datos	El fichero desconocido ha accedido a ficheros que residen en el equipo del usuario.	Binario
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Binario
Probabilidad de que sea malicioso	Posibilidad de que finalmente el fichero desconocido sea una amenaza.	• Media • Alta • Muy Alta
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido.	Fecha
Tiempo de exposición	Tiempo que la amenaza ha permanecido en el parque del cliente sin clasificar.	Fecha
Usuario	Cuenta de usuario bajo la cual el programa se ha ejecutado.	Cadena de caracteres

Tabla 18.28: : campos del fichero exportado Programas actualmente bloqueados

Campo	Comentario	Valores
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Equipo origen de la amenaza	Nombre del equipo si el programa bloqueado venga de un equipo de la red del cliente.	Cadena de caracteres
IP origen de la amenaza	Dirección IP del equipo si el programa bloqueado venga de un equipo de la red del cliente.	Cadena de caracteres
Usuario origen de la amenaza	Usuario registrado en la máquina origen del programa bloqueado.	Cadena de caracteres

Tabla 18.28: : campos del fichero exportado Programas actualmente bloqueados

- **Herramienta de filtrado**

Campo	Comentario	Valores
Fechas	Establece un intervalo de fechas desde el momento actual hacia el pasado.	• Últimas 24 horas • Últimos 7 días • Último mes
Buscar	• **Equipo**: dispositivo donde reside el elemento desconocido. • **Amenaza:** nombre del archivo. • **Hash**: Cadena resumen de identificación del archivo. • **Origen de la amenaza**: permite buscar por el usuario, la IP o el nombre del equipo origen del elemento bloqueado.	Cadena de caracteres
Modos de protección	Modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido.	• Hardering • Lock
Acceso a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Binario
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Binario

Tabla 18.29: campos de filtrado para el listado Programas actualmente bloqueados

- **Ventana de detalle**

Muestra información detallada del programa bloqueado. Consulta el apartado "**Detección del malware y Detalles del programa bloqueado**" en la página **450**.

Listado Historial de programas bloqueados

Muestra un histórico de todos eventos que se han producido a lo largo del tiempo relativos a los procesos bloqueados.

Este listado no tiene su panel correspondiente y es accesible únicamente mediante el botón **Historial** del listado **Programas actualmente bloqueados en clasificación**, situado en la esquina superior derecha.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido.	Cadena de caracteres
Ruta	Nombre del fichero desconocido y ruta en el equipo del usuario.	Cadena de caracteres
Acción	Acción ejecutada por Cytomic EPDR.	• Bloqueado • Reclasificado a GW • Reclasificado a MW • Reclasificado a PUP
Ha accedido a datos 	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Binario
Se ha comunicado con equipos externos	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Binario
Modo de protección	Modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido.	• Audit • Hardening • Lock
Excluido	El fichero desconocido ha sido desbloqueado / excluido por el administrador para permitir su ejecución.	Binario
Probabilidad de que sea malicioso	Posibilidad de que finalmente el fichero desconocido sea malware.	• Media • Alta • Muy Alta
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido.	Fecha

Tabla 18.30: campos del listado Historial de programas bloqueados

- **Campos mostrados en fichero exportado**

*En el menú de contexto de Historial de programas bloqueados se muestra un desplegable con dos entradas diferentes: Exportar y Exportar listado y detalles. En este apartado se muestra el contenido de Exportar. Para obtener información sobre Exportar listado y detalles consulta el apartado "***Ficheros exportados Excel***" en la página* **464**.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido.	Cadena de caracteres
Amenaza	Nombre del fichero desconocido.	Cadena de caracteres
Ruta	Ruta en el equipo del usuario del fichero desconocido.	Cadena de caracteres
Modo de protección	Modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido.	• Audit • Hardening • Lock
Acción	Acción ejecutada por Cytomic EPDR.	• Bloqueado • Reclasificado a GW • Reclasificado a MW • Reclasificado a PUP
Acceso a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Binario
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Binario
Excluido	El fichero desconocido ha sido desbloqueado / excluido por el administrador para permitir su ejecución.	Binario
Probabilidad de que sea malicioso	Posibilidad de que finalmente el fichero desconocido sea malware.	• Media • Alta • Muy Alta
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido.	Fecha
Tiempo de exposición	Tiempo que el fichero desconocido ha permanecido en el parque del cliente sin clasificar.	Fecha
Usuario	Cuenta de usuario bajo la cual el programa se ha ejecutado.	Cadena de caracteres

Tabla 18.31: campos del fichero exportado Historial de programas bloqueados

Campo	Comentario	Valores
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Equipo origen de la amenaza	Equipo origen del programa bloqueado.	Cadena de caracteres
IP origen de la amenaza	IP origen del programa bloqueado.	Cadena de caracteres
Usuario origen de la amenaza	Usuario origen del programa bloqueado.	Cadena de caracteres

Tabla 18.31: campos del fichero exportado Historial de programas bloqueados

- **Herramienta de filtrado**

Campo	Comentario	Valores
Buscar	• **Equipo**: dispositivo donde reside el fichero desconocido. • **Amenaza**: nombre de la amenaza. • **Hash**: cadena resumen de identificación del archivo. • **Origen de la amenaza**: permite buscar por el usuario, la IP o el nombre del equipo origen de la amenaza.	Cadena de caracteres
Fechas	Establece un intervalo de fechas desde el momento actual hacia atrás.	• Últimas 24 horas • Últimos 7 días • Último mes
Acción	Acción desencadenada por Cytomic EPDR.	• Bloqueado • Reclasificado a GW • Reclasificado a MW • Reclasificado a PUP
Excluido	El fichero desconocido ha sido desbloqueado / excluido por el administrador para permitir su ejecución.	Binario
Modos de protección	Modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido.	• Hardening • Lock
Acceso a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Binario
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Binario

Tabla 18.32: campos del fichero exportado Historial de programas bloqueados

- **Ventana de detalle**

Muestra información detallada del programa bloqueado. Consulta el apartado "**Detección del malware y Detalles del programa bloqueado**" en la página **450**.

Listado de Programas permitidos por el administrador

Este listado muestra en detalle todos los elementos en clasificación o clasificados como amenazas que el administrador actualmente está permitiendo su ejecución.

> *Este listado solo es accesible desde el widget Programas permitidos por el administrador.*

Campo	Descripción	Valores
Programa	Nombre del malware o PUP que se permite su ejecución. Si es un elemento desconocido se indica el nombre del fichero en su lugar.	Cadena de caracteres
Clasificación actual	Tipo de amenaza.	• Malware • PUP • Bloqueado • Bloqueado reclasificado a Malware / PUP • Bloqueado reclasificado a Goodware
Amenaza	Nombre de la amenaza.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Permitido por	Usuario de la consola que creó la exclusión.	Cadena de caracteres
Permitido desde	Fecha en la que el administrador creó la exclusión del fichero.	Fecha
Borrar	Retira la exclusión del fichero.	

Tabla 18.33: campos del listado Programas permitidos por el administrador

- **Campos incluidos en fichero exportado**

Campo	Descripción	Valores
Programa	Nombre y ruta del fichero desconocido o que contiene la amenaza.	Cadena de caracteres

Tabla 18.34: campos del fichero exportado Programas permitidos por el administrador

Campo	Descripción	Valores
Tipo actual	Tipo del fichero en el momento en el que se accede al listado.	• Malware • PUP • Bloqueado • Bloqueado reclasificado a Malware / PUP • Bloqueado reclasificado a Goodware
Tipo original	Tipo del fichero en el momento en el que se comenzó a permitir su bloqueo.	• Malware • PUP • Bloqueado • Bloqueado reclasificado a Malware / PUP • Bloqueado reclasificado a Goodware
Amenaza	Nombre del malware o PUP que se permite su ejecución. Si es un elemento desconocido se indica el nombre del fichero en su lugar.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Permitido por	Usuario de la consola que creó la exclusión.	Cadena de caracteres
Permitido desde	Fecha en la que el administrador creó la exclusión del fichero.	Fecha

Tabla 18.34: campos del fichero exportado Programas permitidos por el administrador

- **Herramienta de filtrado**

Campo	Comentario	Valores
Buscar	• **Amenaza**: nombre del malware o PUP. • **Permitido por**: usuario de la consola que creó la exclusión. • **Programa**: nombre del fichero que contiene la amenaza. • **Hash**: cadena resumen de identificación del archivo.	Cadena de caracteres

Campo	Comentario	Valores
Clasificación actual	Tipo del fichero en el momento en el que se accede al listado.	• Malware • PUP • Goodware • En clasificación (Bloqueados y sospechoso)
Clasificación original	Tipo del fichero en el momento en el que se comenzó a permitir su bloqueo.	• Malware • PUP • Bloqueado • Sospechoso

Tabla 18.35: campos de filtrado para el listado Programas permitidos por el administrador

Listado Historial de Programas permitidos por el administrador

Muestra un histórico de todos eventos que se han producido a lo largo del tiempo relativos a las amenazas y ficheros desconocidos en clasificación que el administrador permitió su ejecución.

Este listado no tiene su panel correspondiente y es accesible únicamente mediante el botón **Historial** del listado **Programas permitidos por el administrador**, situado en la esquina superior derecha.

Campo	Descripción	Valores
Programa	Nombre y ruta del fichero desconocido o que contiene la amenaza.	Cadena de caracteres
Clasificación actual	Tipo de la amenaza que se permitió su ejecución.	• Malware • PUP • Bloqueado • Sospechoso
Amenaza	Nombre del malware o PUP que se permite su ejecución. Si es un elemento desconocido se indica el nombre del fichero en su lugar.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Acción	Acción aplicada sobre el elemento permitido.	• Exclusión eliminada por el usuario • Exclusión eliminada por reclasificación • Exclusión añadida por el usuario • Exclusión mantenida por reclasificación

Tabla 18.36: campos del listado Historial de Programas permitidos por el administrador

Campo	Descripción	Valores
Usuario	Cuenta de usuario de la consola que inicio el cambio en el fichero permitido.	Cadena de caracteres
Fecha	Fecha en la que se produjo el evento.	Fecha

Tabla 18.36: campos del listado Historial de Programas permitidos por el administrador

- **Campos incluidos en fichero exportado**

Campo	Descripción	Valores
Programa	Nombre del fichero desconocido o que contiene la amenaza.	Cadena de caracteres
Tipo actual	Último tipo de la amenaza que se permitió su ejecución.	• Malware • PUP • Bloqueado • Sospechoso
Tipo original	Tipo del fichero cuando se produjo el evento.	• Malware • PUP • Bloqueado • Sospechoso
Amenaza	Nombre del malware o PUP que se permite su ejecución. Si es un elemento desconocido se indica el nombre del fichero en su lugar.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Acción	Acción aplicada sobre el elemento permitido.	• Exclusión eliminada por el usuario. • Exclusión eliminada por reclasificación. • Exclusión añadida por el usuario. • Exclusión mantenida por reclasificación.
Usuario	Cuenta de usuario de la consola que inicio el cambio en el fichero permitido.	Cadena de caracteres
Fecha	Fecha en la que se produjo el evento.	Fecha

Tabla 18.37: campos del fichero exportado Historial de Programas permitidos por el administrador

- **Herramienta de filtrado**

Campo	Descripción	Valores
Buscar	• **Usuario**: cuenta de usuario de la consola que inicio el cambio en el fichero permitido. • **Programa**: nombre del fichero que contiene la amenaza. • **Hash**: cadena resumen de identificación del archivo.	Cadena de caracteres
Clasificación actual	Tipo del fichero en el momento en el que se accede al listado.	• Malware • PUP • Goodware • En clasificación (Bloqueados y sospechoso)
Clasificación original	Tipo del fichero en el momento en el que se comenzó a permitir su bloqueo.	• Malware • PUP • En clasificación (Bloqueado) • En clasificación (Sospechoso)
Acción	Acción aplicada sobre el elemento permitido.	• Exclusión eliminada por el usuario • Exclusión eliminada por reclasificación • Exclusión añadida por el usuario • Exclusión añadida por reclasificación

Tabla 18.38: campos de filtrado para el listado Historial de Programas permitidos por el administrador

Listado de Actividad de malware / PUP

Muestra el listado de las amenazas encontradas en los equipos protegidos con Cytomic EPDR. Este detalle es necesario para poder localizar el origen de los problemas, determinar la gravedad de las incidencias y, si procede, tomar las medidas necesarias de resolución y de actualización de la política de seguridad de la compañía.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres

Tabla 18.39: campos del listado de Actividad del malware / PUP

Campo	Comentario	Valores
Amenaza	Nombre de la amenaza detectada.	Cadena de caracteres
Ruta	Ruta completa donde reside el fichero infectado.	Cadena de caracteres
Ejecutado alguna vez	La amenaza se llegó a ejecutar y el equipo puede estar comprometido.	Binario
Ha accedido a datos	La amenaza ha accedido a datos que residen en el equipo del usuario.	Binario
Se ha comunicado con equipos externos	La amenaza se comunica con equipos remotos para enviar o recibir datos.	Binario
Acción	Acción aplicada sobre el malware.	• Movido a cuarentena • Bloqueado • Desinfectado • Eliminado • Detectado
Fecha	Fecha de la detección de la amenaza en el equipo.	Fecha

Tabla 18.39: campos del listado de Actividad del malware / PUP

- **Campos mostrados en fichero exportado**

*En el menú de contexto de Listado de actividad Malware / PUP se muestra un desplegable con dos entradas diferentes: Exportar y Exportar listado y detalles. En este apartado se muestra el contenido de Exportar. Para obtener información sobre Exportar listado y detalles consulta el apartado "***Ficheros exportados Excel***" en la página* **464**

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres
Amenaza	Nombre de la amenaza detectada.	Cadena de caracteres
Ruta	Ruta completa donde reside el fichero infectado.	Cadena de caracteres
Acción	Acción aplicada sobre el malware.	• Movido a cuarentena • Bloqueado • Desinfectado • Eliminado • Permitido
Ejecutado	La amenaza se llegó a ejecutar y el equipo puede estar comprometido.	Binario
Acceso a datos	La amenaza ha accedido a datos que residen en el equipo del usuario.	Binario

Campo	Comentario	Valores
Conexiones externas	La amenaza se comunica con equipos remotos para enviar o recibir datos.	Binario
Excluido	La amenaza ha sido excluida por el administrador para permitir su ejecución.	Binario
Fecha	Fecha de la detección de la amenaza en el equipo.	Fecha
Tiempo de exposición	Tiempo que la amenaza ha permanecido en el parque del cliente sin clasificar.	Cadena de caracteres
Usuario	Cuenta de usuario bajo la cual la amenaza se ha ejecutado.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Equipo origen de la infección	Nombre del equipo si el intento de infección viene de un equipo de la red del cliente.	Cadena de caracteres
IP origen de la infección	Dirección IP del equipo si el intento de infección viene de un equipo de la red del cliente.	Cadena de caracteres
Usuario origen de la infección	Usuario registrado en la máquina origen de la infección.	Cadena de caracteres

Tabla 18.40: campos del fichero exportado Actividad del malware / PUP

- **Herramienta de filtrado**

Campo	Comentario	Valores
Buscar	• **Equipo**: dispositivo donde se realizó la detección. • **Amenaza**: nombre de la amenaza. • **Hash**: Cadena resumen de identificación del archivo. • **Origen de la infección**: busca por el usuario, la IP o el nombre del equipo origen del fichero infectado.	Cadena de caracteres
Tipo	Tipo de amenaza a mostrar.	• Malware • PUP
Fechas	Establece un intervalo de fechas desde el día presente hacia el pasado.	• Últimas 24 horas • Últimos 7 días • Último mes • Último año
Ejecutado	La amenaza se llegó a ejecutar y el equipo puede estar comprometido.	Binario

Tabla 18.41: campos de filtrado para el listado Actividad del malware / PUP

Campo	Comentario	Valores
Acción	Acción aplicada sobre la amenaza.	• Movido a cuarentena • Bloqueado • Desinfectado • Eliminado • Permitido
Acceso a datos	La amenaza ha accedido a datos que residen en el equipo del usuario.	Binario
Conexiones externas	La amenaza se comunica con equipos remotos para enviar o recibir datos.	Binario

Tabla 18.41: campos de filtrado para el listado Actividad del malware / PUP

- **Ventana de detalle**

Muestra información detallada del programa clasificado como malware / PUP. Consulta el apartado "**Detección del malware y Detalles del programa bloqueado**" en la página **450**.

Listado de Actividad de exploits

Muestra el listado de equipos con programas comprometidos por intentos de explotación de vulnerabilidades. Este detalle es necesario para poder localizar el origen los problemas, determinar la gravedad de las incidencias y, si procede, tomar las medidas necesarias de resolución y de actualización de la política de seguridad de la compañía.

Cytomic EPDR ejecuta una acción por cada exploit detectado:

- **Permitido**: la protección anti-exploit está configurada en modo "Auditar". El exploit se ejecutó.
- **Bloqueado**: el exploit fue bloqueado antes de su ejecución.
- **Permitido por el usuario**: se preguntó al usuario del equipo si finalizar el proceso comprometido y el usuario decidió permitir que el exploit continuara ejecutándose.
- **Proceso finalizado**: el exploit fue eliminado, pero se llegó a ejecutar parcialmente.
- **Pendiente de reinicio**: se informó al usuario de la necesidad de reiniciar el equipo para eliminar completamente el exploit. Mientras tanto éste se seguirá ejecutando.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres
Programa comprometido	Programa que recibió el ataque de tipo exploit.	Cadena de caracteres

Tabla 18.42: campos del listado de Actividad de exploits

Campo	Comentario	Valores
Acción	Acción aplicada sobre el exploit.	• Permitido por el usuario. • Permitido. • Bloqueado. • Proceso finalizado. • Pendiente de reinicio.
Exploit ejecutado	El exploit se llegó a ejecutar o fue bloqueado antes de afectar al programa vulnerable.	Binario
Fecha	Fecha de la detección del intento de exploit en el equipo.	Fecha

Tabla 18.42: campos del listado de Actividad de exploits

- **Campos mostrados en fichero exportado**

*En el menú de contexto de Actividad de exploits se muestra un desplegable con dos entradas diferentes: Exportar y Exportar listado y detalles. En este apartado se muestra el contenido de Exportar. Para obtener información sobre Exportar listado y detalles consulta el apartado "***Ficheros exportados Excel***" en la página* **464**

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres
Programa comprometido	Programa que recibió el ataque de tipo exploit.	Cadena de caracteres
Usuario	Cuenta de usuario bajo la cual se ejecutaba el programa que recibió el exploit.	Cadena de caracteres
Hash	Cadena resumen de identificación del programa comprometido.	Cadena de caracteres
Last action	Acción aplicada sobre el exploit.	• Permitido por el usuario • Permitido por el administrador • Bloqueo inmediato • Bloqueo tras finalizar proceso
Riesgo	El equipo está o ha estado en situación riesgo o el exploit se pudo bloquear antes de afectar al programa vulnerable.	Binario
Fecha	Fecha de la detección del intento de exploit en el equipo.	Fecha

Tabla 18.43: campos del fichero exportado Actividad del malware / PUP

- **Herramienta de búsqueda**

Campo	Comentario	Valores
Buscar	• **Equipo**: dispositivo donde se realizó la detección. • **Hash**: Cadena resumen de identificación del programa comprometido. • **Programa comprometido**: nombre del fichero comprometido o de su ruta.	Cadena de caracteres
Fechas	Intervalo de fechas desde el día presente hacia el pasado.	• Últimas 24 horas • Últimos 7 días • Último mes
Exploit ejecutado	El exploit se llegó a ejecutar o fue bloqueado antes de afectar al programa vulnerable.	Binario
Acción	Acción aplicada sobre el exploit.	• Permitido por el usuario • Permitido • Bloqueado • Proceso finalizado • Pendiente de reinicio

Tabla 18.44: campos de filtrado para el listado Actividad de exploits

- **Ventana de detalle**

Muestra información detallada del programa clasificado como exploit. Consulta el apartado "**Detección exploit**" en la página **453**.

Listado de Amenazas detectadas por el antivirus

El listado de detecciones ofrece información consolidada y completa de todas las detecciones realizadas en todas las plataformas soportadas y desde todos los vectores de infección analizados, utilizados por los hackers para intentar infectar equipos en la red.

Campo	Descripción	Valores
Equipo	Nombre del equipo donde se realizó la detección.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres

Tabla 18.45: campos del listado Amenazas detectadas por el antivirus

Campo	Descripción	Valores
Grupo	Grupo dentro del árbol de grupos de Cytomic EPDR a la que pertenece el equipo.	• Cadena de caracteres • Grupo Todos • Grupo nativo • Grupo Directorio activo
Tipo de amenaza	Clase de la amenaza detectada.	• Virus • Spyware • Herramientas de hacking y PUPs • Phising • Sospechosos • Acciones peligrosas bloqueadas • Tracking cookies • URLs con malware • Otros.
Ruta	Ruta del sistema de ficheros donde reside la amenaza.	Cadena de caracteres
Acción	Acción desencadenada por Cytomic EPDR.	• Borrado • Desinfectado • En cuarentena • Bloqueado • Proceso terminado
Fecha	Fecha de la detección.	Fecha

Tabla 18.45: campos del listado Amenazas detectadas por el antivirus

- **Campos mostrados en fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo donde se realizó la detección.	Cadena de caracteres
Nombre malware	Nombre de la amenaza detectada.	Cadena de caracteres

Tabla 18.46: campos del fichero exportado Amenazas detectadas por el antivirus

Campo	Descripción	Valores
Tipo de amenaza	Clase de la amenaza detectada.	• Virus • Spyware • Herramientas de hacking y PUPs • Phising • Sospechosos • Acciones peligrosas bloqueadas • Tracking cookies • URLs con malware • Otros
Tipo de malware	Subclase de la amenaza detectada.	Cadena de caracteres
Número de detecciones	Número de veces que Cytomic EPDR detectó la amenaza en el equipo y en la fecha indicada.	Numérico
Acción	Acción desencadenada por Cytomic EPDR.	• Movido a cuarentena • Borrado • Bloqueado • Proceso terminado
Detectado por	Motor que detectó la amenaza.	• Control de dispositivos • Protección de Antispam para Exchange • Protección de Contenido para Exchange • Protección de Buzones para Exchange • Protección de Transporte para Exchange • Protección de ficheros • Firewall • Protección de correo • Protección avanzada • Análisis bajo demanda • Control de acceso Web • Protección Web
Ruta de detección	Ruta del sistema de ficheros donde reside la amenaza.	Cadena de caracteres
Excluido	La amenaza ha sido excluida del análisis por el administrador para permitir su ejecución.	Binario
Fecha	Fecha de la detección.	Fecha

Tabla 18.46: campos del fichero exportado Amenazas detectadas por el antivirus

Campo	Descripción	Valores
Grupo	Grupo dentro del árbol de grupos de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo donde se realizó la detección.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador de la red.	Cadena de caracteres

Tabla 18.46: campos del fichero exportado Amenazas detectadas por el antivirus

- **Herramienta de filtrado**

Campo	Descripción	Valores
Equipo	Nombre del equipo donde se realizó la detección.	Cadena de caracteres
Fechas	• **Rango**: establece un intervalo de fechas desde el día presente hacia el pasado. • **Rango personalizado**: establece una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes • Último año
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Tipo de Amenazas	Clase de amenaza.	• Virus • Spyware • Herramientas de hacking y PUPs • Phising • Sospechosos • Acciones peligrosas bloqueadas • Tracking cookies • URLs con malware • Otros

Tabla 18.47: campos de filtrado para el listado Amenazas detectadas por el antivirus

- **Ventana de detalle**

Muestra información detallada del virus detectado.

Campo	Descripción	Valores
Amenaza	Nombre de la amenaza.	Cadena de caracteres
Acción	Acción que ejecutó Cytomic EPDR.	• Movido a cuarentena • Borrado • Bloqueado • Proceso terminado
Equipo	Nombre del equipo donde se realizó la detección. Incluye un enlace a la ventana Detalles del equipo	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.	Cadena de caracteres
Ruta de detección	Ruta del sistema de ficheros donde reside la amenaza.	Cadena de caracteres
Nombre	Nombre de la amenaza.	Cadena de caracteres
Tipo de amenaza	Clase de la amenaza.	Cadena de caracteres
Tipo de malware	Clase de malware.	• Virus • Spyware • Herramientas de hacking y PUPs • Phishing • Sospechosos • Acciones peligrosas bloqueadas • Tracking cookies • URLs con malware • Otros.
Detectado por	Módulo que realizó la detección.	
Fecha	Fecha de la detección.	Fecha

Tabla 18.48: detalle del listado de Amenazas detectadas por el antivirus

Listado de Dispositivos bloqueados

Este listado muestra en detalle todos los equipos de la red que tienen limitado el acceso a alguno de los periféricos conectados.

