CYTOMIC

Guía de administración CYTOMIC Nexus_

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/

Autor : Cytomic

Versión: 1.70

Fecha: 3/19/2024

Acerca de la Guía de administración de CYTOMIC Nexus

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

http://nexus-documents.cytomic.ai/AdvancedGuide/Nexus-Manual-ES.pdf

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

https://nexus-documents.cytomic.ai/Help/v77000//Partners/es-es/index.htm

Información sobre las novedades de la versión

Para conocer las novedades de la última versión de CYTOMIC Nexus consulta la siguiente URL:

http://documents.managedprotection.pandasecurity.com/ReleaseNotes/v77000//Partners/es-es/ReleaseNotes.html

Productos soportados por CYTOMIC Nexus

Advanced EDR

Guía de administración:

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

Ayuda online del producto:

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

Advanced EPDR

Guía de administración

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

Ayuda online del producto:

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

Información técnica sobre módulos y servicios compatibles con CYTOMIC Nexus

Cytomic Insights

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

Cytomic Data Watch

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

Cytomic Patch

Encontrarás más información en el capítulo **Configuración de Cytomic Patch** de las ayudas Web de Advanced EDR, Advanced EPDR.

Cytomic Encryption

También puedes consultar el capítulo **Cytomic Encryption (cifrado de dispositivos)** de las correspondientes guías de administración de Advanced EDR y Advanced EPDR.

Cytomic SIEMConnect

Guía de infraestructura:

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

Manual de descripción de eventos:

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

Tabla de contenidos

Capítulo 1

Prólogo

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

CONTENIDO DEL CAPÍTULO

¿A quién está dirigida esta guía?

La presente documentación tiene como destinatario dos tipos de público:

- Partners o distribuidores vinculados mediante contrato a Cytomic , que aprovisionan y gestionan de forma remota las soluciones de seguridad en sus clientes.
- Compañías de tamaño grande con la gestión del servicio de seguridad informática delegado en cada departamento o centro de trabajo, que quieren establecer y controlar centralizadamente el cumplimiento de las directrices de protección de toda la empresa.

¿Qué es CYTOMIC Nexus?

CYTOMIC Nexus es la solución en la nube que permite al partner y a la gran empresa una gestión sencilla y centralizada del ciclo de vida de sus clientes y usuarios, desde la asignación de versiones de prueba (trial) hasta la configuración remota de sus productos. Todo ello de forma muy simple y centralizando la gestión en una única consola web, disponible en todo momento y desde cualquier lugar.

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.

Consulta en otro capítulo o punto del manual.

Capítulo 2

Información básica de CYTOMIC Nexus

CYTOMIC Nexus es un producto dirigido a proveedores de servicios y grandes compañías que desean gestionar las soluciones de seguridad de sus clientes y usuarios de forma centralizada y desde una única herramienta.

Además, CYTOMIC Nexus ayuda a configurar y a supervisar la seguridad informática de aquellas empresas de tamaño grande que cuentan con centros de trabajo donde el servicio de seguridad se ha delegado en cada departamento técnico local.

CONTENIDO DEL CAPÍTULO

Beneficios de CYTOMIC Nexus

CYTOMIC Nexus es un servicio que Cytomic pone a disposición de sus partners y grandes cuentas para facilitar la gestión de sus clientes y de los productos de seguridad que han adquirido. El uso del servicio reporta los siguientes beneficios:

- Facilitar el control de los clientes y de las delegaciones remotas o departamentos.
- Incrementar la eficiencia de las operaciones.
- Facilitar la venta y adopción de productos de seguridad de Cytomic.

- Mejorar el reconocimiento y la satisfacción de los clientes y usuarios.
- Re-centralizar los servicios de seguridad.

Facilitar el control de los clientes y de las delegaciones remotas o departamentos

- Agiliza la relación del partner con los clientes, almacenando en una única herramienta toda la información necesaria para su gestión diaria (información de contacto etc).
- Mejora la organización y eficiencia interna del partner y de los departamentos técnicos de grandes compañías con un sistema de roles y grupos. Establece diferentes permisos de acceso al usuario de la consola web y niveles de visibilidad sobre los clientes o centros de trabajo.
- Alerta de forma proactiva sobre situaciones de desprotección, visualizando en tiempo real información clave sobre el estado de los clientes y centros de trabajo: productos y módulos asignados, licencias consumidas o a punto de caducar, renovaciones pendientes etc.