Campo	Descripción	Valores
Equipo	Nombre del equipo desprotegido.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	• Cadena de caracteres • Grupo Todos • Grupo nativo • Grupo Directorio activo
Tipo	Familia del dispositivo afectado por la configuración de seguridad.	• Unidades de almacenamiento extraíbles • Dispositivos de captura de imágenes • Unidades de CD/DVD • Dispositivos Bluetooth • Módems • Dispositivos móviles
Acción	Tipo de acción efectuada sobre el dispositivo.	• Bloquear • Permitir Lectura • Permitir Lectura y escritura
Fecha	Fecha en la se aplicó la acción.	Fecha

Tabla 18.49: campos del listado Dispositivos bloqueados

- **Campos mostrados en fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Nombre	Nombre del periférico conectado al equipo y afectado por la configuración de seguridad.	Cadena de caracteres

Tabla 18.50: campos del fichero exportado Dispositivos bloqueados

Campo	Descripción	Valores
Tipo	Clase de dispositivo.	• Unidades de almacenamiento extraíbles • Dispositivos de captura de imágenes • Unidades de CD/DVD • Dispositivos Bluetooth • Módems • Dispositivos móviles
Id. de instancia	Identificador del dispositivo afectado.	Cadena de caracteres
Número de detecciones	Número de veces que se detectó una operación no permitida sobre el dispositivo.	Numérico
Acción	Tipo de acción efectuada sobre el dispositivo.	• Bloquear • Permitir Lectura • Permitir Lectura y escritura
Detectado por	Módulo que detectó la operación no permitida.	Control de dispositivos
Fecha	Fecha en la se detectó la operación no permitida.	Fecha
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres

Tabla 18.50: campos del fichero exportado Dispositivos bloqueados

- **Herramienta de filtrado**

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Buscar equipo	Nombre del equipo.	Cadena de caracteres

Tabla 18.51: campos de filtrado para el listado Dispositivos bloqueados

Campo	Descripción	Valores
Fechas	• **Rango**: establece un intervalo de fechas desde el día presente hacia el pasado. • **Rango personalizado**: establece una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes
Tipo de dispositivo	Familia del dispositivo afectado por la configuración de seguridad.	• Unidades de almacenamiento extraíbles • Dispositivos de captura de imágenes • Unidades de CD/DVD • Dispositivos Bluetooth • Módems • Dispositivos móviles

Tabla 18.51: campos de filtrado para el listado Dispositivos bloqueados

- **Ventana de detalle**

Muestra información detallada del dispositivo bloqueado.

Campo	Descripción	Valores
Dispositivo	Nombre del dispositivo bloqueado.	Cadena de caracteres
Acción	Acción que ejecutó Cytomic EPDR.	• Movido a cuarentena • Borrado • Bloqueado • Proceso terminado
Equipo	Nombre del equipo donde se realizó el bloqueo del dispositivo.	Cadena de caracteres
Tipo de equipo	Clase del equipo.	• Estación • Portátil • Dispositivo móvil • Servidor
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Nombre	Nombre del dispositivo bloqueado.	Cadena de caracteres
Tipo de dispositivo	Categoría del dispositivo.	• Unidades de almacenamiento extraíbles • Dispositivos de captura de imágenes

Tabla 18.52: detalle del listado Dispositivos bloqueados

Campo	Descripción	Valores
		• Unidades de CD/DVD • Dispositivos Bluetooth • Módems • Dispositivos móviles
Id. de instancia	Identificador del dispositivo afectado.	Cadena de caracteres
Bloqueado por	Módulo que realizó la detección.	Control de dispositivos
Número de detecciones	Número de bloqueos detectados.	Numérico
Fecha	Fecha de la detección.	Fecha

Tabla 18.52: detalle del listado Dispositivos bloqueados

Listado de Conexiones bloqueadas

Muestra las conexiones bloqueadas por el módulo del cortafuegos del equipo. Para activar el listado de conexiones bloqueadas consulta el apartado "**Informar de todos los bloqueos del firewall**" en la página **242**.

Los bloqueos presentados en este listado se agrupan durante 1 hora siguiendo los criterios mostrados a continuación:

- Equipo
- Aplicación bloqueada
- Sentido
- Regla
- Fecha de bloqueo

Si en el intervalo de una hora se producen varios bloqueos de conexiones iniciadas o recibidas por una misma aplicación, con un mismo sentido, y que además han sido bloqueados por una misma regla, se agruparán en una única entrada del listado.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	• Cadena de caracteres • Grupo Todos • Grupo nativo • Grupo Directorio activo

Tabla 18.53: campos del listado Conexiones bloqueadas

Campo	Descripción	Valores
Aplicación	Ruta y nombre completo del programa que envía o recibe datos pertenecientes al tráfico de red bloqueado.	Cadena de caracteres
Sentido	Sentido de la conexión bloqueada.	• Entrantes • Salientes
Regla	Regla que provocó el bloqueo de tráfico y breve descripción de su definición.	Cadena de caracteres
Número de conexiones bloqueadas	Número de bloqueos agrupados en el intervalo de una hora.	Numérico
Fecha	Fecha en la se bloqueó el tráfico de red.	Fecha

Tabla 18.53: campos del listado Conexiones bloqueadas

- **Campos mostrados en fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Aplicación	Ruta y nombre completo del programa que envía o recibe tráfico de red bloqueado.	Cadena de caracteres
Sentido	Sentido de la conexión bloqueada.	• Entrantes • Salientes
Regla	Regla que provocó el bloqueo de tráfico y breve descripción de su definición.	Cadena de caracteres
Número de bloqueos	Número de bloqueos producidos por la regla en el intervalo de una hora.	Numérico
Fecha	Fecha en la se bloqueó el tráfico de red.	Fecha
Grupo	Carpeta dentro del árbol de grupos de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres

Tabla 18.54: campos del fichero exportado Conexiones bloqueadas

Campo	Descripción	Valores
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres

Tabla 18.54: campos del fichero exportado Conexiones bloqueadas

- **Herramienta de filtrado**

Campo	Descripción	Valores
Búsqueda	Filtra los resultados del listado por el nombre del Equipo, la aplicación o la regla que provocó el bloqueo de tráfico de red.	**Cadena de texto**
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Fechas	• **Rango**: establece un intervalo de fechas desde el día presente hacia el pasado. • **Rango personalizado**: establece una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes

Tabla 18.55: campos de filtrado para el listado Conexiones bloqueadas

- **Ventana de detalle**

Muestra información detallada de la conexión bloqueada:.

Campo	Descripción	Valores
Regla	Regla que bloqueó el tráfico. Si la regla no ha sido eliminada de la configuración incluirá un enlace que lleva a su definición.	Cadena de caracteres
Equipo	Nombre del equipo donde se bloqueó el tráfico de red. Incluye un enlace a la ventana Detalles del equipo.	Cadena de caracteres
Tipo de equipo	Clase del equipo.	• Estación • Portátil • Servidor
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Aplicación	Ruta y nombre completo del programa que envía o recibe tráfico de red bloqueado.	Cadena de caracteres
Sentido	Dirección de la conexión.	• Entrantes • Salientes
Número de conexiones bloqueadas	Número de bloqueos producidos por la regla en el intervalo de una hora.	Numérico

Tabla 18.56: detalle del listado Conexiones bloqueadas

Campo	Descripción	Valores
Fecha	Fecha en la se bloqueó el tráfico de red.	Fecha

Tabla 18.56: detalle del listado Conexiones bloqueadas

Listado de Intentos de intrusión bloqueados

Este listado muestra los ataques de red recibidos por los equipos y bloqueados por el módulo de cortafuegos.

Campo	Descripción	Valores
Equipo	Nombre del equipo que recibió el ataque de red.	Cadena de caracteres
Dirección IP	Dirección IP del interface red principal del equipo que recibió el ataque de red.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Tipo de intrusión	Indica el tipo de intrusión detectado. Consulta el apartado "**Bloquear intrusiones**" en la página **240** para obtener más información acerca de cada uno de los ataques enumerados.	• Todos los intentos de intrusión • ICMP attack • UDP port scan • Header lengths • UDP flood • TCP flags check • Smart WINS • IP explicit pathLand attack • Smart DNS • ICMP filter echo request • OS detection • Smart DHCP • SYN flood • Smart ARP • TCP port scan
Fecha	Fecha y hora en la que Cytomic EPDR registró el ataque en el equipo.	Fecha

Tabla 18.57: campos del listado Intentos de intrusión bloqueados

- **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres

Tabla 18.58: campos del fichero exportado Intentos de intrusión bloqueados

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	Cadena de caracteres
Equipo	Nombre del equipo que recibió el ataque de red.	Cadena de caracteres
Tipo de intrusión	Indica el tipo de intrusión detectado. Consulta el apartado "**Bloquear intrusiones**" en la página **240** para obtener más información acerca de cada uno de los ataques enumerados.	• ICMP attack • UDP port scan • Header lengths • UDP flood • TCP flags check • Smart WINS • IP explicit path • Land attack • Smart DNS • ICM filter echo request • OS detection • Smart DHCP • SYN flood • Smart ARP • TCP port scan
Dirección IP local	Dirección IP del equipo que recibió el ataque de red.	Cadena de caracteres
Dirección IP remota	Dirección IP del equipo que inició el ataque de red.	Cadena de caracteres
MAC remota	Dirección física del equipo que inició el ataque de red, siempre que se encuentre en el mismo segmento de red que el equipo que recibió el ataque.	Cadena de caracteres
Puerto Local	Si el ataque es TCP o UDP indica el puerto donde se recibió el intento de intrusión.	Numérico
Puerto remoto	Si el ataque es TCP o UDP indica el puerto desde donde se envió el intento de intrusión.	Numérico
Número de detecciones	Número de intentos de intrusión del mismo tipo recibidos.	Numérico
Acción	Acción ejecutada por el cortafuegos según su configuración. Consulta el apartado "**Firewall (Equipos Windows)**" en la página **234**.	Bloquear
Detectado por	Motor de detección que realizó la detección del ataque de red.	Firewall
Fecha	Fecha en la que se registró el ataque de red.	Fecha
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres

Tabla 18.58: campos del fichero exportado Intentos de intrusión bloqueados

Campo	Descripción	Valores
Dirección IP	Dirección IP del interface red principal del equipo que recibió el ataque de red.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres

Tabla 18.58: campos del fichero exportado Intentos de intrusión bloqueados

- **Herramienta de filtrado**

Campo	Descripción	Valores
Fechas	• **Rango**: establece un intervalo de fechas desde el día presente hacia el pasado. • **Rango personalizado**: establece una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes
Tipo de intrusión	Indica el tipo de intrusión detectado. Consulta el apartado "**Bloquear intrusiones**" en la página **240** para obtener más información acerca de cada uno de los ataques enumerados.	• Todos los intentos de intrusión • ICMP attack • UDP port scan • Header lengths • UDP flood • TCP flags check • Smart WINS • IP explicit pathLand attack • Smart DNS • ICMP filter echo request • OS detection • Smart DHCP • SYN flood • Smart ARP • TCP port scan
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor

Tabla 18.59: campos de filtrado para el listado Intentos de intrusión bloqueados

- **Ventana de detalle**

Muestra información detallada del ataque de red detectado.

Campo	Descripción	Valores
Tipo de intrusión	Indica el tipo de intrusión detectado. Consulta el apartado "**Bloquear intrusiones**" en la página **240** para obtener más información acerca de cada uno de los ataques enumerados.	• ICMP attack • UDP port scan • Header lengths • UDP flood • TCP flags check • Smart WINS • IP explicit path • Land attack • Smart DNS • ICM filter echo request • OS detection • Smart DHCP • SYN flood • Smart ARP • TCP port scan
Acción	Acción que ejecutó Cytomic EPDR.	Bloqueado
Equipo	Nombre del equipo donde se realizó la detección.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dirección IP local	Dirección IP del equipo que recibió el ataque de red.	Cadena de caracteres
Dirección IP remota	Dirección IP del equipo que inició el ataque de red.	Cadena de caracteres
MAC remota	Dirección física del equipo que inició el ataque de red, siempre que se encuentre en el mismo segmento de red que el equipo que recibió el ataque.	Cadena de caracteres
Puerto local	Si el ataque es TCP o UDP indica el puerto donde se recibió el intento de intrusión.	Numérico
Puerto remoto	Si el ataque es TCP o UDP indica el puerto desde donde se envió el intento de intrusión.	Numérico
Detectado por	Módulo que realizó la detección.	Firewall

Tabla 18.60: detalle del listado de Intentos de intrusión bloqueados

Campo	Descripción	Valores
Número de detecciones	Número de veces que se repitió de forma sucesiva el mismo tipo de ataque entre los mismos equipos origen y destino.	Numérico
Fecha	Fecha de la detección.	Fecha

Tabla 18.60: detalle del listado de Intentos de intrusión bloqueados

Listado de Accesos a páginas web por categoría

Campo	Descripción	Valores
Categoría	Categoría a la que pertenece la página accedida.	Enumeración de las categorías soportadas.
Accesos permitidos	Número de accesos que se han permitido a la categoría de página indicada en el campo Categoría.	Numérico
Dispositivos permitidos	Número de equipos que han podido acceder a páginas pertenecientes a la categoría de página indicada en el campo Categoría.	Numérico
Accesos denegados	Número de accesos que se han denegado a la categoría de página indicada en el campo Categoría.	Numérico
Equipos denegados	Número de equipos que no han podido acceder a páginas pertenecientes a la categoría de página indicada en el campo Categoría.	Numérico

Tabla 18.61: campos del listado Accesos a páginas web por categoría

- **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Categoría	Categoría a la que pertenece la página accedida.	Enumeración de las categorías soportadas.
Accesos permitidos	Número de accesos que se han permitido a la categoría de página indicada en el campo Categoría.	Numérico
Dispositivos permitidos	Número de equipos que han podido acceder a páginas pertenecientes a la categoría de página indicada en el campo Categoría.	Numérico
Accesos denegados	Número de accesos que se han denegado a la categoría de página indicada en el campo Categoría.	Numérico
Equipos denegados	Número de equipos que no han podido acceder a páginas pertenecientes a la categoría de página indicada en el campo Categoría.	Numérico

Tabla 18.62: campos del fichero exportado Accesos a páginas web por equipo

- **Herramienta de filtrado**

Campo	Descripción	Valores
Fechas	• **Rango**: permite establecer un intervalo de fechas desde el día presente hacia el pasado. • **Fecha personalizada**: permite establecer una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes • Último año
Categoría	Categoría a la que pertenece la página accedida.	Enumeración de las categorías soportadas.

Tabla 18.63: campos de filtrado para el listado Accesos a páginas web por equipo

Listado de Accesos a páginas web por equipo

El acceso a páginas web por equipo lista todos los equipos encontrados en la red indicando el número de accesos permitidos y denegados por cada categoría accedida.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Grupo	Grupo dentro del árbol de grupos de Cytomic EPDR a la que pertenece el equipo.	• Cadena de caracteres • Grupo Todos • Grupo nativo • Grupo Directorio activo
Categoría	Categoría a la que pertenece la página accedida.	Enumeración de las categorías soportadas.
Accesos permitidos	Número de accesos que se han permitido a la categoría de página indicada en el campo Categoría.	Numérico
Accesos denegados	Numero de accesos que se han denegado a la categoría de página indicada en el campo Categoría.	Numérico

Tabla 18.64: campos del listado Accesos a páginas web por equipo

- **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres

Tabla 18.65: campos del fichero exportado Accesos a páginas web por equipo

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Categoría	Categoría a la que pertenece la página accedida.	Enumeración de las categorías soportadas
Accesos permitidos	Número de accesos que se han permitido a la categoría de página indicada en el campo Categoría.	Numérico
Accesos denegados	Numero de accesos que se han denegado a la categoría de página indicada en el campo Categoría.	Numérico
Grupo	Grupo dentro del árbol de grupos de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres

Tabla 18.65: campos del fichero exportado Accesos a páginas web por equipo

- **Herramienta de búsqueda**

Campo	Descripción	Valores
Fechas	• **Rango**: establece un intervalo de fechas desde el día presente hacia atrás. • **Rango personalizado**: establece una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes
Categoría	Categoría a la que pertenece la página accedida.	Enumeración de las categorías soportadas.
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres

Tabla 18.66: campos de filtrado para el listado Accesos a páginas web por equipo

Capítulo 19

Gestión de amenazas, elementos en clasificación y cuarentena

Cytomic EPDR es capaz de equilibrar la eficacia entre el servicio de seguridad que ofrece y el impacto sobre la actividad diaria que percibirán los usuarios protegidos. Este equilibro se consigue a través de varias herramientas configurables por el administrador.

CONTENIDO DEL CAPÍTULO

Introducción a las herramientas de gestión de amenazas

El administrador cuenta con varias **herramientas** para gestionar la amenazas encontradas y los ficheros desconocidos en proceso de clasificación:

- Gestión del bloqueo de los procesos desconocidos.
- Gestión de la ejecución de los procesos clasificados como malware.
- Gestión de la cuarentena.

Gestión del bloqueo de los procesos desconocidos

Para reforzar la protección de los equipos de la red, Cytomic EPDR incorpora el modo **Hardening** y **Lock** en su perfil de configuración avanzada de Windows, para impedir la ejecución de procesos desconocidos.

*Para obtener más información sobre los modos de protección avanzados consulta el apartado "**Protección permanente avanzada**" en la página **35**.*

Las tecnologías Machine Learning que se ejecutan en las plataformas Big Data de Cytomic analizan los procesos desconocidos y los clasifican de forma automática dentro de las primeras 24 horas desde que son vistos por primera vez. La clasificación de un proceso desconocido produce una categoría no ambigua (goodware o malware) compartida para todos los clientes de Cytomic, de forma que puedan beneficiarse del conocimiento acumulado hasta la fecha.

Durante el tiempo de clasificación, Cytomic EPDR bloquea la ejecución de los procesos en estudio para evitar potenciales situaciones de peligro. En la mayor parte de los casos la clasificación se produce de forma automática y en tiempo real. Si el análisis automatizado no es capaz de clasificar el proceso desconocido con el 99'999% de certeza que se le exige, será necesaria la intervención de un experto en análisis de malware que estudie de forma manual la muestra.

En los casos donde la clasificación tardará algún tiempo, el administrador puede considerar necesario asumir ciertos riesgos y permitir la ejecución del fichero sin esperas.

Gestión de la ejecución de los procesos clasificados como malware

El administrador puede permitir la ejecución de ciertos tipos de malware que, a pesar de estar considerados como amenazas, implementan algunas funcionalidades valoradas por los usuarios. Este es el caso por ejemplo de PUPs, programas generalmente en forma de barras de navegador, que ofrecen capacidades de búsquedas al tiempo que recolectan información privada del usuario o confidencial de la empresa con objetivos publicitarios.

Gestión de la cuarentena

El administrador tiene acceso a los elementos considerados como amenazas y, por lo tanto, eliminados de los equipos de los usuarios.

Acceso a los recursos para gestionar amenazas

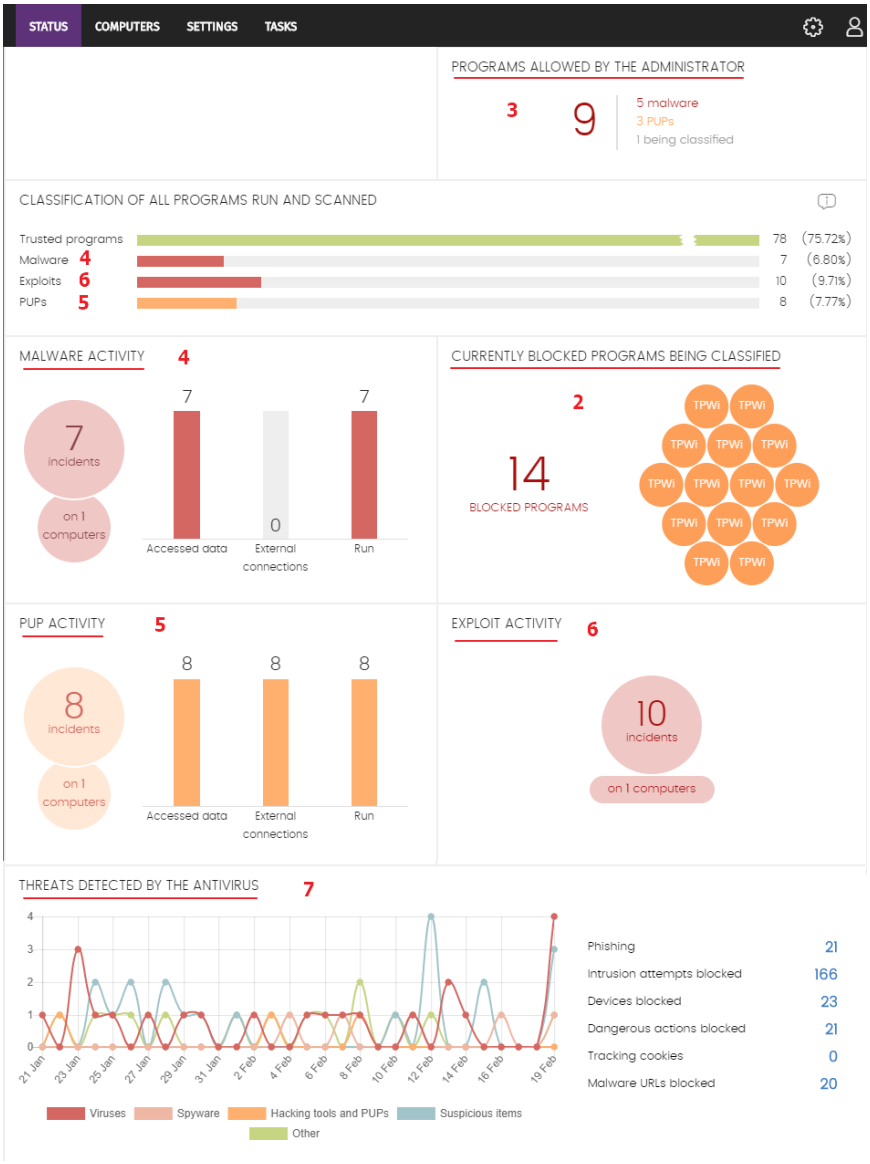


Figura 19.1: acceso a las herramientas de gestión de bloqueados y exclusiones desde el panel de control

Los elementos bloqueados y excluidos se gestionan desde la zona **Estado** de la consola de administración. A continuación, se muestra una guía de referencia rápida que permite localizar cada uno de los recursos.

Todos los recursos mostrados son accesibles desde el Menú superior **Estado (1).** Haz clic en los widgets apropiados del panel de control mostrado en la figura 19.1.

Mostrar los elementos bloqueados por Cytomic EPDR

- **Para listar los elementos actualmente bloqueados por estar clasificados como malware:** panel Actividad de malware y Panel Clasificación de todos los programas ejecutados y analizados **(4).**
- **Para listar los elementos actualmente bloqueados por estar clasificados como PUP:** panel Actividad de PUP y Panel Clasificación de todos los programas ejecutados y analizados **(5).**
- **Para listar los elementos actualmente bloqueados por estar clasificados como Exploit:** panel Actividad de Exploit y Panel Clasificación de todos los programas ejecutados y analizados **(6).**
- **Para listar los elementos actualmente bloqueados por estar clasificados como virus:** panel Amenazas detectadas por el antivirus **(7).**
- **Para listar los elementos actualmente bloqueados por estar en proceso de clasificación:** panel Programas actualmente bloqueados en clasificación **(2).**

Mostrar los elementos excluidos del bloqueo por el administrador

- **Para listar los programas clasificados como amenaza, PUP o desconocidos actualmente excluidos de bloqueos:** panel Programas permitidas por el administrador **(3).**
- **Para listar un histórico de los programas actualmente excluidos:** panel Programas permitidos por el administrador **(3)**, menú contextual Histórico.
- **Para listar los cambios de estado de un programa excluido:** panel Programas permitidos por el administrador **(3)**, menú contextual Histórico.
- **Para listar los programas clasificados como afectados por un Exploit y permitidos por el sistema:** panel Actividad de Exploit y Panel Clasificación de todos los programas ejecutados y analizados **(6).**

Añadir y eliminar exclusiones

- **Para añadir una exclusión sobre un malware**: panel Actividad de malware **(4)**, selección de una amenaza, **No volver a detectar.**
- **Para añadir una exclusión sobre un PUP**: panel Actividad del PUP **(5)**, selección de una amenaza, **No volver a detectar.**
- **Para añadir una exclusión sobre un virus**: panel Amenazas detectadas por el antivirus **(6)**, selección de una amenaza, **Restaurar y no volver a detectar.**
- **Para eliminar una exclusión:** panel Programas permitidos por el administrador **(3)**, selección de una amenaza con el icono 🗑.

Cambio de comportamiento de los bloqueos

- **Para cambiar el comportamiento de las reclasificaciones**: panel Programas permitidos por el administrador **(3)**, link **Cambiar comportamiento.**

Diagrama de estados de los procesos encontrados

permite la creación de exclusiones, mediante las cuales un programa en clasificación o clasificado como malware podrá ejecutarse.

> *IMPORTANTE: De forma general se desaconseja el desbloqueo de elementos. Los elementos bloqueados por estar clasificados como peligrosos representan un riesgo cierto para la integridad de los sistemas de IT de la empresa y sus datos. Para los elementos bloqueados por ser desconocidos existe una probabilidad alta de que terminen siendo clasificados como peligrosos. Por estas razones se recomienda evitar a toda costa el desbloqueo de elementos desconocidos o clasificados como malware / PUP.*

Diagrama de estados para ficheros conocidos

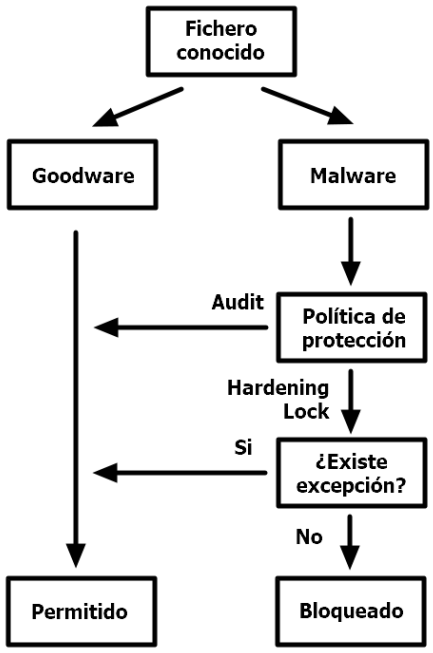


Figura 19.2: diagrama de acciones para procesos conocidos y ya clasificados

En el caso de un fichero clasificado por Cytomic EPDR como malware/PUP y una política de protección avanzada distinta de **Audit**, los ficheros serán bloqueados a no ser que el administrador genere una excepción que permita su ejecución.

Ficheros desconocidos

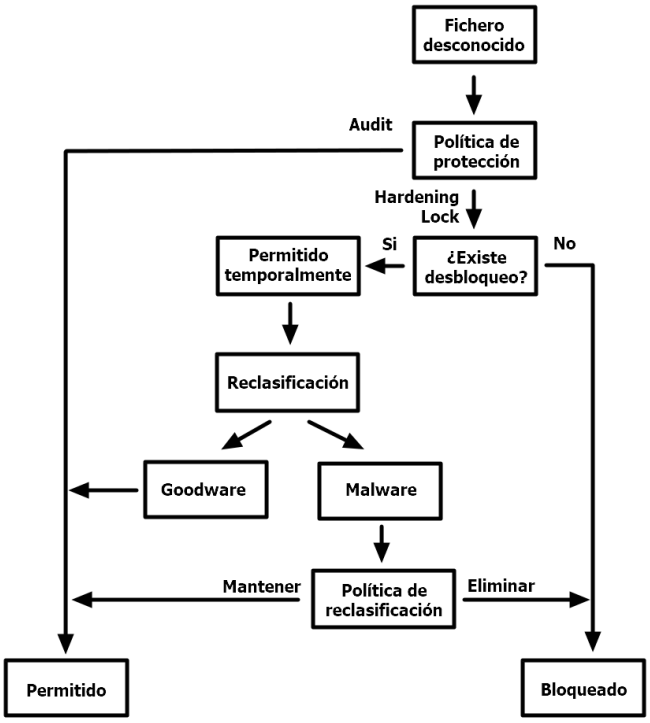


Figura 19.3: diagrama de acciones para procesos desconocidos

En el caso de los ficheros desconocidos (sin clasificar) y una política de protección avanzada distinta de **Audit**, los ficheros se bloquearán a no ser que el administrador de la red genere una excepción. Aparte de esto, Cytomic EPDR clasificará el fichero y, dependiendo del resultado y de la política de reclasificación elegida, lo bloqueará o se seguirá ejecutando.

Política de reclasificación

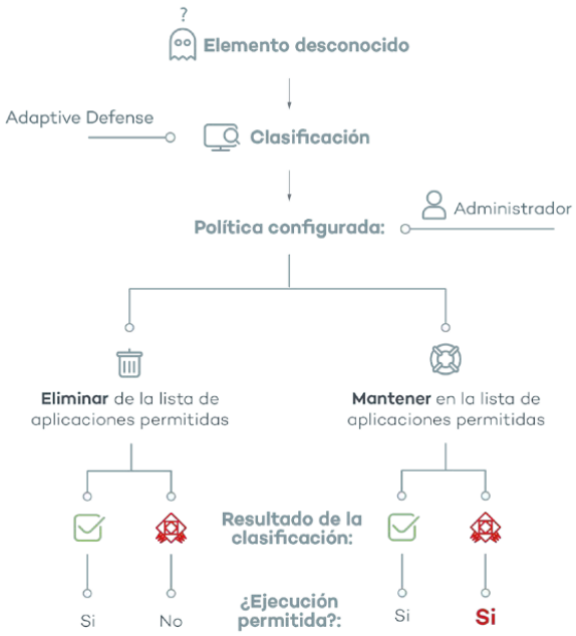


Figura 19.4: comportamiento de Cytomic EPDR ante la política de reclasificación elegida y el resultado de la clasificación

La política de reclasificación establece el comportamiento automático de Cytomic EPDR cuando un elemento desbloqueado por el administrador cambia su estado interno y es necesario tomar una nueva decisión.

En los casos en los que el administrador crea una excepción para desbloquear un elemento desconocido previamente bloqueado por Cytomic EPDR, lo normal es que con el tiempo el elemento se clasifique como malware o goodware. Si es goodware no se requiere ningún tipo de consideración adicional ya que el sistema ya su ejecución. Por el contrario, si el elemento es clasificado como malware, la política de reclasificación entra en juego, permitiendo al administrador definir el comportamiento de Cytomic EPDR:

- **Eliminar de la lista de Programas permitidos por el administrador**: si el fichero desconocido se ha clasificado como goodware se seguirá ejecutando de forma normal, si es clasificado como malware la exclusión se eliminará de forma automática y el fichero quedará nuevamente bloqueado, a no ser que el administrador genere una nueva exclusión manual para ese fichero.
- **Mantener en la lista de Programas permitidos por el administrador**: tanto si el fichero desconocido se ha clasificado como goodware o malware la exclusión se mantiene y el fichero seguirá ejecutándose.

Cambiar la política de reclasificación

Desde el menú superior **Estado**, en el panel **Programas permitidos por el administrador**, el link **Cambiar comportamiento** muestra una ventana emergente donde se puede seleccionar la política de reclasificación a aplicar.

> *La política de reclasificación es general para todos los equipos de la red e independiente de la configuración de seguridad asignada.*

En caso de seleccionar **Mantener en la lista de Programas permitidos por el administrador**, se muestra en el listado **Programas permitidos por el administrador** una franja de color rojo indicando que esta elección puede dar lugar a situaciones potencialmente peligrosas. Un escenario típico es el de un elemento desconocido originalmente, desbloqueado por el administrador para poder ser ejecutado mientras se clasifica y que, una vez terminado su análisis, resulta ser peligroso. En este caso se continuaría su ejecución por no eliminarse la exclusión de forma automática debido a la política de reclasificación **Mantener en la lista de Programas permitidos por el administrador** elegida.

Trazabilidad de las reclasificaciones

Es necesario conocer si Cytomic EPDR ha reclasificado un elemento desconocido, sobre todo si el administrador ha elegido la política de **Mantener en la lista de Programas permitidos por el administrador**.

Trazabilidad mediante el Histórico de Programas permitidos

Para visualizar el histórico de reclasificaciones y eventos de un fichero excluido, desde **Programas permitidos por el administrador** haz clic en el menú contextual para mostrar el histórico de Programas permitidos. En este listado permite buscar por el nombre de la amenaza, y en el campo **acción** se detallará el tipo de evento que se ha sucedido.

Trazabilidad mediante alertas

Las alertas le dan al administrador la posibilidad de recibir notificaciones por correo en el momento en que se producen los bloqueos por ficheros desconocidos. También se envía información de las reclasificaciones de los ficheros que previamente ha desbloqueado.

Para habilitar las notificaciones por correo en bloqueos de ficheros desconocidos:

- En la zona **Configuración**, haz clic en la entrada **Mis alertas** del panel lateral y habilita los siguientes tipos de alertas:
  - Programas bloqueados en proceso de clasificación.
  - Clasificaciones de archivos que han sido permitidos por el administrador.

Añadir un desbloqueo / exclusión de elementos

Al añadir una exclusión de un elemento ejecutable con extensión .exe o .com, Cytomic EPDR permitirá la ejecución de todas las librerías y binarios utilizados en el programa excluido, excepto aquellos ya conocidas y clasificadas como amenazas. En cualquier caso, los elementos excluidos se siguen monitorizando para clasificados como goodware o malware o actualizar su clasificación tanto si se trata de goodware como de amenazas conocidas.

Dependiendo de si el administrador quiere permitir la ejecución de un fichero en clasificación o de un fichero ya clasificado como amenaza, el control de exclusiones se aplica desde el panel **Programas actualmente bloqueados en clasificación** o desde **Actividad del Malware / PUP.**

Exclusión de elementos desconocidos pendientes de clasificación

Si los usuarios no pueden esperar a que el sistema haya completado la clasificación para liberar el bloqueo de forma automática, el administrador puede utilizar el botón **Desbloquear** al abrir un elemento bloqueado en el panel **Programas actualmente bloqueados en clasificación**.

Una vez desbloqueado, el elemento desaparecerá del panel **Programas actualmente bloqueados en clasificación** ya que el administrador asume el riesgo de su ejecución. No obstante, Cytomic EPDR continuará analizando el proceso hasta completar su clasificación. El elemento desbloqueado aparecerá en el listado de **Programas permitidos por el administrador**, mostrado en el apartado "**Ventana de detalle**" en la página **409**.

Exclusión de elementos clasificados como malware o PUP

Excluir un elemento clasificado como malware es la operación equivalente a desbloquear un elemento bloqueado sin clasificar, si bien en este caso se está permitiendo la ejecución de un programa que Cytomic EPDR ya ha clasificado de forma efectiva como dañino o peligroso para el sistema.

Desde el panel **Actividad de malware / PUP** el administrador puede utilizar el botón **No volver a detectar** seleccionando previamente la amenaza que quiere permitir su ejecución.

Una vez excluido el elemento deja de generar incidentes en los paneles de **Actividad de malware / PUP** y se añade al listado de **Programas permitidos por el administrador,** tal y como se indica en el apartado "**Gestión de los elementos excluidos**". Si el administrador quiere permitir la ejecución de un fichero ya clasificado como amenaza, el control de exclusiones se aplica desde el panel **Amenazas detectadas por el antivirus**.

Gestión de los elementos excluidos

La gestión de los todos los elementos excluidos y el comportamiento del sistema ante reclasificaciones, tanto de procesos conocidos y clasificados como una amenaza como de desconocidos, se ejecuta desde el panel **Programas permitidos por el administrador**.

Este panel permite visualizar y gestionar los ficheros actualmente permitidos, así como acceder a un histórico de los elementos excluidos.

Mostrar las exclusiones en curso

Programas permitidos por el administrador muestra los elementos que tienen una exclusión activa. Todos los elementos que aparecen listados tienen permitida su ejecución.

Historial

Haz clic en el menú de contexto, **Historial** para visualizar el histórico de cambios realizado sobre los ficheros excluidos en Cytomic EPDR. El listado muestra el ciclo de estados completo de un fichero, desde que entra en el listado de **Programas permitidos por el administrador** hasta que sale del mismo, pasando por todos los cambios de estado intermedios que el sistema o el administrador pueda haber provocado.

Estrategias para supervisar la clasificación de ficheros

En el funcionamiento diario de un equipo protegido con Cytomic EPDR es posible que aparezca un pequeño porcentaje de programas desconocidos que tengan que ser clasificados. Dependiendo de la configuración avanzada, estos programas serán bloqueados hasta que los procesos de clasificación emitan un resultado (goodware o malware), con lo que los usuarios no podrán utilizar estos programas de forma temporal.

Si el departamento de IT controla la instalación de programas en los equipos de la red y quiere minimizar el impacto del software desconocido en el trabajo de los usuarios, pero a su vez no se aceptan concesiones a la seguridad (es decir, permitir temporalmente la ejecución de programas sin clasificar), es recomendable preparar de antemano la ejecución del software nuevo antes de su instalación y uso masivo.

El procedimiento de preparación se puede dividir en tres pasos, mostrados a continuación:

- Configurar el PC de pruebas.
- Instalar el software.
- Reclasificar los programas bloqueados.
- Envío del programa directamente a la nube de Cytomic.

Configurar el equipo de pruebas

El objetivo es determinar si el software a utilizar en la red ya es conocido como malware, o es desconocido para Cytomic. Para ello se puede utilizar el equipo de un usuario de la red, o utilizar un equipo dedicado en exclusiva a este objetivo. Este equipo debe tener asignada inicialmente una configuración de seguridad avanzada **Hardening**.

Instalar el software

Instala el software y ejecútalo de forma normal. Si Cytomic EPDR encuentra algún módulo o programa desconocido lo bloqueará mostrando una ventana emergente en el equipo. Además, se

añadirá un nuevo elemento en el panel **Programas actualmente bloqueados en clasificación**. Internamente, Cytomic EPDR registrará los eventos generados por el uso del programa y enviará los binarios a la nube para poder estudiarlos.

Si no se han presentado bloqueos en el modo Hardening, cambia la configuración a modo Lock y vuelve a ejecutar el programa recién instalado. Si aparecen nuevos bloqueos el panel **Programas actualmente bloqueados en clasificación** los reflejará.

Reclasificar los programas bloqueados

En el momento en que Cytomic EPDR emite una clasificación de los programas bloqueados se envía una notificación por correo al administrador avisando del desbloqueo si la clasificación es goodware, o su bloqueo por considerarse una amenaza. Cuando todos los procesos hayan sido reclasificados como goodware, el software instalado será apto para su ejecución en el parque informático.

Envío del programa directamente a la nube de Cytomic

Debido a que Cytomic EPDR está preparado para no impactar en el rendimiento de la red en el caso de tener que enviar ficheros a la nube de Cytomic, su envío puede demorarse en el tiempo. Si quieres acelerar el proceso ponte el contacto con el departamento de soporte de Cytomic.

Gestión de la zona de backup / cuarentena

La cuarentena en Cytomic EPDR es el área de backup donde se copian los elementos eliminados por haber sido clasificados como amenaza.

Los elementos eliminados se almacenan en el propio equipo del usuario, en el directorio `Quarantine` de la carpeta donde se instaló el software. Se trata de una carpeta inaccesible al resto de procesos del equipo y cifrada, de manera que no es posible el acceso ni la ejecución de los programas allí contenidos de forma directa, si no es a través de la consola Web.

La cuarentena es compatible con las plataformas Windows, macOS y Linux. No se soporta en dispositivos Android.

El envío de elementos al área de backup es automático y establecido por el departamento de Cytomic Labs en Cytomic, según su clasificación después de haber efectuado el análisis.

Una vez que los elementos sospechosos han sido enviados a Cytomic, se pueden producir cuatro situaciones:

- **Si se comprueba que los elementos son maliciosos**: se desinfectan y posteriormente se restauran a su ubicación original, siempre y cuando exista desinfección para ello.
- **Si se comprueba que los elementos son maliciosos y no existe manera de desinfectarlos**: permanece en la cuarentena durante 7 días.

- **Si se comprueba que no se trata de elementos perjudiciales**: se restauran directamente a su ubicación.
- **Si se comprueba que son elementos sospechosos**: se almacenan durante 30 días como máximo. Si finalmente resultan ser goodware se restauran automáticamente.

Cytomic EPDR no borra ningún fichero del equipo del usuario. Todos los elementos eliminados son enviados al área de backup.

Visualizar los elementos en cuarentena

El administrador visualiza los elementos introducidos en la cuarentena mediante los listados y los widgets del Panel de control, indicados a continuación:

- Actividad de malware.
- Actividad de PUP.
- Amenazas detectadas por el antivirus.

Obtén el listado de elementos introducidos en cuarentena con ayuda de las herramientas de filtrado, reflejados en el campo **Acción** como **Movido a cuarentena** o **Eliminado**.

Restaurar elementos de cuarentena

Haz clic en el botón **Restaurar y no volver a detectar**. Esta acción no solo copia el fichero a su ubicación original, sino que restaura los permisos, propietario, entradas del registro referidas al fichero y otra información referida al fichero.

Capítulo 20

Análisis forense

Cytomic EPDR incorpora un conjunto de tecnologías avanzadas que permiten detectar y bloquear la ejecución del malware desconocido o especialmente diseñado para pasar inadvertido en las estaciones de trabajo y servidores de las compañías. Estas tecnologías recogen una gran cantidad de información sobre las acciones ejecutadas en los equipos del cliente gracias a la monitorización permanente de todos los procesos en funcionamiento. Con esta información es posible determinar hasta qué punto ha sido comprometida la red del cliente, y así poder ayudar al administrador de la red a tomar las medidas apropiadas.

La consola Web pone a disposición del administrador toda esta información a través de varios recursos, dependiendo del grado de detalle que se necesite:

- Páginas de detalle extendido.
- Tablas de acciones.
- Diagramas de grafos.
- Ficheros Excel.

CONTENIDO DEL CAPÍTULO

Detalle de los programas bloqueados

Cytomic EPDR permite visualizar el detalle extendido de los programas cuando son bloqueados por alguna de las tecnologías de detección avanzada que incorpora.

Para acceder al detalle extendido de las amenazas avanzadas haz clic en el menú superior **Estado**, añade uno de los listados mostrados a continuación y haz clic en uno de los elementos del listado:

- **Actividad de Malware y PUPs** para abrir la ventana **Detección del malware**.
- **Actividad de Exploits** para abrir la ventana **Detección de exploit**.
- **Programas actualmente bloqueados en clasificación** para abrir la ventana **Detalles del programa bloqueado**.
- **Programas bloqueados por el administrador** para abrir la ventana **Detalle del programa bloqueado**.

Dependiendo del tipo de amenaza se añadirá la pestaña **Detalles** a la ventana para mostrar información extendida.

Detección del malware y Detalles del programa bloqueado

La ventana se divide en secciones siguientes:

- Información general.
- Equipo afectado.
- Impacto de la amenaza en el equipo.
- Origen de la infección.
- Apariciones en otros equipos.

Información general

Campo	Descripción
Amenaza	Nombre de la amenaza y hash que la identifica.
Acción	Tipo de acción que Cytomic EPDR ha ejecutado sobre el elemento. • Movido a Cuarentena. • Bloqueado. • Desinfectado. • Eliminado.

Tabla 20.1: campos de la sección Información general en Detección de malware, PUP y programas bloqueados en clasificación

Equipo afectado

*Consulta el capítulo "**Gestión de amenazas, elementos en clasificación y cuarentena**" en la página **437** para obtener información sobre las acciones que el administrador puede ejecutar sobre los elementos encontrados.*

Campo	Descripción
Equipo	Nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos.
Visualizar parches disponibles	Si el módulo Cytomic Patch está activado muestra los parches y actualizaciones pendientes de instalar en el equipo.
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.
Modo de protección	Configuración de la protección avanzada en el momento de producirse la detección (**Audit**, **Hardening**, **Lock**).
Ruta de detección	Ruta del sistema de ficheros donde reside la amenaza.

Tabla 20.2: campos de la sección Equipo afectado en Detección de malware, PUP y programas bloqueados en clasificación

Impacto de la amenaza en el equipo

Campo	Descripción
Amenaza	Nombre de la amenaza detectada y cadena resumen de identificación del archivo (hash). Haz clic en los dos botones para ampliar información en Internet mediante el buscador Google y la web de Virustotal. Si la amenaza es de reciente aparición se mostrará la leyenda **Nueva amenaza.**
Actividad	Resumen de las acciones más importantes ejecutadas por el malware: • **Se ha ejecutado** • **Ha accedido a datos** • **Ha intercambiado datos con otros equipos** • **Ver detalle de actividad completo**: al hacer clic se muestra la pestaña **Actividad** tratada en el apartado "**Tablas de acciones**". • **Ver gráfica de actividad**: al hacer clic se muestra la gráfica de **Actividad** tratada en el apartado "**Grafos de ejecución**".
Fecha de detección	Fecha en la que Cytomic EPDR detectó la amenaza en la red del cliente.
Tiempo de exposición	Tiempo que la amenaza ha permanecido sin clasificar en la red del cliente.

Tabla 20.3: campos de la sección Impacto de la amenaza en el equipo en Detección de malware, PUP y programas bloqueados en clasificación

Origen de la infección

Campo	Descripción
Equipo origen de la amenaza	Si el intento de infección viene de un equipo de la red del cliente, indica el nombre del equipo.
IP origen de la amenaza	Si el intento de infección viene de un equipo de la red del cliente, indica la dirección IP del equipo.
Usuario origen de la amenaza	Usuario conectado en la máquina origen de la infección.

Tabla 20.4: campos de la sección Origen de la infección en Detección de malware, PUP y programas bloqueados en clasificación

Apariciones en otros equipos

Muestra todos los equipos de la red donde fue visto el malware detectado.

Campos	Descripción
Equipo	Nombre del equipo.
Ruta del archivo	Ruta y nombre del fichero que contiene el malware.
Fecha primera aparición	Fecha en la que la amenaza fue detectada por primera vez en ese equipo.

Tabla 20.5: campos de la sección Apariciones en otros equipos en Detección de malware, PUP y programas bloqueados en clasificación

Detección exploit

La ventana se divide en 5 secciones:

- Información general.
- Equipo afectado.
- Impacto de la amenaza en el equipo.
- Origen de la infección.
- Apariciones en otros equipos.

Información general

Campo	Descripción
Programa comprometido	Nombre del programa que fue afectado por el exploit y hash que lo identifica.
Acción	Muestra el tipo de acción que Cytomic EPDR ha ejecutado sobre el programa afectado por el exploit. • **Permitido**: la protección anti-exploit está configurada en modo **Audit**. El exploit se ejecutó. • **Bloqueado**: el exploit fue bloqueado antes de su ejecución. • **Permitido por el usuario**: se preguntó al usuario del equipo si finalizar el proceso comprometido y el usuario decidió permitir que el exploit continúe ejecutándose. • **Proceso finalizado**: el exploit fue eliminado, pero se llegó a ejecutar parcialmente. • **Pendiente de reinicio**: se informó al usuario del equipo de la necesidad de reiniciar el equipo para eliminar completamente el exploit. Mientras tanto el exploit se seguirá ejecutando.

Tabla 20.6: campos de la sección Información general en Detección exploit

Equipo afectado

Campo	Descripción
Equipo	Nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos.
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.
Modo de protección	Configuración de la protección avanzada en el momento de producirse la detección (**Audit**, **Hardening**, **Lock**).
Ruta de detección	Ruta del sistema de ficheros donde reside la amenaza.

Tabla 20.7: campos de la sección Equipo afectado en Detección exploit

Impacto del exploit en el equipo

Campo	Descripción
Programa comprometido	Ruta y nombre del programa que recibió el intento de explotación. Si Cytomic EPDR detectó que el programa no está actualizado a la última versión publicada por el proveedor, mostrará el aviso **Programa vulnerable.**
Actividad	• **Se ha ejecutado**: el exploit se llegó a ejecutar antes de ser detectado por Cytomic EPDR. • **Ver detalle de actividad completo**: al hacer clic se muestra la pestaña **Actividad** tratada en el apartado"**Tablas de acciones**". • **Ver gráfica de actividad**: al hacer clic se muestra la gráfica de **Actividad** tratada en el apartado "**Grafos de ejecución**".
Fecha de detección	Fecha en la que Cytomic EPDR detectó el exploit en la red del cliente.
Últimas URLs accedidas	Listado de las URLs accedidas por el proceso vulnerable en el momento en que fue afectado por el exploit.

Tabla 20.8: campos de la sección Impacto del exploit en el equipo en Detección exploit

Detalle del programa bloqueado

La ventana se divide en las secciones siguientes:

- Información general.
- Equipo.
- Programa bloqueado.

Información general

Campo	Descripción
Programa bloqueado	Nombre del programa bloqueado por el administrador.

Tabla 20.9: campos de la sección Información general en Detalle del programa bloqueado

Equipo

Campo	Descripción
Equipo	Nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos.
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.

Tabla 20.10: campos de la sección Equipo en Detalle del programa bloqueado

Programa bloqueado

Campo	Descripción
Nombre	Nombre del programa bloqueado por el administrador.
Ruta	Ruta del programa bloqueado por el administrador dentro del equipo del usuario o servidor.
Hash	Hash del programa bloqueado por el administrador.
Fecha de detección	Fecha en la que Cytomic EPDR bloqueó la ejecución del programa.

Tabla 20.11: campos de la sección Programa bloqueado en Detalle del programa bloqueado

Tablas de acciones

Cytomic EPDR permite visualizar las acciones de los programas cuando son detectados por alguna de las tecnologías de detección avanzada que incorpora.

Para acceder a la tabla de acciones de las amenazas avanzadas haz clic en el menú superior **Estado**, añade uno de los listados mostrados a continuación y haz clic en uno de los elementos del listado:

- **Actividad de Malware y PUPs** para abrir la ventana **Detección del malware**.
- **Actividad de Exploits** para abrir la ventana **Detección de exploit**.
- **Programas actualmente bloqueados en clasificación** para abrir la ventana **Detalles del programa**

bloqueado.

- **Bloqueos por políticas avanzadas de seguridad** para abrir la ventana **Bloqueo por política avanzada de seguridad.**

Haz clic en la pestaña **Actividad** para mostrar la tabla de acciones de la amenaza.

La información de la amenaza se muestra en una tabla de acciones, que incluye los eventos producidos más relevantes.

La cantidad de acciones ejecutadas por un proceso es muy alta, visualizarlas todas dificultaría la extracción de información útil para realizar un análisis forense.

El contenido de la tabla se presenta inicialmente ordenado por fecha, de esta forma es más fácil seguir el curso de la amenaza.

La tabla de acciones contiene los campos mostrados a continuación:

Campo	Comentario	Valores
Fecha	Fecha de la acción registrada.	Fecha
Nº veces	Número de veces que se ejecutó la acción. Una misma acción ejecutada varias veces de forma consecutiva solo aparece una vez en el listado de acciones con el campo Nº veces actualizado.	Numérico
Acción	Tipo de acción registrada en el sistema y línea de comandos asociada a la ejecución de la acción.	• Descargado de • Comunica con • Accede a datos • Accede • Es accedido por • LSASS.EXE abre • LSASS.EXE es abierto por • Es ejecutado por • Ejecuta • Es creado por • Crea • Es modificado por • Modifica • Es cargado por • Carga • Es borrado por

Tabla 20.12: campos de la tabla de acciones de una amenaza

Campo	Comentario	Valores
		• Borra • Es renombrado por • Renombra • Es matado por • Mata proceso • Crea hilo remoto • Hilo inyectado por • Es abierto por • Abre • Crea • Es creado por • Crea clave apuntando a Exe • Modifica clave apuntando a Exe.
Path/URL/ Clave de Registro / IP:Puerto	Entidad de la acción. Según el tipo de acción contiene diferentes valores.	• **Clave del registro**: acciones que impliquen modificación del registro de Windows. • **IP:Puerto**: acciones que implican una comunicación con un equipo local o remoto. • **Path**: acciones que implican acceso al disco duro del equipo. • **URL**: acciones que implican el acceso a una URL.
Hash del Fichero/Valor del Registro / Protocolo-Dirección/ Descripción	Campo que complementa a la entidad.	• **Hash del Fichero**: para todas las acciones que implican acceso a un fichero. • **Valor del Registro**: para todas las acciones que implican un acceso al registro.