Incrementar la eficiencia de las operaciones

- Reduce desplazamientos al permitir instalaciones y mantenimiento remotos, además de disponer de actualizaciones de producto automáticas.
- Reduce el tiempo de gestión de la seguridad de los clientes y centros de trabajo, permitiendo asignar una misma configuración a múltiples destinatarios de forma centralizada.
- Reduce costes minimizando la curva de aprendizaje al gestionar todo el ciclo de venta y la seguridad de los clientes y centros de trabajo desde una única herramienta.

Facilitar la venta y la adopción de productos de seguridad de Cytomic

- **Mayor rotación de los activos en las ventas** y mejora la velocidad al adoptar de nuevas tecnologías: permite ofrecer y asignar licencias de prueba (trial) de los productos de Cytomic en la misma llamada al cliente.
- **Mayor sencillez operativa**: ya no es necesario solicitar la aprobación del proveedor de software para asignar licencias de productos de Cytomic.
- **Mayor flexibilidad**: permite manejar diferentes duraciones de licencias y realizar venta cruzada de las soluciones de Cytomic.

Mejorar el reconocimiento y satisfacción de los clientes y usuarios

Los beneficios obtenidos al utilizar CYTOMIC Nexus redundan a su vez en clientes y usuarios:

- Clientes y usuarios más tranquilos al sentirse protegidos y perfectamente gestionados en todo momento.
- Clientes y usuarios más satisfechos, lo que a su vez promueve recomendaciones hacia nuevos clientes.
- Visibilizar al departamento técnico del partner o gran empresa frente al cliente, personalizando la consola de administración y la protección del equipo del usuario con su identidad corporativa.

Re-centralización del servicio de seguridad

En grandes compañías donde el servicio de seguridad se ha delegado en cada centro de trabajo o departamento, CYTOMIC Nexus permite centralizar su gestión en una única consola con los siguientes beneficios:

- Mayor control del servicio de seguridad ofrecido a nivel global en la empresa.
- Unificar los criterios de seguridad al establecer de forma centralizada las directrices básicas de protección que se aplicarán en todos los centros de trabajo.
- Incrementa la seguridad monitorizando de forma centralizada los resultados de las políticas de seguridad aplicadas en las distintas delegaciones de la empresa.
- Gestión de los casos particulares mediante el acceso centralizado a la consola web de cada departamento / delegación.

Características de CYTOMIC Nexus

Modelo flexible para gestionar las licencias de producto

Soporte de varios modelos de licenciamiento en función de los requisitos de la gran cuenta o del modelo de negocio que el partner tenga implementado:

- **Modelo de licenciamiento mensual**: las licencias asignadas a los clientes le son facturadas al partner mensualmente. Las licencias no tienen caducidad y su duración se extiende hasta que el partner las retira del cliente.
- **Modelo de licenciamiento anual**: las licencias se asignan a los clientes con una duración de 1, 2 o 3 años, y éstas le son facturadas al partner al inicio del periodo, pudiéndolas renovar de forma manual cuando desee o de forma automática cuando caduquen.
- **Modelo de licenciamiento simplificado**: el partner o gran cuenta no desea gestionar las licencias comerciales de sus clientes o usuarios y delega este proceso en Cytomic. Únicamente puede asignar licencias de prueba (trial) desde la consola web de CYTOMIC Nexus. El resto de operaciones se realizan telefónicamente o por mail a través del comercial asignado.

Gestión del ciclo de vida del producto

Crea y asigna directamente desde la consola web versiones de evaluación (trial). Renueva automáticamente las licencias de los clientes y usuarios para aumentar las posibilidades de cross sell y up sell.

Gestión de la seguridad

Instala y despliega servicios de forma remota, ahorrando en costes de desplazamiento y optimizando el tiempo de trabajo. Configurar la solución de seguridad instalada en los equipos de los clientes de forma individual o para todos ellos, ahorrando tiempo de gestión.

En grandes compañías donde se ha delegado la gestión de la seguridad en los distintos centros de trabajo o departamentos que la forman, CYTOMIC Nexus permite centralizar el establecimiento de las directrices de protección.