Tabla 20.12: campos de la tabla de acciones de una amenaza

Campo	Comentario	Valores
		• **Protocolo-Dirección**: para todas las acciones que implican una comunicación con un equipo local o remoto. Los valores posibles son: • TCP • UDP • Bidirectional • Unknown • Descripción
Confiable	El fichero está firmado digitalmente.	Binario

Tabla 20.12: campos de la tabla de acciones de una amenaza

Sujeto y predicado de las acciones

El formato utilizado para presentar la información en el listado de acciones mantiene cierto paralelismo con el lenguaje natural:

- Todas las acciones tienen como sujeto el fichero clasificado como amenaza. Este dato no se indica en cada línea de la tabla de acciones porque es común para todas las líneas.
- Todas las acciones tienen un verbo que relaciona el sujeto (la amenaza clasificada) con un complemento, llamado entidad. La entidad se corresponde con el campo **Path/URL/Clave de Registro /IP:Puerto** de la tabla.
- La entidad se complementa con un segundo campo que añade información a la acción, indicado en el campo **Hash del Fichero/Valor del Registro /Protocolo-Dirección/Descripción**.

En la tabla **20.13** se muestras dos acciones de ejemplo de un mismo malware hipotético:

Fecha	Nº veces	Acción	Path/URL/ Registro/IP	Hash/Registro/ Protocolo/Descripción	Confiable
3/30/ 2015 4:38:40 PM	1	Comunica con	`54.69.32.99:80`	TCP-Bidirectional	NO
3/30/ 2015 4:38:45 PM	1	Carga	`PROGRAM_FILES|\ MOVIES TOOLBAR\SAFETYN`	`9994BF035813FE8EB6BC98E CCBD5B0E1`	NO

Tabla 20.13: listado de acciones de una amenaza de ejemplo

La primera acción indica que el malware (sujeto) se conecta (Acción **Comunica con**) con la dirección `IP 54.69.32.99:80` (entidad) mediante el protocolo TCP-Bidireccional.

La segunda acción indica que el malware (sujeto) carga (Acción **Carga**) la librería `PROGRAM_FILES|\MOVIES TOOLBAR\SAFETYNUT\SAFETYCRT.DLL` con hash `9994BF035813FE8EB6BC98ECCBD5B0E1.`

Al igual que en el lenguaje natural, en Cytomic EPDR se implementan dos tipos de oraciones:

- **Activa**: son acciones predicativas (con un sujeto y un predicado) relacionados por un verbo en forma activa. En estas acciones, el verbo de la acción relaciona el sujeto, que siempre es el proceso clasificado como amenaza y un complemento directo, la entidad, que puede ser de múltiples tipos según la acción.
- **Pasiva**: son acciones donde el sujeto (el proceso clasificado como amenaza) pasa a ser sujeto paciente (que recibe la acción, no la ejecuta) y el verbo aparece en forma pasiva (ser + participio). En este caso el verbo pasivo relaciona el sujeto pasivo que recibe la acción con la entidad, que es la que ejecuta la acción.

Ejemplos de acciones activas son:

- Comunica con
- Carga
- Crea

Ejemplos de acciones pasivas son:

- Es creado por
- Descargado de

La tabla **20.14** muestra una acción pasiva de ejemplo para un malware hipotético:

Fecha	Nº veces	Acción	Path/URL/ Registro/IP	Hash/Registro/ Protocolo/Descripción	Confiable
3/30/2015 4:51:46 PM	1	Es ejecutado por	`WINDOWS|\ explorer.exe`	`7522F548A84ABAD8FA516D E5AB3931EF`	NO

Tabla 20.14: ejemplo de acción pasiva

En esta acción el malware (sujeto pasivo) es ejecutado (acción pasiva **Es ejecutado por**) por el programa `WINDOWS|\explorer.exe` (entidad) de hash `7522F548A84ABAD8FA516DE5AB3931EF`.

Las acciones de tipo activa permiten inspeccionar en detalle los pasos que ha ejecutado la amenaza. Por el contrario, las acciones de tipo pasivo suelen reflejar el vector de infección utilizado por el malware (qué proceso lo ejecutó, qué proceso lo copió al equipo del usuario etc.).

Grafos de ejecución

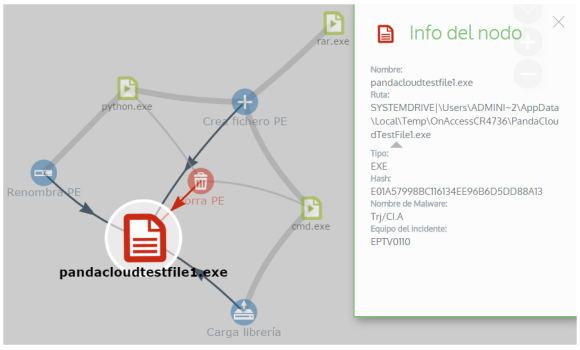


Figura 20.1: amenaza representada mediante grafos

Cytomic EPDR permite visualizar las acciones de los programas en un grafo cuando son detectados por alguna de las tecnologías de detección avanzada que incorpora.

Para acceder al grafo de ejecución de las amenazas avanzadas haz clic en el menú superior **Estado**, añade uno de los listados mostrados a continuación y haz clic en uno de los elementos del listado:

- **Actividad de Malware y PUPs** para abrir la ventana **Detección del malware**.
- **Actividad de Exploits** para abrir la ventana **Detección de exploit**.
- **Programas actualmente bloqueados en clasificación** para abrir la ventana **Detalles del programa bloqueado**.
- **Bloqueos por políticas avanzadas de seguridad** para abrir la ventana **Bloqueo por política avanzada de seguridad.**

Haz clic en la pestaña **Actividad** y **Ver gráfica de actividad** para mostrar el grafo de ejecución de la amenaza.

Los grafos de ejecución representan de forma visual la información mostrada en las tablas de acciones, poniendo énfasis en el enfoque temporal. Los grafos se utilizan inicialmente para tener, de un solo vistazo, una idea general de las acciones desencadenadas por la amenaza.

Diagramas

La cadena de acciones en la vista de grafos de ejecución se representa mediante dos elementos:

- **Nodos**: en su mayoría accione o elementos informativos.
- **Líneas y flechas**: unen los nodos de acción e informativos para establecer un orden temporal y asignar a cada nodo el rol de "sujeto" o "predicado".

Nodos

Muestran la información mediante su icono asociado, color y un panel descriptivo que se muestra a la derecha de la pantalla cuando se seleccionan con el ratón.

El código de colores utilizado es:

- **Rojo**: elemento no confiable, malware, amenaza.
- **Naranja**: elemento desconocido, no catalogado.
- **Verde**: elemento confiable, goodware.

La tabla 20.15 lista los nodos de tipo acción junto con una breve descripción:

Símbolo	Descripción	Símbolo	Descripción
	• Fichero descargado. • Fichero comprimido creado.		Fichero ejecutable borrado.
	Socket / comunicación usada.		Librería cargada.
	La monitorización comenzó.		Servicio instalado.
	Proceso creado.		Fichero ejecutable renombrado.
	• Fichero ejecutable creado. • Librería creada. • Clave en el registro creada.		Proceso detenido o cerrado.
	• Fichero ejecutable modificado. • Clave de registro modificada.		Hilo creado remotamente.
	Fichero ejecutable mapeado para escritura.		Fichero comprimido abierto.

Tabla 20.15: representación gráfica de acciones en el diagrama de grafos

La tabla 20.16 lista los nodos de tipo descriptivo junto con una breve descripción:

Símbolo	Descripción
	Nombre de fichero y extensión. • **Verde**: goodware. • **Naranja**: no catalogado. • **Rojo**: malware/PUP.

Tabla 20.16: tipos de nodo en el diagrama de grafos

Símbolo	Descripción
	Equipo interno (está en la red corporativa). • **Verde**: confiable. • **Naranja**: desconocido. • **Rojo**: no confiable.
	Equipos externos. • **Verde**: confiable. • **Naranja**: desconocido. • **Rojo**: no confiable.
	País asociado a la IP de un equipo externo.
	Fichero y extensión.
	Clave del registro.

Tabla 20.16: tipos de nodo en el diagrama de grafos

Líneas y flechas

Las líneas del diagrama de grafos relacionan los diferentes nodos y ayudan a establecer visualmente el orden de ejecución de las acciones.

Los dos atributos de una línea son:

- **Grosor de la línea**: número de veces que ha aparecido la relación en el diagrama. A mayor número de veces mayor tamaño de la línea.
- **Flecha**: dirección de la relación entre los dos nodos.

La línea temporal (Timeline)

Controla la visualización de la cadena de acciones ejecutadas por la amenaza a lo largo del tiempo. Mediante los botones situados en la parte inferior de la pantalla visualiza el momento preciso donde la amenaza ejecutó cierta acción, y recupera información extendida para ayudar en los procesos de análisis forense.

Es posible seleccionar un intervalo concreto de la línea temporal arrastrando los selectores de intervalo hacia la izquierda o derecha para abarcar la franja más interesante.

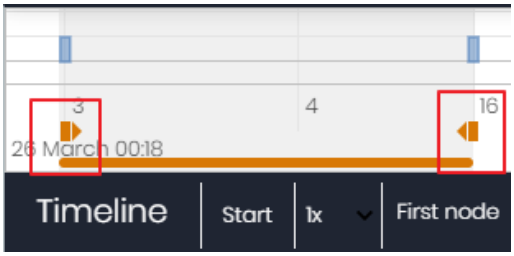


Figura 20.2: selectores del intervalo temporal a presentar

Una vez seleccionado el intervalo, el grafo mostrará únicamente las acciones y nodos que caigan en dentro de él. El resto de acciones y nodos quedará difuminado en el diagrama.

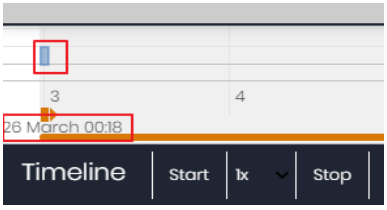


Figura 20.3: timestamp, fecha y acciones de la amenaza

Las acciones de la amenaza se representan en la línea temporal como barras verticales acompañadas del time stamp, que marca la hora y minuto donde ocurrieron.

Para poder ver la ejecución completa de la amenaza y la cadena de acciones que ejecutó, se utilizan los siguientes controles:

- **Iniciar**: comienza la ejecución de la Timeline a velocidad 1x. Los grafos y las líneas de acciones irán apareciendo según se vaya recorriendo la línea temporal.
- **1x**: establece la velocidad de recorrido de la línea temporal.
- **Detener**: detiene la ejecución de la línea temporal.
- **+ y -**: zoom in y zoom out de la línea temporal.
- **< y >**: mueve la selección del nodo al inmediatamente anterior o posterior.
- **Zoom inicial**: recupera el nivel de zoom inicial si se modificó con los botones + y –.
- **Seleccionar todos los nodos**: mueve los selectores temporales para abarcar toda la línea temporal.
- **Primer nodo**: establece el intervalo temporal en el inicio, paso necesario para iniciar la visualización de la TimeLine completa.

> *Para poder visualizar el recorrido completo de la Timeline primero selecciona "Primer nodo" y después "Iniciar". Para ajustar la velocidad de recorrido selecciona el botón 1x.*

Filtros

En la parte superior del diagrama de grafos se encuentran los controles para filtrar la información que se mostrará.

- **Acción**: desplegable que selecciona un tipo de acción de entre todas las ejecutadas por la

amenaza. El diagrama solo mostrará los nodos que coincidan con el tipo de acción seleccionada y aquellos nodos adyacentes relacionados con esta acción.

- **Entidad**: desplegable que selecciona una entidad (contenido del campo Path/URL/Entrada de registro /IP:Puerto).

Recolocar los nodos y zoom general del grafo

Para mover el grafo en las cuatro direcciones y hacer zoom in o zoom out utiliza los controles situados en la parte superior derecha del grafo.

> *Para hacer zoom in y zoom out más fácilmente utiliza la rueda central del ratón.*

- El símbolo  abandona la vista de grafos.
- Para ocultar la zona de botones Timeline a fin de ganar espacio de la pantalla haz clic en el icono  situado en la parte inferior derecha del grafo.
- El comportamiento del grafo representando en pantalla es configurable mediante el panel accesible al seleccionar el botón situado en la zona superior izquierda del grafo.

Ficheros exportados Excel

Cytomic EPDR permite exportar a un fichero Excel el detalle extendido de los programas cuando son detectados por alguna de las tecnologías de detección avanzada que incorpora.

Para obtener el fichero Excel con el detalle extendido de las amenazas avanzadas detectadas sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Estado y** añade uno de los listados siguientes:
  - **Actividad de Malware y PUPs**.
  - **Actividad de Exploits**.
  - **Programas actualmente bloqueados en clasificación**.
- Haz clic en el menú de contexto situado en la parte superior derecha del listado y elige la opción **Exportar listado y detalles.** Se descargará un fichero Excel con los detalles extendidos de todas las amenazas mostradas en el listado.

Campo	Descripción	Valores
Fecha	Fecha de la acción registrada.	Fecha
Hash	Cadena resumen de identificación de la amenaza.	Cadena de caracteres

Tabla 20.17: campos del fichero exportado Listado y detalles

Campo	Descripción	Valores
Amenaza	Nombre de la amenaza.	Cadena de caracteres
Usuario	Cuenta de usuario bajo la cual se ejecutó la amenaza.	Cadena de caracteres
Equipo	Nombre del equipo donde se encontró la amenaza.	Cadena de caracteres
Ruta	Nombre de la amenaza y ruta en el equipo del usuario.	Cadena de caracteres
Acceso a datos	La amenaza ha accedido a ficheros que residen en el equipo del usuario.	Binario
Acción	Tipo de acción registrada en el sistema.	• Descargado de • Comunica con • Accede a datos • Accede • Es accedido por • LSASS.EXE abre • LSASS.EXE es abierto por • Es ejecutado por • Ejecuta • Es creado por • Crea • Es modificado por • Modifica • Es cargado por • Carga • Es borrado por • Borra • Es renombrado por • Renombra • Es matado por • Mata proceso • Crea hilo remoto • Hilo inyectado por • Es abierto por • Abre • Crea • Es creado por • Crea clave apuntando a Exe • Modifica clave apuntando a Exe

Tabla 20.17: campos del fichero exportado Listado y detalles

Campo	Descripción	Valores
Línea de comandos	Línea de comandos asociada a la ejecución de la acción.	Cadena de caracteres
Fecha del evento	Fecha y hora en la que el evento se registró en el equipo del cliente.	Cadena de caracteres
Nº veces	Número de veces que se ejecutó la acción. Una misma acción ejecutada varias veces de forma consecutiva solo aparece una vez en el listado de acciones con el campo Nº veces actualizado.	Numérico
Path/URL/Clave de Registro / IP:Puerto	Entidad de la acción. Según sea el tipo de acción podrá contener diferentes valores.	• **Clave del registro**: acciones que implican modificación del registro de Windows. • **IP:Puerto**: acciones que implican una comunicación con un equipo local o remoto. • **Path**: acciones que implican acceso al disco duro del equipo. • **URL**: acciones que implican el acceso a una URL.
Hash del Fichero/Valor del Registro / Protocolo-Dirección/ Descripción	Campo que complementa a la entidad.	• **Hash del Fichero**: acciones que implican acceso a un fichero. • **Valor del Registro**: acciones que implican un acceso al registro. • **Protocolo-Dirección**: acciones que implican una comunicación con un equipo local o remoto. Los valores posibles son: • TCP • UDP • Bidirectional • UnKnown • Descripción

Tabla 20.17: campos del fichero exportado Listado y detalles

Campo	Descripción	Valores
Confiable	El fichero está firmado digitalmente.	Binario

Tabla 20.17: campos del fichero exportado Listado y detalles

Interpretación de las tablas de acciones y grafos

Las tablas de acciones y grafos de actividad son representaciones de los volcados de evidencias recogidas en el equipo del usuario, que deberán ser interpretadas por el administrador de la red. Por esta razón se requieren ciertos conocimientos técnicos para poder extraer pautas e información clave en cada situación.

A continuación, se ofrecen unas directrices básicas para interpretar las tablas de acciones mediante varios ejemplos de amenazas reales.

El nombre de las amenazas aquí indicadas puede variar entre diferentes proveedores de seguridad. Para identificar un malware concreto se recomienda utilizar su hash.

Ejemplo 1: actividad del malware Trj/OCJ.A

En la pestaña **Detalles** se muestra la información fundamental del malware encontrado. En este caso los datos relevantes son los siguientes:

- **Amenaza**: Trj/OCJ.A
- **Equipo**: XP-BARCELONA1
- **Ruta de detección**: `TEMP|\Rar$EXa0.946\appnee.com.patch.exe`
- **Actividad**

La pestaña **Actividad** contiene acciones ya que el modo de Cytomic EPDR configurado era Hardening y el malware ya residía en el equipo en el momento en que Cytomic EPDR se instaló, siendo desconocido en el momento de su ejecución.

- **Hash**

Con la cadena de hash se podrá obtener más información de recursos web como Virus total para tener una idea general de la amenaza y funcionamiento.

- **Ruta de detección**

La ruta donde se detectó el malware por primera vez en el equipo pertenece a un directorio temporal y contiene la cadena RAR: la amenaza procede de un fichero empaquetado que el programa WinRar descomprimió temporalmente en el directorio, y dió como resultado el ejecutable `appnee.com.patch.exe`.

- **Pestaña Actividad**

Paso	Fecha	Acción	Ruta
1	3:17:00	Es creado por	`PROGRAM_FILES|\WinRAR\WinRAR.exe`
2	3:17:01	Es ejecutado por	`PROGRAM_FILES|\WinRAR\WinRAR.exe`
3	3:17:13	Crea	`TEMP|\bassmod.dll`
4	3:17:34	Crea	`PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\AMTLIB.DLL.BAK`
5	3:17:40	Modifica	`PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\amtlib.dll`
6	3:17:40	Borra	`PROGRAM_FILES|\ADOBE\ACROBAT 11.0\ACROBAT\AMTLIB.DLL.BAK`
7	3:17:41	Crea	`PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\ACROBAT.DLL.BAK`
8	3:17:42	Modifica	`PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\Acrobat.dll`
9	3:17:59	Ejecuta	`PROGRAM_FILES|\Google\ Chrome\Application\chrome.exe`

Tabla 20.18: listado de acciones Trj/OCJ.A

Los pasos 1 y 2 indican que el malware fue descomprimido por el `WinRar.Exe` y ejecutado desde el mismo programa: el usuario abrió el fichero comprimido e hizo clic en el binario que contiene.

Una vez en ejecución, en el paso 3 el malware crea una dll (bassmod.dll) en una carpeta temporal y otra (paso 4) en el directorio de instalación del programa Adobe Acrobat 11. En el paso 5 también modifica una dll de Adobe, quizá para aprovechar algún tipo de exploit del programa.

Después de modificar otras dlls lanza una instancia de Chrome y en ese momento termina la Timeline; Cytomic EPDR catalogó el programa como amenaza después de esa cadena de acciones sospechosas y detuvo su ejecución.

En la Timeline no aparecen acciones sobre el registro, de modo que es muy probable que el malware no sea persistente o no haya podido ejecutarse hasta el punto de sobrevivir a un reinicio del equipo.

El programa Adobe Acrobat 11 ha resultado comprometido, de modo que se recomienda su reinstalación. Gracias a que Cytomic EPDR monitoriza ejecutables tanto si son goodware como malware, la ejecución de un programa comprometido será detectada en el momento en que desencadene acciones peligrosas, terminando en su bloqueo.

Ejemplo 2: comunicación con equipos externos en BetterSurf

BetterSurf es un programa potencialmente no deseado que modifica el navegador instalado en el equipo del usuario e inyecta anuncios en las páginas Web que visite.

En la pestaña **Detalles** se muestra la información fundamental del malware encontrado. En este caso se cuenta con los siguientes datos:

- **Nombre**: PUP/BetterSurf
- **Equipo**: MARTA-CAL
- **Ruta de detección**: `PROGRAM_FILES|\VER0BLOCKANDSURF\N4CD190.EXE`
- **Tiempo de permanencia**: 11 días 22 horas 9 minutos 46 segundos
- **Tiempo de exposición**

En este caso el tiempo de exposición ha sido muy largo: durante casi 12 días el malware ha estado latente en la red del cliente. Este comportamiento es cada vez más usual, y puede deberse a varios motivos: que el malware no haya realizado ninguna acción sospechosa hasta muy tarde, o que simplemente el usuario descargó el fichero, pero tardó en ejecutarlo. En ambos casos la amenaza no era conocida anteriormente, con lo cual no se disponía de una firma con la que el sistema antivirus pueda compararla.

- **Pestaña Actividad**

Paso	Fecha	Acción	Ruta
1	08/03/2015 11:16	Es creado por	`TEMP|\08c3b650-e9e14f.exe`
2	18/03/2015 11:16	Es creado por	`SYSTEM|\services.exe`
3	18/03/2015 11:16	Carga	`PROGRAM_FILES|\VER0BLOF\N4Cd190.dll`
4	18/03/2015 11:16	Carga	`SYSTEM|\BDL.dll`
5	18/03/2015 11:16	Comunica con	`127.0.0.1:13879`
6	18/03/2015 11:16	Comunica con	`37.58.101.205:80`
7	18/03/2015 11:17	Comunica con	`5.153.39.133:80`
8	18/03/2015 11:17	Comunica con	`50.97.62.154:80`
9	18/03/2015 11:17	Comunica con	`50.19.102.217:80`

Tabla 20.19: listado de acciones PUP/BetterSurf

Se puede apreciar como el malware establece comunicación con varias IPs. La primera de ellas (paso 5) es el propio equipo y el resto son IPs del exterior a las que se conecta por el puerto 80, de las cuales probablemente se descarguen los contenidos de publicidad.

La principal medida de prevención en este caso será bloquear las IPs en el cortafuegos corporativo.

> *Antes de añadir reglas para el bloqueo de IPs en el cortafuegos corporativo se recomienda consultar las IPs a bloquear en el RIR asociado (RIPE, ARIN, APNIC etc.) para comprobar la red del proveedor al que pertenecen. En muchos casos la infraestructura remota utilizada por el malware es compartida con servicios legítimos alojados en proveedores, tales como Amazon y otros, de modo que bloquear IPs equivaldría a bloquear también el acceso a páginas Web legítimas.*

Ejemplo 3: acceso al registro con PasswordStealer.BT

PasswordStealer.BT es un troyano que registra la actividad del usuario en el equipo y envía la información obtenida al exterior. Entre otras cosas, es capaz de capturar la pantalla del usuario, registrar las teclas pulsadas y enviar ficheros a un servidor C&C (Command & Control).

En la pestaña **Detalles** se muestra la información fundamental de la amenaza encontrada. En este caso se cuenta con los siguientes datos relevantes:

- **Ruta de la detección**: `APPDATA|\microsoftupdates\micupdate.exe`

Por el nombre y la localización del ejecutable, el malware se hace pasar por una actualización de Microsoft. Este malware en concreto no tiene capacidad para contagiar equipos por sí mismo, requiere que el usuario ejecute de forma manual la amenaza.

- **Pestaña Actividad**

El modo de Cytomic EPDR configurado era Hardening: el malware ya residía en el equipo en el momento en que Cytomic EPDR se instaló y era desconocido en el momento de su ejecución.

- **Tabla de acciones**

Paso	Fecha	Acción	Ruta
1	31/03/2015 23:29	Es ejecutado por	`PROGRAM_FILESX86|\internet explorer\iexplore.exe`
2	31/03/2015 23:29	Es creado por	`INTERNET_CACHE|\Content.IE5\ QGV8PV80\ index[1].php`
3	31/03/2015 23:30	Crea clave apuntando a Exe	`\REGISTRY\USER\S-1-5[...]9-5659\Software\Microsoft\Windows\ CurrentVersion\Run?MicUpdate`
4	31/03/2015 23:30	Ejecuta	`SYSTEMX86|\notepad.exe`
5	31/03/2015 23:30	Hilo inyectado por	`SYSTEMX86|\notepad.exe`

Tabla 20.20: listado de acciones PasswordStealer.BT

En este caso el malware es creado en el paso 2 por una página Web y ejecutado por el navegador Internet Explorer.

> *El orden de las acciones tiene una granularidad de 1 microsegundo. Por esta razón, las acciones ejecutadas dentro del mismo microsegundo pueden aparecer desordenadas en la Timeline, como sucede en el paso 1 y paso 2.*

Una vez ejecutado, el malware se hace persistente en el equipo del usuario en el paso 3, añadiendo una rama en el registro que lanzará el programa en el inicio del sistema. Después comienza a ejecutar acciones propias del malware, tales como arrancar un `notepad` e inyectar código en uno de sus hilos.

Como acción de resolución en este caso, y en ausencia de un método de desinfección conocido, se puede minimizar el impacto de este malware borrando la entrada del registro. Es muy posible que en un equipo infectado el malware impida modificar dicha entrada; dependiendo del caso sería necesario arrancar el equipo en modo seguro o con un CD de arranque para borrar dicha entrada.

Ejemplo 4: acceso a datos confidenciales en Trj/Chgt.F

Trj/Chgt.F fue publicado por wikileaks a finales de 2014 como herramienta utilizada por las agencias gubernamentales de algunos países para realizar espionaje selectivo.

En este ejemplo se muestra directamente a la pestaña **Actividad** para observar el comportamiento de esta amenaza avanzada.

- **Tabla de acciones**

Paso	Fecha	Acción	Ruta
1	4/21/2015 2:17:47	Es ejecutado por	`SYSTEMDRIVE|\Python27\pythonw.exe`
2	4/21/2015 2:18:01	Accede a datos	`#.XLS`
3	4/21/2015 2:18:01	Accede a datos	`#.DOC`
4	4/21/2015 2:18:03	Crea	`TEMP|\doc.scr`
5	4/21/2015 2:18:06	Ejecuta	`TEMP|\doc.scr`
6	4/21/2015 2:18:37	Ejecuta	`PROGRAM_FILES|\Microsoft Office\Office12\WINWORD.EXE`
7	4/21/2015 8:58:02	Comunica con	`192.168.0.1:2042`

Tabla 20.21: listado de acciones Trj/Chgt.F

Inicialmente el malware es ejecutado por el intérprete de Python (paso 1) para luego acceder a un documento de tipo Excel y otro de tipo Word (paso 2 y 3). En el paso 4 se ejecuta un fichero de extensión `scr`, probablemente un salvapantallas con algún tipo de fallo o error que provoque una situación anómala en el equipo aprovechada por el malware.

En el paso 7 se produce una conexión de tipo TCP. La dirección IP es privada de modo que se estaría conectando a la red del propio cliente.

En este caso se deberá comprobar el contenido de los ficheros accedidos para evaluar la pérdida de información, aunque viendo la Timeline la información accedida no parece haber sido extraída de la red del cliente.

Cytomic EPDR desinfectará por sí mismo la amenaza y bloqueará de forma automática posteriores ejecuciones del malware en este y en otros clientes.

Capítulo 21

Alertas

El sistema de alertas es un recurso utilizado por Cytomic EPDR para comunicar de forma rápida al administrador situaciones de importancia para el buen funcionamiento del servicio de seguridad.

En conjunto, las alertas informan al administrador de las situaciones mostradas a continuación:

- Detección de malware, PUP o exploits.
- Detección de ataques de red.
- Intento de uso de dispositivos externos no autorizados
- Reclasificación de elementos desconocidos, malware o PUP.
- Bloqueo de procesos desconocidos para Cytomic EPDR y en proceso de clasificación.
- Cambios en el estado de las licencias.
- Errores de instalación y desprotegidos.

CONTENIDO DEL CAPÍTULO

Alertas por correo

Son mensajes generados por Cytomic EPDR cuando se producen determinados eventos y enviados a las cuentas de correo configuradas como destinatarios, generalmente mantenidas por los administradores de la red.

Configuración de alertas por correo

Desde el menú superior **Configuración**, en el panel de la izquierda **Alertas** se muestra la ventana de configuración desde donde el administrador indica las direcciones de correo que recibirán los mensajes en **Enviar las alertas a la siguiente dirección**. También puede habilitar o deshabilitar de forma global cada una de las alertas a enviar.

Nivel de acceso del administrador y envío de alertas

Las alertas se definen de forma independiente por cada usuario de la consola. El contenido de una alerta queda limitado por la visibilidad de los equipos administrados que tiene asignado el rol de la cuenta de usuario.

Tipos de alertas

Tipo	Frecuencia	Condición	Información contenida
Detecciones de malware / PUP (solo protección en tiempo real)	Máximo 2 mensajes por equipo – malware – día.	• Por cada malware detectado en tiempo real en el equipo.Solo en equipos Windows.	• Primer o segundo mensaje. • Nombre del programa malicioso. • Nombre del equipo. • Grupo. • Fecha y hora UTC. • Ruta del programa malicioso. • Hash. • Tabla de acciones de programa. • Listado de equipos donde fue previamente visto el malware.
Detecciones de exploits	Máximo de 10 alertas al día por equipo y exploit	• Por cada detección de exploit que se produzca. Solo en equipos Windows.	• Nombre, ruta y hash del programa que recibió el intento de explotación. • Nombre del equipo. • Grupo. • Fecha y hora UTC. • Acción ejecutada. • Nivel de riesgo del equipo. • Valoración de la seguridad del programa atacado. • Tabla de acciones de programa. • Posible origen del exploit.

Tabla 21.1: tabla de alertas

Tipo	Frecuencia	Condición	Información contenida
Programas bloqueados en proceso de clasificación	Por cada programa desconocido detectado en el sistema de ficheros en tiempo real.	Solo en equipos Windows.	• Nombre del programa desconocido. • Nombre del equipo. • Grupo. • Fecha y hora UTC. • Ruta del programa desconocido. • Hash. • Tabla de acciones de programa. • Listado de equipos donde fue previamente visto el programa desconocido.
Programas bloqueados por el administrador	Por cada programa bloqueado.	Solo en equipos Windows.	• Nombre del programa • Hash • Ruta del programa • Nombre del equipo • Grupo al que pertenece el equipo • Usuario que lanzó el programa • Fecha del bloqueo
Clasificaciones de archivos que han sido permitidos por el administrador	Los archivos permitidos por el administrador son aquellos que han sido bloqueados por ser desconocidos para Cytomic EPDR o por haber sido clasificados como amenazas, pero el administrador permite su ejecución. El sistema genera un correo de alerta cada vez que una clasificación se completa, ya que es posible que la acción emprendida por el sistema puede cambiar después de la clasificación, según se indica en la política de reclasificación configurada por el administrador. *Consulta el apartado "**Política de reclasificación**" en la página **443** para obtener más información sobre las políticas de reclasificación.*		
Elemento reclasificado a goodware eliminando o manteniendo la exclusión	El sistema emite una alerta indicando los datos de cada elemento desconocido pero que el administrador permitió su ejecución. Cuando está clasificado como goodware, la exclusión se elimina o se mantiene según la política de reclasificación elegida. En ambos casos se envia una alerta por si el administrador quiere eliminar manualmente la exclusión sobre el elemento, o se le avisa de que la exclusión fue eliminada de forma automática.		

Tabla 21.1: tabla de alertas

Tipo	Frecuencia	Condición	Información contenida
Equipos con error en la protección y errores durante la instalación	Cada vez que se detecte el hecho relevante	• Por cada equipo desprotegido de la red. • Equipos con la protección en estado de error o fallo en la instalación de la protección	• Nombre del equipo. • Grupo. • Descripción. • Sistema operativo. • Dirección IP. • Ruta del directorio activo. • Dominio. • Fecha y hora UTC. • **Motivo de la desprotección**: Protección con error o Error instalando.
Equipos sin licencia	Cada vez que se detecte el hecho relevante	Por cada equipo que intenta licenciarse, pero no lo consigue por falta de licencias libres.	• Nombre del equipo. • Descripción. • Sistema operativo • Dirección IP • Grupo • Ruta del directorio activo • Dominio. • Fecha y hora UTC. • Motivo de la desprotección: equipo sin licencia.
Errores durante la instalación	Cada vez que se detecte el hecho relevante	• Por cada uno de los equipos de la red, cada vez que se crea una nueva situación que derive en el cambio de estado **(1)** de protegido a desprotegido. • Si en un mismo momento se detectan varios motivos que derivan en el cambio de estado en un mismo equipo, solo se genera una alerta con todos los motivos.	• Nombre del equipo. • Estado de la protección. • Razón del cambio del estado de la protección.

Tabla 21.1: tabla de alertas

Tipo	Frecuencia	Condición	Información contenida
Equipos no administrados descubiertos	Cada vez que se detecte el hecho relevante	• Cada vez que un equipo descubridor termina un descubrimiento. • El descubrimiento ha encontrado equipos no vistos anteriormente en la red.	• Nombre del equipo descubridor. • Número de equipos descubiertos. • Enlace al listado de los equipos descubiertos en la consola.

Tabla 21.1: tabla de alertas

Cambios de estado (1)

Las razones de cambio de estado que generan una alerta son:

- **Protección con error**: sólo se contempla el estado de las protecciones antivirus y protección avanzada, en aquellas plataformas que las soporten, y cuando las licencias del cliente las incluyan.
- **Error instalando**: se enviará alerta cuando se haya producido un error en la instalación que requiera de la intervención del usuario (e.g., no hay espacio en disco), y no ante errores transitorios que podrían solucionarse autónomamente tras varios reintentos.
- **Sin licencia**: cuando el equipo no ha recibido una licencia tras registrarse, por no haber libres en ese momento.

Las razones de cambio de estado que no generan una alerta son:

- **Sin licencia**: cuando el administrador ha quitado la licencia al dispositivo o cuando Cytomic EPDR haya retirado la licencia automáticamente al equipo por haberse reducido el número de licencias contratadas.
- **Instalando**: por no resultar útil recibir una alerta cada vez que se instala un equipo.
- **Protección desactivada**: este estado es consecuencia de un cambio de configuración voluntario.
- **Protección desactualizada**: no implica necesariamente que el equipo este desprotegido, pese a estar desactualizado.
- **Pendiente de reinicio**: no implica necesariamente que el equipo este desprotegido.
- **Desactualizado el conocimiento**: no implica necesariamente que el equipo este desprotegido.

Capítulo 22

Envío programado de informes y listados

Cytomic EPDR envía por correo electrónico toda la información de seguridad que se produce en los equipos que protege. Este método de entrega facilita la compartición de información entre los distintos departamentos de la empresa, así como permite guardar un histórico de todos los eventos producidos por la plataforma, más allá de los límites de capacidad de la consola Web. De esta forma, es posible realizar un seguimiento completo del estado de la seguridad sin necesidad de que el administrador tenga que acudir a la consola web, ahorrando tiempo de gestión.

El envío automático de informes por correo electrónico permite entregar a las personas interesadas toda la información de los eventos de seguridad generados, sin dejar espacio a manipulaciones para poder evaluar de forma precisa el estado de la seguridad de la red.

CONTENIDO DEL CAPÍTULO

Características de los informes

Según el intervalo de tiempo abarcado

Dependiendo del momento en el que se produce la información incluida en el informe se distinguen dos tipos:

- **Informes consolidados**: reúnen en un solo documento toda la información generada en un intervalo de fechas.
- **Informes instantáneos**: contienen información que refleja el estado de la seguridad de la red en un momento concreto.

Según la forma de envío

Cytomic EPDR genera y envía informes de forma automática según la configuración establecida en el programador de tareas o de forma manual bajo demanda.

Con el envío de informes automáticos, los destinatarios obtendrán de forma automática y sin necesidad de acudir a la consola Web la información producida en el parque de equipos gestionado.

Según el formato de salida

Dependiendo del tipo de informe Cytomic EPDR entrega informes en formato pdf y /o csv.

Según su contenido

Dependiendo del tipo de informe su contenido será configurable, permitiendo abarcar más o menos módulos soportados por Cytomic EPDR o estableciendo filtros para limitar la información a equipos que cumplan con determinadas características.

Tipos de informes

Cytomic EPDR permite generar 3 tipos de documentos, cada uno de ellos con sus características asociadas:

- Vistas de listados
- Informes ejecutivos
- Listados de dispositivos

A continuación se resumen las características de cada tipo de informe:

Tipo	Intervalo	Envío	Contenido	Salida
Vistas de listados	Instantáneo	Automático	Configurable mediante búsquedas	csv
Informes ejecutivos	Consolidado	Automático y bajo demanda	Configurable por categorías y por grupos	pdf,csv, excel, word
Listados de dispositivos	Instantáneo	Automático	Configurable mediante filtros	csv

Tabla 22.1: resumen de tipos de informes y sus características

Requisitos para generar informes

Los usuarios con el rol de solo lectura podrán previsualizar los informes ejecutivos pero no podrán programar el envío de nuevos informes.

A continuación se detallan las tareas previas que el administrador deberá realizar antes de poder utilizar la funcionalidad de envío de informes y listados programados.

Vistas de listados

El administrador deberá de crear previamente una vista y configurar las herramientas de búsqueda hasta que el listado muestre la información que considere relevante. Una vez hecho esto podrá crear un envío programado. Consulta el apartado "**Gestión de listados**" en la página **57**. para obtener información de cómo crear vistas de listados con búsquedas asociadas.

Informes ejecutivos

No es necesaria la ejecución de ninguna tarea previa: su contenido se determina en el momento de configurar el envío programado.

Listado de dispositivos filtrado

El administrador deberá crear un filtro o utilizar uno de los filtros ya creados en Cytomic EPDR. Consulta el apartado "**Árbol de filtros**" en la página **152** para obtener más información acerca del manejo y configuración de los filtros.

Acceso al envío de informes y listados

Desde la sección Envíos programados

Para acceder al listado de tareas que envían informes y listados haz clic en el menú superior **Estado**, panel lateral **Envíos programados.** Se mostrará una pantalla con las herramientas necesarias para buscar tareas de envío ya creadas, editarlas, borrarlas o crear nuevas.

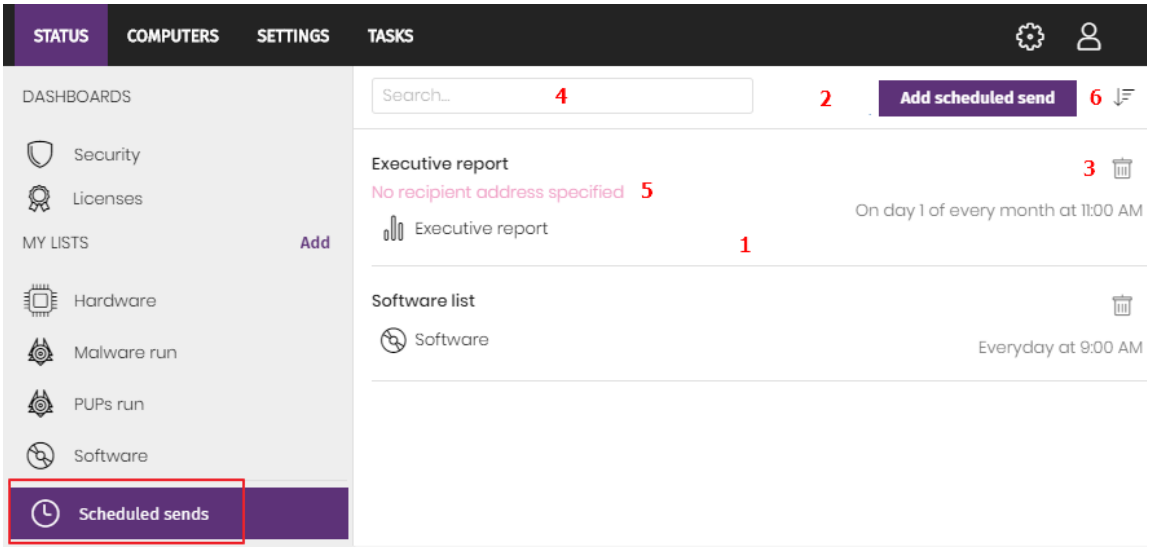


Figura 22.1: ventana para gestionar los envíos programados

Desde una vista de listado

Las vistas de listados se almacenan en el panel lateral izquierda del menú superior **Estado**, y cada una de ellas puede enviarse de forma programada siguiendo los pasos mostrados a continuación:

- **Desde el menú de contexto**: haz clic en el menú de contexto de la vista de listado y en la opción **Programar envío** . Se mostrará la ventana de información requerida explicada en el apartado "**Información requerida para el envío de informes y listados**".
- **Desde la propia vista del listado**: haz clic en el icono situado en la esquina superior derecha de la ventana. Se mostrará la ventana de información requerida explicada en el apartado "**Información requerida para el envío de informes y listados**".

Al completarse la creación del envío programado se mostrará un mensaje emergente en la esquina superior derecha de la pantalla indicado la generación de una nueva tarea de envío.

Desde un filtro

- En el menú superior **Equipos** haz clic en la pestaña para mostrar el árbol de filtros.
- Al hacer clic en un filtro, el listado de dispositivos se actualizará para mostrar los dispositivos cuyos atributos satisfagan las condiciones impuestas por el filtro seleccionado.
- Haz clic en el icono del menú de contexto asociado al filtro y selecciona la opción **Programar**

envío. Se mostrará la ventana de información requerida explicada en el apartado "**Información requerida para el envío de informes y listados**".

Al completarse la creación del envío programado se mostrará un mensaje emergente en la esquina superior derecha de la pantalla indicado la generación de una nueva tarea de envío.

Al completarse la creación del envío programado se mostrará un mensaje emergente en la esquina superior o inferior derecha de la pantalla indicado la generación de una nueva tarea de envío y un enlace para ver el listado de envíos programados. Consulta el apartado "**Listado de envíos programados**".

Gestión de informes

Para crear, borrar, editar y listar envíos programados haz clic en el menú superior **Estado** y en el menú lateral **Envíos programados**.

Listado de envíos programados

En el panel de la derecha se muestran los envíos programados ya creados **(Figura 22.1 1)**.

Todas las tareas de envío incluye un nombre y debajo una serie de mensajes que indican si faltan datos por indicar en la configuración del envío programado **(Figura 22.1 5).**

Crear envíos programados

Haz clic sobre el botón **Añadir envío programado (Figura 22.1 2)** para mostrar la ventana de configuración.

Consulta el apartado "**Información requerida para el envío de informes y listados**" para obtener información sobre los datos que el administrador debe aportar al crear un envío programado.

Ordenar envíos programados

Haz clic en el icono **(6)** para desplegar un menú de contexto con las opciones de ordenación disponibles:

- Ordenado por fecha de creación
- Ordenado por nombre
- Ascendente
- Descendente

Borrar y editar envíos programados

Para borrar y editar un envío programado sigue los pasos mostrados a continuación:

- Para borrar un envío programado utiliza el icono **(Figura 22.1 3)**.

- Haz clic en el nombre del envío programado para editarlo.

Una vista de listado o listado filtrado que tenga configurado un envío programado no podrá borrarse hasta que el envío programado sea eliminado.

Los listados enviados por un envío programado se corresponden a una vista de listado o a un listado filtrado concretos. Si éstos son modificados, el envío programado se actualizará con la nueva configuración.

Información requerida para el envío de informes y listados

Campo	Descripción
Nombre	Nombre de la entrada que se mostrará en el listado de envíos programados.
Enviar automáticamente	Frecuencia de envío del informe o listado: • **Todos los días**: el envío se producirá todos los días a la hora seleccionada. • **Todas la semanas**: el envío se producirá todos las semanas a la hora y día de la semana seleccionados. • **Todos los meses**: el envío se producirá todos los meses en el día del mes y hora seleccionados.
Tipo de informe	Tipo de informe que se enviará: • Informe ejecutivo • Vista de listado • Listado de dispositivos
Previsualizar informe	Este enlace solo se muestra cuando el tipo de informe elegido es Informe ejecutivo. Al hacer clic se abrirá una nueva pestaña en el navegador con el contenido del informe para previsualizarlo antes de configurar su envío programado, descargarlo o imprimirlo mediante la barra de herramientas superior. Para los listados el formato elegido es csv y por lo tanto la opción de previsualizar no estará disponible.
Fechas	Intervalo de tiempo que abarca el informe. • Último año • Último mes • Últimos 7 días • Últimas 24 horas Este campo solo se muestra cuando el tipo de informe es Informe ejecutivo. En los listados se incluyen datos pertenecientes al momento en el que se generan.
Equipos	De qué equipos se extraen datos para generar el informe ejecutivo: • **Todos los equipos.** • **Los grupos seleccionados**: muestra el árbol de grupos para seleccionar de forma individual los grupos mediante las casillas de selección. Este campo solo está disponible cuando el tipo de informa es Informe ejecutivo.
Para	Direcciones de correo separadas por comas que recibirán el informe.
CC	Direcciones de correo en copia separadas por comas que reciben el informe.

Tabla 22.2: información para generar informes bajo demanda

Campo	Descripción
CCO	Direcciones de correo en copia oculta separadas por comas que recibirán el informe.
Asunto	Frase resumen que describe el correo.
Formato	• **Para vistas de listado**: adjunta un fichero en formato csv al correo. • **Para informes ejecutivos**: formato (Pdf, Excel, Word) del fichero adjunto al correo electrónico que contiene el informe.
Idioma	Idioma en el que se envía el informe.
Contenido	Tipo de información que incluye el informe: • **Tabla de contenidos:** índice de los distintos apartados dentro del informe. • **Estado de licencias**: muestra la información de las licencias contratadas, consumidas y su fecha de caducidad. Consulta el apartado "**Visualizar las licencias contratadas**" en la página **136**. • **Estado de seguridad**: funcionamiento del software Cytomic EPDR en los equipos de la red donde ha sido instalado. • **Detecciones**: muestra las amenazas detectadas en la red. • **Acceso web y Spam**: muestra la actividad web de los usuarios. Consulta el apartado "**Paneles / Widgets de seguridad**" en la página **380**. • **Gestión de parches**: muestra el estado del parcheo de los equipos. Consulta el apartado "**Paneles / widgets en Cytomic Patch**" en la página **321**. • **Cifrado**: muestra el estado del cifrado en los equipos de la red. Consulta el apartado "**Paneles / widgets en Cytomic Encryption**" en la página **360**.

Tabla 22.2: información para generar informes bajo demanda

Contenido de los informes y listados

Vistas de listados

El contenido de los listados enviados equivale a la opción **Exportar** de una vista de listado, y contiene el fichero csv correspondiente al listado elegido. Consulta el apartado "**Gestión de listados**" en la página **57** para obtener información sobre los tipos de listados disponibles en Cytomic EPDR y su contenido.

El listado incluirá los equipos visibles para la cuenta de usuario que modificó por última vez el envío programado.

Listados de dispositivos

El contenido del informe enviado se corresponde con el listado de dispositivos filtrados por un criterio. Consulta el apartado "**Listado de equipos**" en la página **165** para obtener información sobre el

contenido del fichero csv enviado y el apartado "**Árbol de filtros**" en la página **152** para obtener información acerca del manejo y configuración de los filtros.

Informe ejecutivo

Dependiendo de la configuración establecida en el campo **Contenido,** el informe ejecutivo contendrá los datos mostrados a continuación:

Campo	Descripción
Tabla de contenidos	Muestra un índice con enlaces a las distintas secciones incluidas en el informe ejecutivo.
Contenido	Tipo de información que incluye el informe: • **Estado de licencias**: muestra la información de las licencias contratadas, consumidas y su fecha de caducidad. Consulta el apartado "**Visualizar las licencias contratadas**" en la página **136**. • **Estado de seguridad la red**: funcionamiento de software Cytomic EPDR en los equipos de la red donde ha sido instalado. Incluye el widget **Estado de protección** e información sobre los **Equipos conectados**, **Protecciones actualizado** y **Conocimiento actualizado**. • **Detecciones**: muestra las amenazas detectadas en la red. Incluye los widgets y listados mostrados a continuación: ◦ Clasificación de todos los programas ejecutados y analizados ◦ Equipos con más detecciones (top 10) ◦ Actividad del malware ◦ Actividad de PUPs ◦ Actividad de exploits ◦ Últimas detecciones de malware ◦ Últimas detecciones de PUPs ◦ Últimas detecciones de exploits ◦ Amenazas detectadas por el antivirus ◦ Filtrado de contenidos en Exchange servers • **Acceso web y Spam**: muestra la actividad web de los usuarios. Incluye los widgets: ◦ **Accesos a páginas web** ◦ **Categorías más accedidas (Top 10)** ◦ **Categorías más accedidas por equipo (Top 10)**

Tabla 22.3: contenido del informe ejecutivo

Campo	Descripción
	• **Categorías más bloqueadas (Top 10)** • **Categorías más bloqueadas por equipo (Top 10)** • **Spam detectado en Exchange Server**. Consulta el apartado "**Paneles / Widgets de seguridad**" en la página **380**. • **Gestión de parches**: muestra el estado del parcheo de los equipos. Incluye los widgets y listados mostrados a continuación: • **Estado de gestión de parches.** • **Equipos con más parches disponibles (top 10)**: listado de los 10 equipos de la red que tiene más parches disponibles sin instalar agrupados por su tipo: parches de seguridad, parches no de seguridad y Service Packs. • **Parches más críticos (top 10)**. listado de los 10 parches más críticos ordenado por el número de equipos afectados. Consulta el apartado "**Paneles / widgets en Cytomic Patch**" en la página **321** • **Data Control**: muestra el estado del despliegue de Cytomic Data Watch y los equipos con mayor cantidad de ficheros PII detectados en la red. • **Estado del despliegue de Data Control**: indica el estado de las licencias del módulo y las funcionalidades activadas en los equipos de la red. • **Archivos por tipo de información personal**: muestra el número de archivos PII encontrados por cada tipo de entidad soportada en el último inventario diario generado. • **Equipos por información personal**: muestra el número de equipos con archivos PII encontrados en la red por cada tipo de entidad soportada en el último inventario diario generado. • **Equipos con más archivos con información personal (top 10)**: muestra los equipos que contienen el mayor número de ficheros PII en la red. Consulta el apartado "**Paneles / widgets en Cytomic Data Watch**" en la página **277** • **Cifrado**: muestra el estado del cifrado de los equipos. Incluye los widgets y listados mostrados a continuación: • **Estado del cifrado** • **Equipos compatibles con cifrado** • **Equipos cifrados** • **Método de autenticación aplicado**

Tabla 22.3: contenido del informe ejecutivo

Campo	Descripción
	• **Últimos equipos cifrados:** listado de los 10 equipos que han sido cifrados recientemente por Cytomic Encryption, ordenados por 'Fecha de cifrado'. Cada linea del listado contiene el nombre del equipo, grupo al que pertenece, sistema operativo instalado, método de autenticación configurado y fecha de cifrado. Consulta el apartado "**Paneles / widgets en Cytomic Encryption**" en la página **360**.

Tabla 22.3: contenido del informe ejecutivo

Parte 7

Resolución de incidencias de seguridad

Capítulo 23: Herramientas de resolución

Capítulo 24: Tareas

Capítulo 23

Herramientas de resolución

Cytomic EPDR cuenta con varias herramientas de resolución que permiten al administrador solucionar los problemas encontrados en las fases de Protección, Detección y Monitorización del ciclo de protección adaptativa. Algunas de estas herramientas son automáticas y no necesitan que el administrador intervenga, otras sin embargo requieren la ejecución de acciones concretas a través de la consola Web.

La tabla **23.1** muestra las herramientas disponibles por plataforma y sus características.

Herramienta de resolución	Plataforma	Tipo	Acción
Análisis y desinfección automático de equipos	Windows, macOS, Linux, Android	Automático	Detecta y desinfecta el malware cuando se registra un movimiento en el sistema de ficheros (copia, movimiento, ejecución) o en un vector de infección soportado.
Análisis y desinfección bajo demanda de equipos	Windows, macOS, Linux, Android	Automático (Programado) / Manual	Detecta y desinfecta el malware en el sistema de ficheros cuando lo requiera el administrador: en franjas horarias concretas o cuando cree la tarea de resolución.
Reinicio bajo demanda	Windows	Manual	Fuerza un reinicio del equipo para aplicar actualizaciones, completar desinfecciones manuales y corregir errores detectados en la protección.
Aislamiento de equipos	Windows	Manual	Aísla el equipo de la red, impidiendo la extracción de información confidencial y la propagación de la amenaza a los equipos vecinos.

Tabla 23.1: herramientas de resolución disponibles en Cytomic EPDR

CONTENIDO DEL CAPÍTULO

Análisis y desinfección automática de equipos

Los módulos de protección Cytomic EPDR detecta y desinfecta de forma automática las amenazas encontradas en los equipos protegidos y recibidas en los siguientes vectores de infección:

> *La desinfección automática no requiere de la intervención del administrador, si bien es necesario que esté seleccionada la casilla **Protección de archivos** en la configuración de seguridad asignada al equipo. Consulta el capítulo "**Configuración de estaciones y servidores**" en la página **225** para más información sobre los modos de bloqueo y las configuraciones disponibles en el módulo antivirus de Cytomic EPDR.*

- **Protección avanzada**: bloquea la ejecución del malware desconocido.
- **Web**: malware que se recibe mediante una descarga producida por el navegador web.
- **Correo**: malware que se recibe como adjunto de un correo en el cliente instalado en el equipo.
- **Sistema de ficheros**: cuando se ejecuta, se mueve o se copia un fichero que contiene una amenaza conocida o desconocida y reside en el sistema de almacenamiento del equipo.
- **Red**: intentos de intrusión recibidos por la red y bloqueados por el cortafuegos.
- **Protección Exchange**: detección de malware y spam recibidos en los buzones del servidor de correo.

Ante la detección de una amenaza conocida, Cytomic EPDR desinfecta de forma automática los elementos afectados siempre y cuando exista un método de desinfección conocido. En su defecto, el elemento se moverá a cuarentena.

Comportamiento según la configuración de la protección

Si los módulos de antivirus y protección avanzada están activados, Cytomic EPDR ejecutará las acciones mostradas a continuación en el orden indicado:

Modo de protección avanzada	Protección antivirus	Comportamiento
Audit	Activado	Detección, Desinfección o Cuarentena.
Hardening, Lock	Activado	Detección, Bloqueo de desconocidos, Desinfección o Cuarentena.
Audit	Desactivado	Detección.
Hardening, Lock	Desactivado	Detección, Bloqueo de desconocidos.

Tabla 23.2: comportamiento del producto frente a las amenazas según la configuración del motor Protección avanzada y Protección antivirus

Análisis y desinfección bajo demanda de equipos

*Consulta el capítulo "**Tareas**" en la página **503** para obtener información sobre la gestión de tareas ejecutadas en los equipos y servidores de la red, como visualizar sus resultados y cómo modificar sus parámetros configurados.*

Para analizar y desinfectar bajo demanda un equipo se ofrecen dos posibilidades:

- Mediante la creación de tareas de análisis programadas.
- Mediante un análisis inmediato.

Crear tareas desde el Árbol de equipos

El árbol de equipos permite definir de forma rápida tareas de análisis para grupos completos de equipos.

- Haz clic en el menú superior **Equipos** y en el panel lateral haz clic en el botón para elegir la vista carpetas del Árbol de equipos.
- Dentro del árbol de equipos haz clic en el menú de contexto asociado al grupo de equipos destinatario de la tarea de análisis. Se mostrará el menú contextual de la rama del árbol elegida.
- En el menú contextual haz clic en una de las dos opciones:
  - **Analizar ahora**: crea una tarea con destinatario el grupo de equipos elegido, para su ejecución inmediata.
  - **Programar análisis**: muestra la zona **Tareas** para crear una nueva tarea repetida en el tiempo y / o aplazada. La plantilla de tarea estará parcialmente completada: el campo **Destinatarios** incluye el grupo elegido en el Árbol de Equipos. Completa el resto de la configuración tal y como se describe en el apartado "**Crear tareas desde la zona Tareas**" en la página **504**.

Tareas inmediatas

Las tareas inmediatas (entrada **Analizar ahora** del menú de contexto) tienen las siguientes características:

- Permiten elegir el tipo de análisis (**Todo el ordenador** o **Áreas críticas**). Consulta el punto "**Programación horaria y repetición de la tarea**" en la página **505** para obtener más información.
- **No requieren especificar el momento de ejecución ni la repetición**: son tareas puntuales que se ejecutan en el momento de su definición.
- **No requieren la publicación de la tarea**: Cytomic EPDR publica de forma automática estas tareas.

Para informar del éxito o fracaso en la creación de la tarea inmediata se muestra un mensaje emergente en la consola de administración.

Tareas programadas

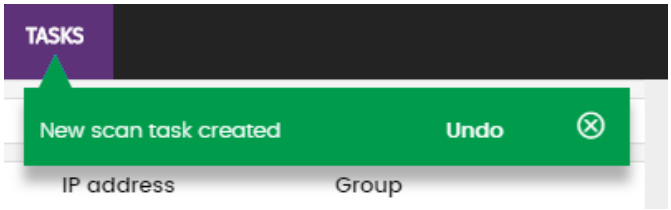


Figura 23.1: mensaje emergente de creación de una nueva tarea de análisis

Las tareas programadas (entrada **Programar análisis** en el menú de contexto) son idénticas a las tareas creadas desde la zona **Tareas** y mostradas en el apartado "**Crear tareas desde la zona Tareas**" en la página **504**, si bien el campo destinatarios aparece completado con el grupo del Árbol de equipos seleccionado. Por lo tanto, es necesario indicar el momento de ejecución de la tarea, la repetición y publicar la tarea para su activación.

Crear tareas desde el listado de equipos

La zona **Equipos** permite crear tareas de forma similar al árbol de equipos o la zona **Tareas**. En este caso, puedes elegir de forma independiente equipos que pertenecen a un mismo grupo o subgrupos.

Según sea del número de equipos destinatarios de la tarea, elige uno de los dos recursos mostrados a continuación:

- **Menú de contexto asociado al equipo**: un único equipo destinatario.
- **Casillas de selección y barra de acciones**: uno o varios equipos pertenecientes a un grupo o

subgrupos.

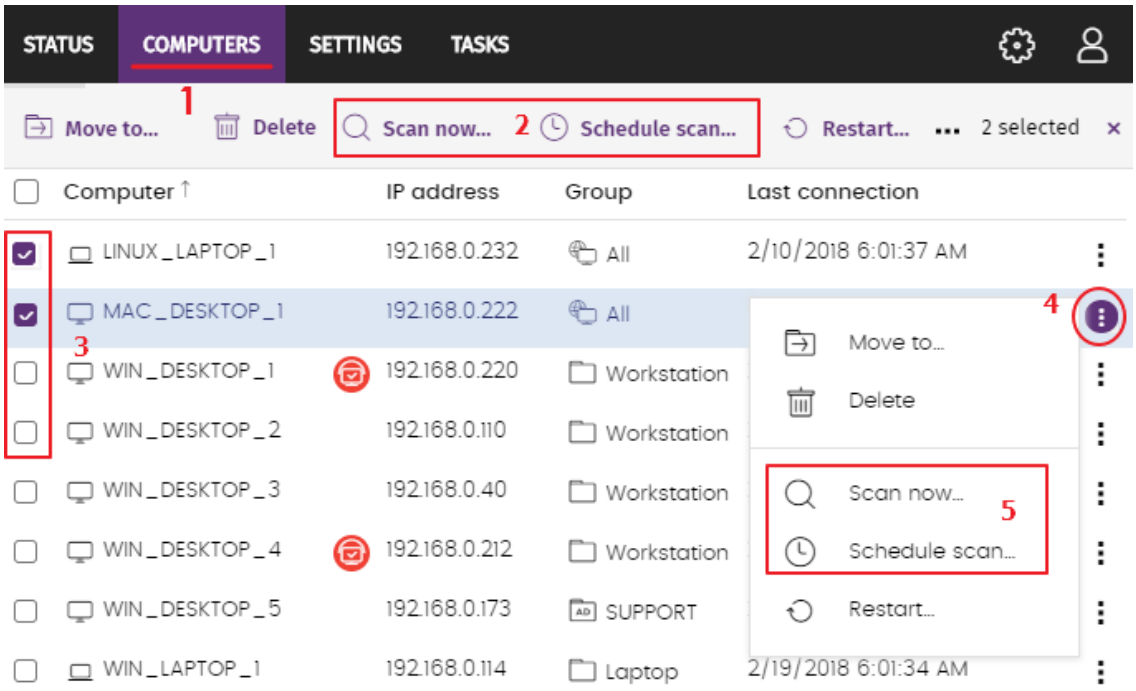


Figura 23.2: menús de contexto y barra de acciones disponibles para la creación rápida de tareas

Menú de contexto asociado al equipo

- Haz clic en el menú superior Equipos **(1)** y elige el grupo del Árbol de equipos al que pertenece el equipo a analizar.
- En el listado de equipos haz clic en el menú de contexto del equipo destinatario de la tarea de análisis. **(4)**
- En el menú de contexto haz clic en una de las dos ramas **(5)**:
  - **Analizar ahora**: crea una tarea con destinatario el equipo elegido para ejecutarse inmediatamente.
  - **Programar análisis**: muestra la zona **Tareas** con una plantilla de tarea parcialmente completada. En el campo destinatarios se incluye el equipo elegido. Completa el resto de la configuración tal y como se describe en el punto "**Crear tareas desde la zona Tareas**" en la página **504**.

Casillas de selección y la barra de acciones

- Haz clic en el menú superior **Equipos (1)** y elige el grupo del árbol de equipos al que pertenece el equipo o equipos a analizar.
- Selecciona los equipos destinatarios de la tarea con las casillas de verificación **(3)**. Se mostrará la barra de acciones **(2)** en la parte superior de la ventana.
- Haz clic en uno de los dos iconos:
  - **Analizar ahora** : crea una tarea con destinatario el grupo de equipos elegido para ejecutarse

inmediatamente.

- **Programar análisis**: muestra la zona **Tareas** con una plantilla de tarea parcialmente completada. En el campo destinatarios se incluye el grupo elegido en el **Árbol de Equipos**. Completa el resto de la configuración tal y como se describe en el apartado "**Crear tareas desde la zona Tareas**" en la página **504**.

Opciones de análisis

Las opciones de análisis configuran los parámetros del motor de antivirus a la hora de escanear el sistema de ficheros de los equipos:

Valor	Descripción
Tipo de análisis	• **Todo el ordenador**: análisis profundo del equipo incluyendo a todos los dispositivos de almacenamiento conectados. • **Áreas críticas**: análisis rápido del equipo que incluye: • `%WinDir%\system32` • `%WinDir%\SysWow64` • Memoria • Sistema de arranque • Cookies • **Elementos específicos**: indica las rutas de los dispositivos de almacenamiento masivo que se analizarán. Se admite el uso de variables de entorno. Se analizará la ruta indicada y todas las carpetas y ficheros que cuelguen de ella.
Detectar virus	Detecta los programas que se introducen en los ordenadores y producen efectos nocivos. Esta opción está siempre activada.
Detectar herramientas de hacking y PUPs	Detecta los programas utilizados por los hackers para causar perjuicios a los usuarios de un ordenador y los programas potencialmente no deseados.
Detectar archivos sospechosos	En los análisis programados el software del equipo se analiza de forma estática, si llegar a ejecutarlo. Esto reduce las posibilidades de detectar ciertos tipos de amenazas. Para mejorar el ratio de detección de este tipo de análisis, activa los algoritmos heurísticos.
Analizar archivos comprimidos	Descomprime y analiza los archivos empaquetados.

Tabla 23.3: opciones de análisis

Valor	Descripción
Excluir del análisis los siguientes archivos	• **No analizar los archivos excluidos para las protecciones permanentes**: los archivos que el administrador ha marcado para permitir su ejecución no serán analizados, junto a los archivos ya excluidos de forma global en la consola. • **Extensiones**: introduce las extensiones de los archivos que no se analizarán separados por comas. • **Archivos**: introduce el nombre de los archivos que no se analizarán separados por comas. • **Directorios**: introduce el nombre de las carpetas que no se analizarán separados por comas.

Tabla 23.3: opciones de análisis

Reiniciar equipos

Para mantener los equipos actualizados a la última versión de la protección, o si se detecta algún error en la protección, el administrador puede reiniciar los equipos involucrados desde la consola web:

- Selecciona el menú superior **Equipos** y localiza el equipo desde el panel de equipos situado a la derecha.
  - **Para reiniciar un único equipo**: selecciona el menú de contexto del equipo en el listado de equipos.
  - **Para reiniciar varios equipos**: mediante las casillas de selección, marca los equipos que quieres reiniciar y haz clic en el icono de la barra de acciones.

Para los equipos que estén apagados Cytomic EPDR guardará la orden de reinicio hasta 7 días, momento en el cual si el equipo no se ha iniciado se desechará.

Aislar un equipo

Cytomic EPDR aísla bajo demanda los equipos de la red para evitar la propagación de las amenazas y la comunicación y extracción de información confidencial.

Aislar equipos funciona en puestos de trabajo y servidores Windows. Los equipos Linux, macOS y Android son incompatibles con esta tecnología.

Cuando un equipo está aislado, sus comunicaciones quedan restringidas al acceso al equipo desde la consola para que el administrador pueda analizar el problema y resolverlo mediante las herramientas suministradas por Cytomic EDR.

El resto de productos y servicios instalados en el equipo de usuario o servidor dejarán de poder comunicarse por red a no ser que el administrador establezca excepciones. Consulta el apartado "**Opciones avanzadas de aislamiento: exclusión de programas**".

Estados de los equipos aislados

Las operaciones **Aislar un equipo** y **Dejar de Aislar un equipo** se ejecutan en tiempo real, pero el proceso puede retrasarse si el equipo no está conectado a Internet. Para reflejar su situación exacta, Cytomic EPDR distingue los 4 estados a través de los iconos mostrados a continuación:

- **Aislando**  : el administrador lanzó una petición para aislar uno o más equipos y se está procesando.
- **Aislado**  : el proceso de aislamiento se completó y el equipo tiene restringidas sus comunicaciones.
- **Dejando de aislar**  : el administrador lanzó una petición para dejar de aislar uno o más equipos y se está procesando.
- **No aislado**: el proceso para retirar el aislamiento del equipo se completó. Las comunicaciones se permiten acorde la configuración definida en otros módulos (firewall, IDS), productos, o en el propio sistema operativo.

Estos iconos acompañan a la columna dirección IP en los listados de **Licencias**, **Estado de la protección** y en la zona **Equipos**.

Aislar uno o varios equipos de la red de la organización

Para aislar uno o varios equipos de la red:

- Haz clic en el menú superior **Equipos** o elige uno de los siguientes listados de equipos:
  - Listado **Estado de protección**.
  - Listado **Licencias**.
- Indica los equipos a aislar con las casillas de selección.
- En la barra de acciones selecciona **Aislar un equipo**. Se mostrará una ventana con un link a **Opciones avanzadas**.
- En **Opciones avanzadas** indica los programas que se seguirán comunicando con el resto de la red a pesar del aislamiento del equipo (exclusión de aislamiento).
- Haz clic en el botón **Aceptar**. El equipo cambiará de estado a **Intentando aislar el equipo**.
- Para aislar un grupo de equipos:

- Haz clic en el menú superior **Equipos**.
- En el Árbol de equipos haz clic en la vista de carpetas y selecciona el grupo a aislar.
- En el menú de contexto selecciona la entrada **Aislar equipos** y haz clic en el botón **Aceptar**.
- Para aislar todos los equipos de la red despliega el menú de contexto del nodo **Todos**.

Quitar el aislamiento de un equipo

- Sigue los pasos indicados en el punto "**Aislar uno o varios equipos de la red de la organización**".
- En la barra de acciones selecciona **Dejar de aislar un equipo**.
- El equipo cambiará de estado a **Intentando dejar de aislar el equipo**.

Opciones avanzadas de aislamiento: exclusión de programas

Al aislar un equipo, solo se permite la comunicación de los procesos correspondientes a los productos de Cytomic. El resto de procesos, incluyendo a los programas de usuario, no podrán comunicarse con los equipos de la organización. Para excluir a ciertos programas de este comportamiento y permitir al usuario seguir utilizando el equipo en cierta medida o poder utilizar determinadas aplicaciones que ayuden al administrador a diagnosticar y resolver el problema, utiliza el link **Opciones avanzadas** de la ventana flotante mostrada al aislar un equipo.

La caja de texto indica los programas a excluir del aislamiento. Estos programas podrán comunicarse con libertad con el resto de equipos de la organización o con el exterior, según indique la configuración del resto de módulos de Cytomic EPDR, de otros productos instalados en el equipo, o del cortafuegos del sistema operativo.

Para acelerar la configuración, la consola de administración retiene la última configuración de procesos excluidos del aislamiento introducida por el administrador. De esta manera, en la caja de texto de un equipo excluido no se mostrará su configuración especifica de procesos excluidos, sino la última configuración que utilizó el administrador en cualquier otro equipo.

Comunicaciones permitidas y denegadas de un equipo aislado

Cytomic EPDR deniega todas las comunicaciones en un equipo aislado excepto las necesarias para poder realizar un análisis forense remoto y utilizar las herramientas de resolución implantadas en Cytomic EPDR. A continuación, se indican las comunicaciones permitidas y denegadas.

Procesos y servicios permitidos en un equipo aislado

- Procesos de sistema:
  - Los servicios necesarios para formar parte de la red corporativa: obtención de IP por DHCP, ARP, nombre de equipo por WINS, DNS etc.
- Procesos de Cytomic EPDR:

- Comunicación con el Gateway por defecto.
- Comunicación con la nube de Cytomic para el funcionamiento de los motores de protección, descarga de ficheros de firmas y administración remota mediante la consola web.
- Descubrimiento de equipos en máquinas aisladas con el rol de descubridor asignado.
- Servidor de ficheros en una máquina aislada con el rol de caché asignado.
- Proxy de conexiones en una máquina con el rol de proxy Cytomic asignado.

Comunicaciones bloqueadas en un equipo aislado

Todas las comunicaciones que no estén incluidas en el punto anterior son denegadas, entre ellas:

- Conexión con el servicio Windows Update del sistema operativo.
- Navegación web, ftp, correo y otros protocolos de Internet.
- Transferencia de ficheros por SMB entre los PCs de la red.
- Instalación remota de equipos con Cytomic EPDR.

Notificar un problema

En algunas ocasiones es posible que el software Cytomic EPDR instalado en los equipos de la red presente un mal funcionamiento. Algunos de los síntomas pueden ser:

- Fallos en el reporte del estado del equipo.
- Fallos en la descarga de conocimiento o de las actualizaciones del motor.
- Motor de protección en estado de error.

Si Cytomic EPDR presenta un mal funcionamiento en alguno de los equipos de la red, es posible contactar con el departamento de soporte de Cytomic a través de la consola y enviar de forma automatizada toda la información necesaria para efectuar un diagnóstico. Para ello haz clic en el menú superior Equipos, selecciona el equipo que presente errores y haz clic en el menú de contexto. Se desplegará un menú con la opción Indícanos el problema.

Permitir el acceso externo a la consola Web

Para aquellos problemas que el administrador de la red no pueda resolver, existe la posibilidad de habilitar el acceso a la consola únicamente para equipo de soporte de Cytomic:

- Haz clic en el menú superior **Configuración**, panel lateral **Usuarios**.
- En la pestaña usuarios haz clic en el control **Permitir al equipo de Cytomic (Panda Security) acceder a mi consola**.

Capítulo 24

Tareas

Una tarea es un recurso implementado en Cytomic EPDR que permite enlazar un proceso a dos variables adicionales: repetición y aplazamiento de la acción.

- **Repetición**: configura la tarea para su ejecución de forma puntual o repetida a lo largo del tiempo.
- **Aplazamiento**: configura la tarea para ser ejecutada en el momento en que se define (tarea inmediata), o aplazado en el tiempo (tarea programada).

CONTENIDO DEL CAPÍTULO

Proceso general de lanzamiento de tareas

Se divide en tres pasos:

- **Creación y configuración de la tarea**: se determinan los equipos afectados, las características de la tarea, el momento en que será lanzado, el número de veces que se ejecutará y el comportamiento en caso de error.
- **Publicación de la tarea una vez creada**: las tareas creadas se introducen en el programador de tareas de Cytomic EPDR para ser lanzadas en el momento marcado por su configuración.
- **Ejecución de la tarea** cuando se alcancen las condiciones especificadas en su definición.

Introducción a la creación de tareas

Dependiendo de la necesidad de configurar todos los parámetros de una tarea, ésta se puede establecer desde varios lugares dentro de la consola:

- Zona de Tareas
- Árbol de equipos
- Zona Equipos
- Listados

El recurso principal para crear una tarea es la zona **Tareas** del menú superior de la consola. En esta ventana se definen las tareas desde cero, controlando todos los aspectos del proceso (destinatarios, aplazamiento, repetición, publicación etc.)

La zona **Equipos**, el Árbol de equipos y los listados permiten programar y lanzar tareas de forma ágil, sin necesidad de pasar por todo el proceso de configuración y publicación de la tarea, si bien se pierde algo de flexibilidad en su definición.

Crear tareas desde la zona Tareas

Para crear una nueva tarea, desde el menú superior haz clic en **Tareas**. Accederás a una ventana donde están listadas todas las tareas creadas, indicando su estado. Para crear una tarea nueva haz clic en el botón **Añadir** y elige el tipo de tarea en el desplegable; se mostrará una ventana con los datos de la tarea, distribuidos en varias zonas:

- **Información general**: nombre de la tarea y descripción.
- **Destinatarios**: equipos que recibirán la tarea.
- **Programación**: configuración del momento en que se lanzará la tarea.

Destinatarios de la tarea

- Haz clic en el link **Destinatarios** (**No se ha asignado a ningún equipo**) para abrir una nueva ventana donde seleccionar los equipos que recibirán la tarea configurada.
- Haz clic en el botón ⊕ para agregar un nuevo equipo y en el botón 🗑 para eliminar los equipos

seleccionados.

> *Para acceder a la ventana de selección de equipos es necesario salvar previamente la tarea. Si la tarea no ha sido salvada se mostrará una ventana de advertencia.*

- Haz clic en el botón **Ver equipos** para abrir la zona **Equipos** filtrada por **Antimalware Scan - Scheduled task** donde se mostrarán todos los equipos seleccionados que recibirán la tarea.

Programación horaria y repetición de la tarea

Se establece mediante tres parámetros:

- **Empieza**: marca el comienzo de la tarea.
- **Tiempo máximo de ejecución**: indica el tiempo máximo que la tarea puede tardar en completarse. Una vez vencido la tarea se cancela con error si no ha terminado.
- **Repetir**: establece cada cuanto tiempo la tarea se vuelve a activar, tomando como referencia la fecha indicada en **Empieza**.

- **Empieza**

Valor	Descripción
Lo antes posible (activado)	La tarea se lanza en el momento si el equipo está disponible (encendido y accesible desde la nube), o en el momento en que se encuentre disponible dentro del margen definido en el desplegable **Equipo apagado.**
Lo antes posible (desactivado)	La tarea se lanza en la fecha seleccionada en el calendario, indicando si se tiene en cuenta la hora del equipo o la hora del servidor Cytomic EPDR.
Equipo apagado	Si el equipo está apagado o inaccesible, la tarea no se podrá lanzar. El sistema de programación de tareas permite establecer la caducidad de la tarea, retrasando su lanzamiento el intervalo de tiempo definido por el usuario, desde 0 (la tarea caduca de forma inmediata si el equipo no está disponible) a infinitivo (la tarea siempre está activa y se espera a que el equipo esté disponible de forma indefinida): • **No ejecutar**: la tarea se cancela si en el momento del lanzamiento el equipo no está encendido. • **Dar un margen de**: permite definir un intervalo de tiempo dentro del cual, si el equipo inicialmente no estaba disponible y vuelve a estarlo, la tarea será lanzada. • **Ejecutar cuando se encienda**: no establece ningún intervalo de tiempo, espera de forma indefinida a que el equipo esté accesible para lanzar la tarea.

Tabla 24.1: comportamiento del inicio de la tarea si el equipo no esta disponible

- **Tiempo máximo de ejecución**

Valor	Descripción
Sin límite	La duración de la ejecución de la tarea no está definida, pudiéndose extenderse hasta el infinito.
1,2, 8 o 24 horas	La duración de la ejecución de la tarea está acotada. Transcurrido el tiempo indicado, la tarea se cancela con error si no ha terminado previamente.
Repetir	Establece un intervalo de repetición cada día, semana mes o año tomando como referencia la fecha indicada en **Empieza.**

Tabla 24.2: configuración de la duración de la tarea

Publicar tareas

Una vez creada y configurada, la tarea aparecerá en el listado de tareas configuradas, pero no estará activada hasta su publicación.

Haz clic en el botón **Publicar ahora** para publicar una tarea e introducirla en el programador de tareas de Cytomic EPDR, encargado de marcar el momento en que se lanzan las tareas según su configuración.

Gestionar tareas

Haz clic en el menú superior **Tareas** para listar, borrar, copiar, cancelar o visualizar los resultados de las tareas creadas.

Listado de tareas creadas

Este listado muestra en detalle todas las tareas creadas, su tipo, estado y otra información relevante.

Campo	Comentario	Valores
Icono	Tipo de la tarea	• Tarea de tipo instalación o desinstalación de parches • Tarea de tipo análisis bajo demanda • Tarea de tipo desinfección
Nombre	Nombre de la tarea creada	Cadena de caracteres
Fecha	Fecha de creación de la tarea	Fecha

Tabla 24.3: campos del listado Tareas creadas

Campo	Comentario	Valores
Estado	• **Pendiente**: la tarea se intentó iniciar, pero la máquina no estaba disponible en ese momento. Se establece un periodo de espera según su configuración. • **En progreso**: la tarea se está ejecutando en este momento. • **Con éxito**: la tarea terminó con éxito. • **Fallida**: la tarea terminó con error. • **Expirada**: la tarea no llegó a comenzar por haber expirado el plazo configurado. • **Cancelada**: la tarea fue cancelada de forma manual.	Cadena de caracteres

Tabla 24.3: campos del listado Tareas creadas

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de tarea	Clase de la tarea	• Análisis • Desinfección • Instalación de parches • Desinstalación de parches • Todos
Buscar tarea	Nombre de la tarea	Cadena de caracteres
Programación	Frecuencia de la repetición de la tarea	• Todos • Inmediata • Una vez • Programada
Ordenar listado	Criterio de ordenación de las tareas creadas.	• Ordenar por fecha de creación • Ordenar por nombre • Ascendente • Descendente

Tabla 24.4: campos de filtrado para el listado Tareas creadas

Modificar tareas publicadas

Haz clic en el nombre de la tarea creada para mostrar la ventana de configuración de la tarea, donde es posible modificar cualquier parámetro de la misma.

> *Las tareas publicadas solo admiten cambio de nombre y de descripción. Para modificar una tarea publicada es necesario copiarla previamente.*

Cancelar tareas publicadas

Para cancelar una tarea ya publicada haz clic en el link Cancelar. La tarea se cancelará, aunque no se borrará de la ventana de tareas para poder acceder a sus resultados.

Borrar tareas

Las tareas ejecutadas no se eliminan automáticamente, para ello es necesario hacer clic en las casillas de selección y después en el icono .

> *Al borrar una tarea se borrarán también sus resultados.*

Copiar tareas

Para crear una nueva con su misma configuración haz clic en el icono .

Ver los resultados de una tarea

Al hacer clic en el link **Ver resultados** las tareas publicadas se muestra los resultados obtenidos hasta el momento. Se abrirá una ventana con los resultados y una serie de filtros que permiten localizar los datos importantes de forma fácil.

Campo	Descripción	Valores
Equipo	Nombre del equipo donde se registró un evento de ejecución de tarea.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Cytomic EPDR a la que pertenece el equipo.	Cadena de caracteres

Tabla 24.5: : parámetros de filtrado sobre el resultado de tareas

Campo	Descripción	Valores
Estado	• **Pendiente**: la tarea se intentó iniciar, pero la máquina no estaba disponible en ese momento. Se establece un periodo de espera según su configuración. • **En progreso**: la tarea se está ejecutando en este momento. • **Con éxito**: la tarea terminó con éxito. • **Fallida**: la tarea terminó con error. • **Expirada**: la tarea no llegó a comenzar por haber expirado el plazo configurado. • **Cancelada**: la tarea fue cancelada de forma manual.	Cadena de caracteres
Parches instalados	En las tareas de tipo instalación de parches indica el número de parches que se instalaron en el equipo.	Numérico
Parches desinstalados	En las tareas de tipo desinstalación de parches indica el número de parches que se desinstalaron en el equipo.	Numérico
Detecciones	En las tareas de tipo análisis indica el número de detecciones realizadas en el equipo.	Numérico
Fecha de comienzo	Fecha de inicio de la tarea.	Fecha
Fecha fin	Fecha de finalización de la tarea.	Fecha

Tabla 24.5: : parámetros de filtrado sobre el resultado de tareas

Herramienta de filtrado de tareas

Campo	Descripción	Valores
Fecha	Desplegable con las fechas en las que la tarea pasó a estado activo según su programación configurada. Una tarea activa puede iniciarse en el momento o esperar a que la máquina esté disponible. Esta fecha se indica en la columna fecha.	Fecha
Estado	• **Pendiente**: la tarea todavía no se ha iniciado por no haber alcanzado la ventana de ejecución configurada. • **En progreso**: la tarea se está ejecutando en este momento. • **Con éxito**: la tarea terminó con éxito. • **Con error**: la tarea terminó con error.	Enumeración

Tabla 24.6: filtros de búsqueda de tareas

Campo	Descripción	Valores
	• **Cancelada (no se puedo iniciar a la hora programada)**: el equipo no estaba disponible en el momento del inicio de la tarea o en el intervalo definido. • **Cancelada:** la tarea fue cancelada de forma manual. • **Cancelada (tiempo máximo expirado)**: la tarea duró mas tiempo que el indicado en la configuración de la tarea y se canceló.	

Tabla 24.6: filtros de búsqueda de tareas

Editar tareas

Para editar una tarea creada o publicada haz clic en su nombre. Se mostrará la ventana de edición con los mismos campos que los incluidos en la ventana de creación de tareas.

Para visualizar un listado de todos los equipos que recibirán la tarea, haz clic en el botón **Ver equipos**. Se mostrará el listado de equipos de la zona **Equipos** con la acción y el tipo de tarea creada como filtro.

Modificación automática de destinatarios en tareas

El conjunto de equipos sobre los que aplica una tarea puede ser difícil de determinar debido a dos factores:

- Los grupos son entidades de agrupación dinámicas, que varían a lo largo del tiempo.
- Las tareas son acciones ejecutadas sobre grupos y definidas en un momento concreto, aunque su ejecución (repetida o no) se puede aplazar en el tiempo.

De esta manera una tarea sobre uno o varios grupos, definida en el momento T1, tiene como destinatarios los equipos que forman los grupos seleccionados, pero en el momento de ejecución T2, los miembros de esos grupos pueden haber cambiado.

A la hora de resolver los equipos que pertenecen a un grupo, se distinguen tres casos según el tipo de tarea:

- Tareas inmediatas.
- Tareas programadas de ejecución única.
- Tareas programadas de ejecución repetida.

Tareas inmediatas

Estas tareas se crean, se publican y se lanzan de forma atómica una única vez. El grupo destinatario se evalúa en el momento en que el administrador crea la tarea. Los equipos afectados parecerán en estado **Pendiente** en la tarea.

Añadir equipos a la tarea

No se admite añadir nuevos equipos a la tarea. Aunque se asignen nuevos equipos al grupo destinatario, estos no recibirán la tarea.

Quitar equipos de la tarea

Sí se pueden retirar equipos de la tarea. Mueve los equipos del grupo destinatario de la tarea a otro grupo para cancelar la tarea.

Tareas programadas de ejecución única

Estas tareas admiten dos estados con respecto a la posibilidad de cambiar los integrantes del grupo de equipos destinatario:

Tareas cuya ejecución comenzó hace menos de 24 horas

En las primeras 24 horas de la ejecución de estas tareas, el administrador puede añadir o retirar equipos a la tarea o a los grupos destinatarios.

Se marca un plazo de 24 horas para abarcar todos los usos horarios en aquellas multinacionales con presencia en varios países.

Tareas cuya ejecución comenzó hace más de 24 horas

Una vez cumplido el plazo de 24 horas, no es posible añadir nuevos equipos y, aunque se asignen nuevos equipos al grupo destinatario, éstos no recibirán la tarea. Para cancelar las tareas en curso sobre equipos muévelos fuera del grupo destinatario.

Tareas programadas de ejecución repetida

Estas tareas admiten agregar o eliminar equipos destinatarios en cualquier momento hasta su cancelación o finalización.

Las tareas programadas de ejecución repetida no muestran los equipos destinatarios en estado Pendiente de forma automática, sino que éstos se irán mostrando de forma progresiva a medida que la plataforma Cytomic reciba información del estado de la tarea de cada equipo.

Parte 8

Información complementaria sobre Cytomic EPDR

Capítulo 25: Requisitos de hardware, software y red

Capítulo 26: La cuenta Cytomic

Capítulo 27: Conceptos clave

Capítulo 25

Requisitos de hardware, software y red

Cytomic EPDR es un servicio cloud y como tal, Cytomic mantiene en sus instalaciones toda la infraestructura necesaria para proteger los equipos de sus clientes sin necesidad de desplegar software o hardware adicional en las redes de las organizaciones. No obstante, es necesario cumplir con ciertos requisitos mínimos en los equipos a proteger y en la red de la organización para garantizar un correcto funcionamiento del producto.

CONTENIDO DEL CAPÍTULO

Requisitos de plataformas Windows

Sistemas operativos soportados

Estaciones de trabajo

- Windows XP SP3 (32 bits)
- Windows Vista (32 y 64-bit)
- Windows 7 (32 y 64-bit)
- Windows 8 (32 y 64-bit)
- Windows 8.1 (32 y 64-bit)
- Windows 10 (32 y 64-bit)

Servidores

- Windows 2003 (32, 64-bit y R2) SP2 y superiores
- Windows 2008 (32 y 64-bit) y 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016 y 2019
- Windows Server Core 2008, 2008 R2, 2012 R2, 2016 y 2019

Requisitos hardware

- **Procesador**: CPU compatible x86 o x64 y con soporte SSE2.
- **Memoria RAM**: 1 Gbyte
- **Espacio libre en el disco duro para la instalación**: 650 Mbytes

Otros requisitos

Para un funcionamiento correcto del producto es necesario mantener actualizados los certificados raíz de los equipos de usuario y servidores. En caso de no cumplir con este requisito, algunas funcionalidades como la comunicación en tiempo real de los agentes con la consola de administración y el módulo Cytomic Patch podrían dejar de funcionar.

Para poder ejecutar acciones de resolución desde Cytomic Orion es necesario abrir las siguientes URLs en el cortafuegos perimetral de la empresa y en el cortafuegos local del equipo si es de otro fabricante distinto de Cytomic:

- eu02.rc.pandasecurity.com

- dir.rc.pandasecurity.com por el puerto 443
- eu01.rc.pandasecurity.com por los puertos 8080 y 443
- ams01.rc.pandasecurity.com por los puertos 8080 y 443

Requisitos de plataformas Windows Exchange

Sistemas operativos soportados

- **Exchange 2003**: Windows Server 2003 32 bits SP2+ y Windows Server 2003 R2 32 bits
- **Exchange 2007**: Windows Server 2003 64 bits SP2+, Windows Server 2003 R2 64 bits, Windows 2008 64 bits y Windows 2008 R2
- **Exchange 2010**: Windows 2008 64 bits y Windows 2008 R2
- **Exchange 2013**: Windows Server 2012 y Windows Server 2012 R2
- **Exchange 2016**: Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016.
- **Exchange 2019**: Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 y Windows Server 2019.

Requisitos hardware y software

Los requisitos de hardware para instalar la protección de Servidores Exchange son los que marca el propio Exchange Server:

- Exchange 2003:

http://technet.microsoft.com/es-es/library/cc164322(v=exchg.65).aspx

- Exchange 2007:

http://technet.microsoft.com/es-es/library/aa996719(v=exchg.80).aspx

- Exchange 2010:

http://technet.microsoft.com/es-es/library/aa996719(v=exchg.141).aspx

- Exchange 2013

http://technet.microsoft.com/es-es/library/aa996719(v=exchg.150).aspx

- Exchange 2016

https://technet.microsoft.com/es-es/library/aa996719(v=exchg.160).aspx

- Exchange 2019

https://docs.microsoft.com/es-es/Exchange/plan-and-deploy/system-requirements?view=exchserver-2019

Versiones Exchange soportadas

- Microsoft Exchange Server 2003 Standard y Enterprise (SP1 / SP2)
- Microsoft Exchange Server 2007 Standard y Enterprise (SP0 / SP1 / SP2 / SP3)
- Microsoft Exchange Server 2007 incluido en Windows SBS 2008
- Microsoft Exchange Server 2010 Standard y Enterprise (SP0 / SP1 / SP2)
- Microsoft Exchange Server 2010 incluido en Windows SBS 2011
- Microsoft Exchange Server 2013 Standard y Enterprise
- Microsoft Exchange Server 2016 Standard y Enterprise
- Microsoft Exchange Server 2019 Standard y Enterprise

Requisitos de plataformas macOS

Sistemas operativos soportados

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina

Requisitos hardware

- **Procesador**: Intel Core 2 Duo
- **Memoria RAM**: 2 Gbyte
- **Espacio libre en el disco duro para la instalación**: 400 Mbytes
- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento del filtrado web y la detección web de malware.

Requisitos de plataformas Linux

Cytomic EPDR se instala tanto en estaciones de trabajo como en servidores Linux. Si no está presente un entorno gráfico en el momento de la instalación las protecciones URL filter y Web filter quedarán deshabilitadas. En equipos sin entorno gráfico utiliza la herramienta `/usr/local/protection-agent/pa_cmd` para controlar la protección.

Para completar la instalación de Cytomic EPDR en plataformas Linux es necesario que el equipo tenga conexión a Internet durante todo el proceso.

Distribuciones de 64 bits soportadas

- Ubuntu 14.04 LTS, 14.10, 15.04, 15.10, 16.0.4 LTS, 16.10, 17.04, 17.10, 18,04, 18.10 y 19.04
- Fedora 23, 24, 25, 26, 27, 28, 29, 30 y 31
- Debian 8, 9 y 10
- RedHat 7, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8, 8.0, 8.1
- CentOS 7, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8, 8.0, 8.1
- LinuxMint 18, 18.1, 18.2, 18.3, 19, 19.1, 19.2

Versión de kernel soportada

- **Versión mínima soportada**: 3.12
- **Versión máxima soportada**: 5.4.1

Gestores de ficheros soportados

- Nautilus
- Pcmanfm
- Dolphin

Requisitos hardware

- **Procesador**: CPU compatible x86 o x64 y con soporte SSE2.
- **Memoria RAM**: 1.5 Gbytes
- **Espacio libre en el disco duro para la instalación**: 100 Mbytes.
- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento del filtrado web y la detección web de malware.
- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento de la detección web de malware.
- **Dependencias del paquete de instalación**

El agente Linux descargará en el proceso de instalación todos los paquetes necesarios para satisfacer las dependencias. De forma general los paquetes necesarios en el sistema para poder funcionar son 3:

- Libcurl
- OpennSSL

- Gcc y las utilidades de compilación (make, makeconfig etc.) en Fedora

> *El proceso de instalación en Fedora incluye la compilación de los módulos necesarios para el buen funcionamiento del agenteCytomic EPDR.*

Para mostrar las dependencias del agente ejecuta los comandos mostrados a continuación en una terminal según la distribución de destino:

- Para distribuciones basadas en Debian: `dpkg --info paquete.deb`
- Para distribuciones basadas en Fedora: `rpm --qRp paquete.rpm`

Requisitos de plataformas Android

Sistemas operativos soportados

- Ice Cream Sandwich 4.0
- Jelly Bean 4.1 - 4.2 - 4.3
- KitKat 4.4
- Lollipop 5.0/5.1
- Marshmallow 6.0
- Nougat 7.0 - 7.1
- Oreo 8.0
- Pie 9.0
- Android 10

Requisitos hardware

Se requiere un mínimo de 10 megabytes de espacio en la memoria interna del dispositivo. Dependiendo del modelo es posible que el espacio requerido sea superior.

Requisitos de red

Para que las notificaciones push funcionen correctamente desde la red de la empresa es necesario abrir los puertos 5228, 5229 y 5230 a todo el bloque de IPs ASN 15169 correspondientes a Google.

Acceso a la consola web

La consola de administración es accesible con la última versión de los navegadores compatibles mostrados a continuación:

- Chrome
- Internet Explorer
- Microsoft Edge
- Firefox
- Opera

Acceso a URLs del servicio

Para el correcto funcionamiento de Cytomic EPDR es necesario que las URL mostradas a continuación sean accesibles desde los equipos protegidos de la red.

Nombre de producto	URLs
Cytomic EPDR	• **https://*.pandasecurity.com** • **http://*.pandasecurity.com** • **https://*.windows.net** • **http://*.pandasoftware.com** • **http://*.globalsign.com** • **http://*.digicert.com**
Antispam y filtrado web	• **http://*.pand.ctmail.com** • **http://download.ctmail.com**
Cytomic Data Watch	• **https://pandasecurity.devo.com**
Cytomic Patch	• Todas las URLs contenidas en el recurso **https://forums.ivanti.com/s/article/URL-Exception-List-for-Ivanti-Patch-for-SCCM** • **https://content.ivanti.com**
Otros	• **http://proinfo.pandasoftware.com/connectiontest.html** • **http://www.iana.org**

Tabla 25.1: URLs de acceso al servicio

Puertos

- Port 80 (HTTP, websocket)
- Port 443 (HTTPS)

Descarga de parches y actualizaciones (Cytomic Patch)

Consulta la pagina de soporte **https://www.pandasecurity.com/spain/support/card?id=700044** para obtener un listado completo de las urls accesibles desde los equipos de la red que recibirán los parches o desde los equipos con rol de caché / repositorio.

Capítulo 26

La cuenta Cytomic

La Cuenta Cytomic ofrece al administrador un mecanismo de auto gestión de credenciales y acceso a los servicios contratados con Cytomic, frente al método estándar de recepción de credenciales por correo electrónico.

Con una Cuenta Cytomic es el propio administrador quien crea y activa el método de acceso a la consola Web de Cytomic EPDR.

CONTENIDO DEL CAPÍTULO

Crear una Cuenta Cytomic

Para crear una nueva Cuenta Cytomic es necesario seguir el procedimiento descrito a continuación.

Recepción del mensaje de correo

- Al adquirir Cytomic EPDR recibirás un mensaje de correo electrónico procedente de Cytomic.
- Haz clic en el vínculo que contiene el mensaje para acceder a la Web desde donde crear la Cuenta Cytomic.

Rellenar el formulario

- Rellena con tus datos el formulario mostrado.
- Utiliza el desplegable situado en la esquina inferior derecha si deseas que la página se muestre en otro idioma.
- Accede al acuerdo de licencia y la política de privacidad haciendo clic en el vínculo correspondiente.
- Haz clic en **Crear** cuando para terminar y recibir un mensaje de correo electrónico en la dirección especificada en el formulario. Utiliza ese mensaje para activar la cuenta.

Activar la Cuenta Cytomic

Una vez creada la Cuenta Cytomic es necesario activarla. Para ello hay que utilizar el mensaje de correo electrónico que has recibido en la bandeja de entrada de la dirección mail utilizada para crear la Cuenta Cytomic.

- Ve a la bandeja de entrada y localiza el mensaje.
- Haz clic en el botón de activación. Al hacerlo, se confirmará como válida la dirección proporcionada al crear la Cuenta Cytomic. En caso de que el botón no funcione, copia en el navegador el enlace que se muestra en el mensaje.
- La primera vez que accedas a la Cuenta Cytomic el sistema te solicitará una confirmación de contraseña. Después, haz clic en el botón **Activar cuenta**.
- Introduce los datos necesarios y haz clic en **Guardar datos**. Si prefieres facilitar los datos en otra ocasión, utiliza la opción **Ahora no**.
- Acepta el acuerdo de licencias y haz clic en **Aceptar**.

Una vez finalizado con éxito el proceso de activación de la Cuenta Cytomic te encontrarás en la página principal de Cytomic Cloud. Desde aquí puedes acceder a la consola Web de Cytomic EPDR. Para ello, utiliza el icono de acceso directo que encontrarás en **Mis servicios**.

Capítulo 27

Conceptos clave

Zero-trust Application Service

Servicio de Cytomic EPDR incluido en la licencia básica que clasifica el 100% de los procesos ejecutados en los equipos de usuario y servidores para emitir una valoración sin ambigüedades (goodware o malware, sin sospechosos).

Adaptador de red

Hardware que permite la comunicación entre diferentes equipos conectados a través de una red de datos. Un equipo puede tener más de un adaptador de red instalado y es identificado en el sistema mediante un número de identificación único.

Cytomic Insights

Servicio avanzado de explotación del conocimiento generado en tiempo real por los productos Cytomic EDR y Cytomic EPDR. Facilita el descubrimiento de amenazas desconocidas, ataques dirigidos y APTs, representando los datos de actividad de los procesos ejecutados por los usuarios y poniendo el énfasis en los eventos relacionados con la seguridad y la extracción de información.

Adware

Programa que una vez instalado o mientras se está instalando, ejecuta, muestra o descarga automáticamente publicidad en el equipo.

Agente Cytomic

Uno de los dos módulos del software de cliente Cytomic EPDR. Se encarga de las comunicaciones entre los equipos de la red y los servidores en la nube de Cytomic, además de gestionar los procesos locales.

Alerta

Ver "**Incidencia**".

Análisis forense

Conjunto de técnicas y procesos ejecutados por el administrador de la red con herramientas especializadas para seguir la ejecución de un programa malicioso y determinar las consecuencias de la infección.

Análisis heurístico

Análisis estático formado por un conjunto de técnicas que inspeccionan el programa sospechoso en base a cientos de características del archivo para determinar la probabilidad de que pueda llevar a cabo acciones maliciosas o dañinas cuando se ejecute en el equipo del usuario.

Antirrobo

Conjunto de tecnologías incorporadas en Cytomic EPDR que facilitan la localización de los dispositivos móviles extraviados y minimizan la exposición de los datos que contienen en caso de robo.

Anti-tamper

Conjunto de tecnologías que evitan la manipulación de los procesos de Cytomic EPDR por parte de amenazas avanzadas y APT que buscan sortear las capacidades de protección de la herramienta de seguridad instalada.

Anti Spam

Tecnología que busca correos no deseados en función de su contenido.

Antivirus

Módulo de protección basado en tecnologías tradicionales (fichero de firmas, análisis heurístico, anti exploit etc.), que detecta y elimina virus informáticos y otras amenazas.

APT (Advanced Persistent Threat)

Conjunto de estrategias emprendidas por hackers orientadas a infectar la red del cliente, utilizando múltiples vectores de infección de forma simultánea para pasar inadvertidos a los antivirus tradicionales durante largos periodos de tiempo. Su objetivo principal es económico (robo de información confidencial de la empresa para chantaje, robo de propiedad intelectual etc.).

ASLR (Address Space Layout Randomization)

Técnica implementada por el sistema operativo para mitigar los efectos de ataques de tipo exploit basados en desbordamiento de buffer. Mediante ASLR el sistema operativo introduce aleatoriedad a la hora de asignar direcciones de memoria para reservar espacio destinado a la pila, el heap y las librerías cargadas por los procesos. De esta forma, se dificulta la utilización ilegítima de llamadas a funciones del sistema por desconocer la dirección física de memoria donde residen.

Árbol de carpetas

Estructura jerárquica formada por agrupaciones estáticas, utilizada para organizar el parque de equipos y facilitar la asignación de configuraciones.

Árbol de filtros

Colección de filtros agrupados en carpetas que facilitan la organización del parque de equipos y la asignación de configuraciones.

Archivo de identificadores / fichero de firmas

Fichero que contiene los patrones que el antivirus utiliza para detectar las amenazas.

ARP (Address Resolution Protocol)

Protocolo utilizado para resolver direcciones del nivel de red a direcciones del nivel de enlace. En redes IP traduce las direcciones IP a direcciones físicas MAC.

Asignación automática de configuraciones

Ver "**Herencia**".

Asignación indirecta de configuraciones

Ver "**Herencia**".

Asignación manual de configuraciones

Asignación de una configuración a un grupo de forma directa, en contraposición al establecimiento de configuraciones automático o indirecto, que utiliza el recurso de la herencia para fijar configuraciones sin intervención del administrador.

Audit

Modo de configuración de Cytomic EPDR para visualizar la actividad de los procesos ejecutados en los equipos protegidos de la red sin desencadenar ninguna acción de protección (desinfección o bloqueo).

Backup

Área de almacenamiento de ficheros maliciosos no desinfectables, así como de spyware y herramientas de hacking detectadas. Todos los programas eliminados del sistema por ser clasificados como amenazas se copian de forma temporal en el área de backup / cuarentena durante un periodo de entre 7 y 30 días según su tipo.

BitLocker

Software instalado en algunas versiones de los equipos Windows 7 y superiores encargado de gestionar el cifrado y descifrado de los datos almacenados en los volúmenes del equipo y utilizado porCytomic Encryption.

Bloquear

Acción de Cytomic EPDR que impide la ejecución de los programas instalados en el equipo del usuario debido a uno de los motivos siguientes:

- Programas clasificados como amenaza.
- Programas desconocidos para Cytomic EPDR y la política de protección avanzada esta configurada como lock o como hardening y su origen es no confiable.
- Programas bloqueados por políticas establecidas por el administrador.

Transmisión de paquetes en redes de datos a todos los nodos de la subred: un paquete de datos llegará a todos los equipos dentro de la misma subred sin necesidad de enviarlo de forma individual a cada nodo. Los paquetes de broadcast no atraviesan encaminadores y utilizan un direccionamiento distinto para diferenciarlos de los paquetes unicast.

Caché / Repositorio (rol)

Equipos que descargan y almacenan de forma automática todos los ficheros necesarios para que otros equipos con Cytomic EPDR instalado puedan actualizar el archivo de identificadores, el agente y el motor de protección sin necesidad de acceder a Internet. De esta manera se produce un ahorro de ancho de banda, ya que cada equipo no descargará de forma independiente las actualizaciones, sino que se hará una única vez de forma centralizada.

Cambio de comportamiento

Al clasificar como malware o goodware un programa que el administrador permitió su ejecución cuando todavía era desconocido, Cytomic EPDR se puede comportar de dos maneras:

- Eliminarlo de la lista de Programas permitidos: si se ha clasificado como goodware seguirá pudiéndose ejecutar, si se ha clasificado como malware, se impedirá su ejecución.
- Mantener en la lista de Programas permitidos: se seguirá permitiendo su ejecución independientemente de que se trate de malware o goodware.

Ciclo de protección adaptativa

Nuevo enfoque de seguridad basado en la integración de un conjunto de servicios de protección, detección, monitorización, análisis forense y resolución, todos ellos centralizados en una única consola de administración accesible desde cualquier lugar y en cualquier momento.

Ciclo de vida del malware

Detalle de todas las acciones desencadenadas por un programa malicioso, desde que fue visto por primera vez en un equipo del cliente hasta su clasificación como malware y posterior desinfección.

Clave de recuperación

Cuando se detecta una situación anómala en un equipo protegido con Cytomic Encryption o en el caso de que hayamos olvidado la contraseña de desbloqueo, el sistema pedirá una clave de recuperación de 48 dígitos. Esta clave se gestiona desde la consola de administración y debe ser introducida para completar el inicio del equipo. Cada volumen cifrado tendrá su propia clave de recuperación independiente.

Configuración

Ver "**Perfil de configuración**".

Control de dispositivos

Módulo que define el comportamiento del equipo protegido al conectar dispositivos extraíbles o de almacenamiento masivo, para minimizar la superficie de exposición del equipo.

Control de acceso a páginas web

Tecnología que controla y filtrar las URLs solicitadas por los navegadores de la red con el propósito de denegar o permitir su acceso, tomando como referencia una base de datos de URLs dividida en categorías o temas.

Consola Web

Herramienta de gestión del servicio de seguridad avanzada Cytomic EPDR, accesible desde cualquier lugar y en cualquier momento mediante un navegador web compatible. Con la consola web el administrador puede desplegar el software de protección, establecer las configuraciones de seguridad y visualizar el estado de la protección. También permite utilizar herramientas de análisis forense que establecen el alcance de los problemas de seguridad.

Cuarentena

Ver "**Backup**".

Cuenta de usuario

Ver "**Usuario (consola)**".

CVE (Common Vulnerabilities and Exposures)

Lista de información definida y mantenida por The MITRE Corporation sobre vulnerabilidades conocidas de seguridad. Cada referencia tiene un número de identificación único, ofreciendo una

nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.

Desbloqueado (programa)

Programas inicialmente bloqueados por no haber obtenido todavía una clasificación, pero que el administrador de la red permite su ejecución de forma selectiva y temporal para minimizar las molestias a los usuarios de la red.

Desbordamiento de buffer

Fallo en la gestión de los buffers de entrada de un proceso. En estos casos, si el volumen de datos recibido es mayor que el tamaño del buffer reservado, los datos sobrantes no se descartan, sino que se escriben en zonas de memoria adyacentes al buffer. Estas zonas de memoria pueden ser interpretadas como código ejecutable en sistemas anteriores a la aparición de la tecnología DEP.

Descubridor (rol)

Equipos capaces descubrir puestos de usuario y servidores no administrados para iniciar una instalación remota del agente Cytomic EPDR.

DEP

Característica de los sistemas operativos que impide la ejecución de páginas de memoria destinadas a datos y marcadas como no ejecutables. Esta característica se diseñó para prevenir la explotación de fallos por desbordamiento de buffer.

Desinfectable

Fichero infectado por malware del cual se conoce el algoritmo necesario para poder revertirlo a su estado original.

DHCP

Servicio que asigna direcciones IP a los nuevos equipos conectados a la red.

Dialer

Programa que marca un número de tarificación adicional (NTA), utilizando para ello el módem. Los NTA son números cuyo coste es superior al de una llamada nacional.

Dirección IP

Número que identifica de manera lógica y jerárquica la interfaz de red de un dispositivo (habitualmente un ordenador) dentro de una red que utilice el protocolo IP.

Dirección MAC

Identificador hexadecimal de 48 bits que corresponde de forma única a una tarjeta o interfaz de red.

Directorio Activo

Implementación propietaria de servicios LDAP (Lightweight Directory Access Protocol, Protocolo Ligero/Simplificado de Acceso a Directorios) para máquinas Microsoft Windows. Permite el acceso a un servicio de directorio para buscar información diversa en entornos de red.

Distribución Linux

Conjunto de paquetes de software y bibliotecas que conforman un sistema operativo basado en el núcleo Linux.

DNS (Domain Name System)

Servicio que traduce nombres de dominio con información de diversos tipos, generalmente direcciones IP.

Dominio

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios está centralizada en un servidor llamado Controlador Principal de Dominio (PDC) o Directorio Activo (AD).

Entidad

Predicado o complemento incluido en las tablas de acciones del módulo análisis forense.

Entidad (Cytomic Data Watch)

Conjunto de datos que tomados como una unidad adquieren un significado propio.

EoL (End Of Life)

Término utilizado para indicar el final del ciclo de vida de un producto. A partir de la fecha indicada el producto ya no recibirá actualizaciones ni parches que corrijan sus defectos, convirtiéndose en un objetivo claro para los hackers.

Equipos sin licencia

Equipos cuya licencia ha caducado o no ha sido posible asignar una licencia válida por haberse superado el número máximo permitido de instalaciones de la protección. Estos equipos no están protegidos, pero son visibles en la consola web de administración.

Excluido (programa)

Son programas inicialmente bloqueados por haber sido clasificados como malware o PUP, pero que el administrador de la red permite su ejecución de forma selectiva y temporal excluyéndolos del análisis.

Exploit

De forma general un exploit es una secuencia de datos especialmente diseñada para provocar un fallo controlado en la ejecución de un programa vulnerable. Después de provocar el fallo, el proceso comprometido interpretará por error parte de la secuencia de datos como código ejecutable, desencadenando acciones peligrosas para la seguridad del equipo.

Firewall

También conocido como cortafuegos, es una tecnología que bloquea el tráfico de red que coincide con patrones definidos por el administrador mediante reglas. De esta manera se limita o impide la comunicación de ciertas aplicaciones que se ejecutan en los equipos, restringiéndose la superficie de exposición del equipo.

Filtro

Contenedor de equipos de tipo dinámico que agrupa de forma automática aquellos elementos que cumplen con todas las condiciones definidas por el administrador. Los filtros simplifican la asignación de configuraciones de seguridad y facilitan la administración de los equipos del parque informático.

FQDN (Fully Qualified Domain Name)

Es un nombre de dominio que especifica la localización de forma precisa y sin ambiguedades dentro del árbol de jerarquía del sistema de nombres DNS. El FQDN especifica todos los niveles del dominio incluyendo el nivel superior y la zona raiz (root).

Fragmentación

En redes de transmisión de datos, cuando la MTU del protocolo subyacente es menor que el tamaño del paquete a transmitir, los encaminadores dividen el paquete en piezas más pequeñas (fragmentos) que se encaminan de forma independiente y se ensamblan en el destino en el orden apropiado.

GDPR (General Data Protection Regulation)

Normativa que regula la protección de los datos de los ciudadanos que viven en la Unión Europea. Consulta el enlace **http://www.privacy-regulation.eu/es/index.htm** para acceder al reglamento completo.

Geolocalizar

Posicionar en un mapa un dispositivo en función de sus coordenadas.

Goodware

Fichero clasificado como legítimo y seguro tras su estudio.

Grafo de actividad / grafo de ejecución

Representación visual de las acciones ejecutadas por las amenazas, poniendo énfasis en el enfoque temporal.

Grupo

Contenedor de tipo estático que agrupa a uno o más equipos de la red. La pertenencia de un equipo a un grupo se establece de forma manual. Los grupos se utilizan para simplificar la asignación de configuraciones de seguridad y para facilitar la administración de los equipos del parque informático.

Grupo de trabajo

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios residen en cada uno de los equipos de forma independiente.

Hardening

Modo de configuración de Cytomic EPDR que bloquea los programas clasificados como malware y los ficheros desconocidos cuyo origen es una fuente no fiable:

- Internet.
- Unidades externas de almacenamiento
- Otros equipos de la red del cliente.

Heap Spraying

Head Spray es una técnica utilizada para facilitar la explotación de vulnerabilidades por parte de un proceso malicioso independiente.

Debido a la constante mejora de los sistemas operativos, la explotación de vulnerabilidades se ha convertido es un proceso muy aleatorio. Debido a que el comienzo de la región de memoria heap de un proceso es predecible, y las posteriores reservas de espacio son secuenciales, Head Spray aporta predictibilidad a los ataques, sobrescribiendo porciones de la región de memoria heap del proceso objetivo. Estas porciones de memoria serán referenciadas más adelante por un proceso malicioso para ejecutar el ataque.

Esta técnica es muy empleada para explotar vulnerabilidades de navegadores y sus plugins correspondientes.

Herencia

Método de asignación automática de configuraciones sobre todos los grupos descendientes de un grupo padre, ahorrando tiempo de gestión. También llamado Asignación automática de configuraciones o Asignación indirecta de configuraciones.

Herramienta de hacking

Programa utilizado por hackers para causar perjuicios a los usuarios de un ordenador, pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc.

Hoaxes

Falsos mensajes de alarma sobre amenazas que no existen y que llegan normalmente a través del correo electrónico.

ICMP (Internet Control Message Protocol)

Protocolo de control y notificación de errores utilizado por el protocolo IP en Internet.

Identificador

Palabra clave utilizada en las búsquedas de Cytomic Data Watch que permite seleccionar un tipo de entidad.

IDP (Identity Provider)

Servicio centralizado responsable de gestionar las identidades de los usuarios.

IFilter

Librería del sistema operativo que permite el acceso al contenido de ficheros ofimáticos.

Incidencia

Mensaje relativo a la protección avanzada de Cytomic EPDR, susceptible de requerir la intervención del administrador. Las incidencias se reciben mediante la consola de administración y el correo electrónico (alertas), y el usuario del equipo protegido mediante mensajes generados por el agente que se visualizan en el escritorio de su dispositivo.

Indexar

Proceso que analiza el contenido de los ficheros y lo almacena en una base de datos de rápido acceso para acelerar su búsqueda.

Informes avanzados

Ver "**Cytomic Insights**".

IP (Internet Protocol)

Principal protocolo de comunicación en Internet para el envío y recepción de los datagramas generados en el nivel de enlace subyacente.

Inventario

Base de datos mantenida por Cytomic Data Watch con los ficheros clasificados como PII encontrados en el parque informático.

Joke

Broma con el objetivo de hacer pensar a los usuarios que han sido afectados por un virus.

Malware

Término general utilizado para referirse a programas que contienen código malicioso (MALicious softWARE), ya sean virus, troyanos, gusanos o cualquier otra amenaza que afecta a la seguridad e integridad de los sistemas informáticos. El malware se infiltra y daña un ordenador sin el conocimiento de su dueño, con finalidades muy diversas.

Llave USB

Dispositivo utilizado en equipos con volúmenes cifrados que permite almacenar la clave en una memoria portátil. De esta forma, no se requiere introducir ninguna contraseña en el proceso de inicio del equipo, aunque es necesario que el dispositivo USB que almacena la contraseña esté conectado en el equipo.

Lock

Modo de configuración de Cytomic EPDR que bloquea los programas desconocidos y los ya clasificados como amenazas.

Machine learning

Es una rama de la inteligencia artificial cuyo objetivo es desarrollar técnicas para capaces de generalizar comportamientos a partir de una información no estructurada suministrada en forma de ejemplos.

Malware freezer

Comportamiento del backup / cuarentena cuyo objetivo es evitar la pérdida de datos por falsos positivos. Todos los ficheros clasificados como malware o sospechosos son enviados a la zona de backup / cuarentena, evitando su borrado completo en previsión de un fallo en la clasificación que derive en pérdida de datos.

MD5 (Message-Digest Algorithm 5)

Algoritmo de reducción criptográfico que obtiene una firma (hash o digest) de 128 bits que representa de forma única una serie o cadena de entrada. El hash MD5 calculado sobre un fichero sirve para su identificación unívoca o para comprobar que no fue manipulado / cambiado.

Microsoft Filter Pack

Paquete de librerías IFilter que abarca todos los formatos de fichero generados por la suite de ofimática Microsoft Office.

MTU (Maximun transmission unit)

Tamaño máximo del paquete que el protocolo subyacente puede transportar.

Normalización

En Cytomic Data Watch, es una tarea que forma parte del proceso de indexación de textos, y que consiste en eliminar todos los caracteres innecesarios (generalmente caracteres separadores o delimitadores) antes de almacenarlos en la base de datos.

Nube (Cloud Computing)

Tecnología que permite ofrecer servicios a través de Internet. En este sentido, la nube es un término que se suele utilizar como una metáfora de Internet en ámbitos informáticos.

OU (Organizational Unit)

Forma jerárquica de clasificar y agrupar objetos almacenados en directorios.

Parche

Pequeños programas publicados por los proveedores de software que modifican sus programas corrigiendo fallos y añadiendo nuevas funcionalidades.

Cytomic Insights

Modulo compatible con Cytomic EPDR que almacena toda la telemetría generada por los procesos ejecutados en los equipos de usuario y servidores, y la presenta de forma gráfica para generar inteligencia de seguridad.

Cytomic Data Watch

Modulo compatible con Cytomic EPDR que descubre ficheros PII en la red de la empresa y monitoriza su acceso para cumplir con las regulaciones de almacenamiento de datos vigentes, tales como la GDRP.

Cytomic Encryption

Módulo compatible con Cytomic EPDR que cifra el contenido de los dispositivos de almacenamiento interno del equipo. Su objetivo es minimizar la exposición de los datos de la empresa ante la pérdida o robo, o en caso de sustitución y retirada de los dispositivos de almacenamiento sin formatear.

Cytomic Patch

Módulo compatible con Cytomic EPDR que parchea y actualizar los programas instalados en los equipos de usuario y servidores para eliminar las vulnerabilidades producidas por fallos de programación, minimizando así su superficie de ataque.

Cytomic SIEMConnect

Modulo compatible con Cytomic EPDR que envía al servidor SIEM de la empresa toda la telemetría generada por los procesos ejecutado en los equipos de usuario y servidores.

Partición de sistema

Zona del disco duro que permanece sin cifrar y que es necesaria para que el equipo complete correctamente el proceso de inicio en los equipos con Cytomic Encryption activado.

Partner

Empresa que ofrece productos y servicios de Cytomic.

Passphrase

También llamado Enhanced PIN (PIN mejorado) o PIN extendido, es una contraseña equivalente al PIN pero que permite añadir caracteres alfanuméricos. Se aceptan letras en mayúscula y minúscula, números, espacios en blanco y símbolos.

Payload

En informática y telecomunicaciones es el conjunto de datos transmitidos útiles, que se obtienen de excluir cabeceras, información de control y otros datos que son enviados para facilitar la entrega del mensaje.

En seguridad informática referida a amenazas de tipo exploit, payload es la parte del código del malware que realiza la acción maliciosa en el sistema, como borrar los ficheros o enviar datos al exterior, frente a la parte del encargado de aprovechar una vulnerabilidad (el exploit) que permite ejecutar el payload.

PDC (Primary Domain Controller)

Es un rol adoptado por servidores en redes Microsoft de tipo Dominio, que gestiona de forma centralizada la asignación y validación de las credenciales de los usuarios para el acceso a los recursos de red. En la actualidad el Directorio Activo cumple esta función.

Perfil de configuración

Un perfil es una configuración específica de la protección o de otro aspecto del equipo administrado. Este perfil es posteriormente asignado a un grupo o grupos y aplicado a todos los equipos que lo forman.

Phishing

Intento de conseguir de forma fraudulenta información confidencial de un usuario mediante el engaño. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito o cuentas bancarias.

PII (Personally Identifiable Information)

Ficheros que contienen datos que pueden ser utilizados para identificar o localizar a personas concretas.

PIN (Personal Identification Number, número de identificación personal)

Secuencia de números que actúa como contraseña simple y es requerida en el inicio de un equipo que tenga un volumen cifrado. Sin el PIN la secuencia de arranque no se completa y el acceso al equipo no es posible.

Proceso comprometido

Son aquellos procesos vulnerables que han sido afectados por un exploit y pueden comprometer la seguridad del equipo de usuario.

Proceso vulnerable

Son programas que, debido a fallos de programación, no son capaces de interpretar correctamente los datos recibidos de otros procesos. Al recibir una secuencia de datos especialmente diseñada (exploit), los hackers pueden provocar un mal funcionamiento del proceso, induciendo la ejecución de código que compromete la seguridad del equipo del usuario.

Programas potencialmente no deseados (PUP)

Son programas que se introducen de forma invisible o poco clara en el equipo aprovechando la instalación de otro programa que es el que realmente el usuario desea instalar.

Protección (módulo)

Una de las dos partes que componen el software Cytomic EPDR que se instala en los equipos. Contiene las tecnologías encargadas de proteger el parque informático y las herramientas de resolución para desinfectar los equipos comprometidos y determinar el alcance de los intentos de intrusión en la red del cliente.

Protección avanzada

Tecnología de monitorización continua y recogida de información de los procesos ejecutados en los equipos Windows de la red para su posterior envío de a la nube de Cytomic. Allí, se analiza mediante técnicas de Machine Learning en entornos Big Data para emitir una clasificación (goodware o malware) precisa.

Protocolo

Conjunto de normas y especificaciones utilizadas para el intercambio de datos entre ordenadores. Uno de los más habituales es el protocolo TCP- IP.

Proxy

Software que hace de intermediario de las comunicaciones establecidas entre dos equipos, un cliente situado en una red interna (por ejemplo, una intranet) y un servidor en una extranet o en internet.

Proxy (rol)

Equipo que hace la funciona de pasarela, conectando a otros puestos de usuario y servidores sin salida directa a Internet con la nube de Cytomic EPDR.

Puerto

Identificador numérico asignado a un canal de datos abierto por un proceso en un dispositivo a través del cual tienen lugar las transferencias de información (entradas / salidas) con el exterior.

QR (Quick Response), código

Representación gráfica en forma de matriz de puntos que almacena de forma compacta información.

Reclasificación de elementos

Ver Cambio de comportamiento.

Red pública

Redes desplegadas en locales abiertos al público como cafeterías, aeropuertos, etc. Debido a su naturaleza publica se recomienda establecer límites en el nivel de visibilidad de los equipos que se conectan a este tipo de redes ellas, y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.

Red de confianza

Redes desplegadas en locales privados, tales como oficinas y domicilios. Los equipos conectados son generalmente visibles por sus vecinos y no es necesario establecer limitaciones al compartir archivos, recursos y directorios.

Responsive / Adaptable (RWD, Responsive Web Design)

Conjunto de técnicas que permiten desarrollar páginas Web que se adaptan de forma automática al tamaño y resolución del dispositivo utilizado para visualizarlas.

RIR (Regional Internet Registry)

Organización que supervisa la asignación y el registro de direcciones IP y de sistemas autónomos (AS, Autonomous System) dentro de una región particular del mundo.

RoI

Configuración específica de permisos que se aplica a una o más cuentas de usuario y autoriza a ver o modificar determinados recursos de la consola.

Rootkits

Programa diseñado para ocultar objetos como procesos, archivos o entradas del Registro de Windows (incluyendo los suyos propios). Este tipo de software es utilizado para esconder evidencias y utilidades en sistemas previamente comprometidos.

ROP

ROP es una técnica de ejecución de exploits que permite a un atacante ejecutar código arbitrario en presencia de defensas como DEP o ASLR.

Los ataques tradicionales basados en desbordamiento de pila consistían en sobrescribir regiones de memoria enviando bloques de datos a la entrada de programas que no controlaban debidamente el tamaño de los datos recibidos. Estos ataques dejaron de funcionar cuando técnicas como DEP fueron implementadas de forma masiva en los sistemas operativos: en esta nueva situación el sistema operativo impide la ejecución del "código desbordado" ya que reside en regiones de memoria marcadas como de no ejecución (datos). ROP sobrescribe la pila de llamadas (call stack) de un proceso para ejecutar zonas de código del propio proceso, conocidas como "gadgets". Así, el atacante puede "armar" un flujo de ejecución alternativo al del proceso original, formado por partes de código del proceso atacado.

SCL (Spam Confidence Level)

Valor normalizado asignado a un mensaje que refleja la probabilidad de que sea Spam, evaluando características tales como su contenido, cabeceras y otros.

Servidor Exchange

Servidor de correo desarrollado por Microsoft. El servidor Exchange almacena los correos electrónicos entrantes y/o salientes y gestiona la distribución de los mismos en las bandejas de entrada configuradas para ello.

Servidor SMTP

Servidor que utiliza el protocolo SMTP -o protocolo simple de transferencia de correo- para el intercambio de mensajes de correo electrónicos entre los equipos.

SIEM (Security Information and Event Management)

Software que ofrece almacenamiento y análisis en tiempo real de las alertas generadas por los dispositivos de red.

Software cliente Cytomic EPDR

Programa que se instala en los equipos a proteger. Se compone de dos módulos: el agente Cytomic y la protección.

Sospechoso

Programa que, tras un análisis de su comportamiento realizado en el equipo del usuario por la protección de Cytomic EPDR, tiene una alta probabilidad de ser considerado malware.

Spam

El término correo basura hace referencia a mensajes no solicitados, habitualmente de tipo publicitario y generalmente enviados en grandes cantidades, que perjudican de alguna manera al receptor.

SSL (Secure Sockets Layer)

Protocolo criptográfico diseñado para la transmisión segura de datos por red.

Spyware

Programa que acompaña a otro y se instala automáticamente en un ordenador (generalmente sin permiso de su propietario y sin que éste sea consciente de ello) para recoger información personal y utilizarla posteriormente.

SYN

Bandera (flag) en el campo TOS (Type Of Service) de los paquetes TCP que los identifican como paquetes de inicio de conexión.

Tarea

Conjunto de acciones programadas para ejecutarse con una frecuencia y en un intervalo de tiempo configurables.

TCO (Total Cost of Ownership, Coste total de Propiedad)

Estimación financiera que mide los costes directos e indirectos de un producto o sistema.

Threat hunting

Conjunto de tecnologías y recursos humanos especializados que permiten detectar los movimientos laterales y otros indicadores tempranos de las amenazas, antes de que ejecuten acciones nocivas para la empresa.

Tiempo de exposición (dwell time)

Tiempo que una amenaza ha permanecido sin ser detectada en un equipo de la red.

TLS (Transport Layer Security)

Nueva versión del protocolo SSL 3.0.

Topología de red

Mapa físico o lógico de los nodos que conforman una red para comunicarse.

Troyanos

Programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad de los datos del usuario.

TCP (Transmission Control Protocol)

Principal protocolo del nivel de transporte dentro de la pila de protocolos de Internet, orientado a la conexión para el envío y recepción de paquetes IP.

TPM (Trusted Platform Module, módulo de plataforma segura)

Es un chip que se incluye en algunas placas base de equipos de sobremesa, portátiles y servidores. Su principal objetivo es proteger la información sensible de los usuarios, almacenando claves y otra información utilizada en el proceso de autenticación.

Ademas, el TPM es el responsable de detectar los cambios en la cadena de inicio del equipo, impidiendo por ejemplo el acceso a un disco duro desde un equipo distinto al que se utilizó para su cifrado.

UDP (User Datagram Protocol)

Protocolo del nivel de transporte dentro de la pila de protocolos de Internet, no confiable y no orientado a la conexión para el envío y recepción de paquetes IP.

Usuario (consola)

Recurso formado por un conjunto de información que Cytomic EPDR utiliza para regular el acceso de los administradores a la consola web y establecer las acciones que éstos podrán realizar sobre los equipos de la red.

Usuario (red)

Personal de la empresa que utiliza equipos informáticos para desarrollar su trabajo.

Variable de entorno

Cadena compuesta por información del entorno, como la unidad, la ruta de acceso o el nombre de archivo, asociada a un nombre simbólico que pueda utilizar Windows. La opción Sistema del Panel de control o el comando set del símbolo del sistema permiten definir variables de entorno.

VDI (Virtual Desktop Infrastructure)

Solución de virtualización de escritorio que consiste en alojar máquinas virtuales en un centro de datos al cual los usuarios acceden desde un terminal remoto con el objetivo de centralizar y simplificar la gestión y reducir los costes de mantenimiento. Se distinguen dos grupos de entornos VDI:

- **Persistente**: el espacio de almacenamiento asignado a cada usuario se respeta entre reinicios, incluyendo el software instalado, datos y actualizaciones del sistema operativo.
- **No persistente**: el espacio de almacenamiento asignado a cada usuario se elimina cuando la instancia VDI se reinicia, restaurándose a su estado inicial y deshaciendo todos los cambios efectuados.

Vector de infección

Puerta de entrada o procedimiento utilizado por el malware para infectar el equipo del usuario. Los vectores de infección más conocidos son la navegación web, el correo electrónico y los pendrives.

Ventana de oportunidad

Tiempo que transcurre desde que el primer equipo fue infectado a nivel mundial por una muestra de malware de reciente aparición hasta su estudio e incorporación a los ficheros de firmas de los antivirus para proteger a los equipos de su infección. Durante este periodo de tiempo el malware puede infectar equipos sin que los antivirus tradicionales sean conscientes de su existencia.

Virus

Programa que se introduce en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

VPN (Virtual Private Network)

Tecnología de red que permite interconectar redes privadas (LAN) utilizando un medio público, como puede ser Internet.

Widget (Panel)

Panel que contiene un gráfico configurable y que representa un aspecto concreto de la seguridad de la red del cliente. El conjunto de widgets forma el dasboard o panel de control de Cytomic EPDR.