Crea y administra clientes y grupos de clientes

Registra clientes nuevos y organízalos en grupos para acelerar la configuración del servicio de seguridad y su gestión.

Gestión centralizada desde una única consola web

CYTOMIC Nexus utiliza para su configuración una consola web. Al tratarse de un servicio cloud, es accesible desde cualquier lugar y en cualquier momento, siendo necesario únicamente un navegador compatible. No se requieren desplazamientos ni de configuraciones específicas de la infraestructura de su red ni de la de sus clientes o departamentos en las grande compañías.

Asigna y renueva licencias

Crea y elimina clientes y los servicios que tengan contratados. Renueva de forma automática o anticipada las licencias asignadas, dependiendo del modelo de licenciamiento elegido.

Aplica centralizadamente configuraciones desde la consola web

Diseña políticas de seguridad flexibles y detalladas creando todas las configuraciones necesarias para cubrir las distintas necesidades de las delegaciones de la empresa. Agiliza el despliegue de las políticas de seguridad aplicando las configuraciones de forma centralizada a grupos de clientes con necesidades comunes.

Envía de forma centralizada tareas de análisis y Cytomic Patch

Crea tareas de análisis e instala actualizaciones del sistema operativo y otros programas en todos los equipos de las delegaciones administradas por la oficina central. Visualiza los resultados de forma consolidada.

Accede a la consola web de cada delegación

Accede a todas las consolas web de administración de los productos de seguridad instalados en cada delegación, para facilitar la gestión de situaciones particulares o asignar un tratamiento

especial a usuarios concretos.

Monitoriza la seguridad

Monitoriza y comprueba mediante una única vista integrada el estado de la protección instalada en los equipos de los clientes y centros de trabajo, permitiendo:

- Monitorizar los equipos protegidos y el grupo al que pertenecen.
- Ver las licencias contratadas, consumidas y fecha de próxima caducidad.
- Comprobar el estado de las protecciones instaladas en los equipos.
- Visualizar el porcentaje de equipos que tienen sin actualizar su motor o su fichero de firmas y el de aquéllos con errores, incluidos los que se hayan podido producir a lo largo del proceso de instalación de la protección.
- Visualizar la distribución de los riesgos detectados en los equipos de cada cliente.

Personaliza la consola del cliente (Co-branding)

Cambia el aspecto visual de los productos del cliente para la resaltar su presencia e imagen de marca.

Productos compatibles

Advanced EPDR

Advanced EPDR es una solución basada en múltiples tecnologías de protección que sustituye a los antivirus tradicionales, completando sus carencias y protegiendo a los equipos de la empresa frente a todo tipo de malware, incluyendo APTs (Advanced Persistent Threat) y otras amenazas avanzadas. Para ello Advanced 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. Además, el producto cuenta con las siguientes características:

- Control de la productividad de los usuarios, impidiendo el acceso a recursos web sin relación con la actividad de la empresa y filtrando el correo corporativo para evitar pérdidas de rendimiento provocadas por el spam.
- Control de aplicaciones, cortafuegos, sistema de detección de intrusos y sistemas anti-robo para dispositivos móviles (smartphones y tablets).
- Herramientas de monitorización, análisis forense y resolución para acotar el alcance de los problemas detectados y solucionarlos.
- Servicio multiplataforma alojado en la nube y compatible con Windows, macOS, Linux, Android, iOS y con entornos virtuales y VDI, tanto persistentes como no persistentes.

Advanced EPDR cubre la seguridad de todos los equipos con una única herramienta y no necesita nueva infraestructura IT en la empresa para su gestión y mantenimiento, reduciendo notablemente el TCO de la solución.

Advanced EDR

Advanced EDR es una solución basada en múltiples tecnologías de protección que complementa al antivirus tradicional instalado en el equipo, protegiendo a los equipos de la empresa frente a todo tipo de malware, incluyendo APTs (Advanced Persistent Threat) y otras amenazas avanzadas. Para ello Advanced EDR 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. Además, el producto cuenta con herramientas de monitorización, análisis forense y resolución para acotar el alcance de los problemas detectados y solucionarlos.

Advanced EDR no necesita nueva infraestructura IT en la empresa para su gestión y mantenimiento, reduciendo notablemente el TCO de la solución.

Módulo Cytomic Insights

Advanced EDR 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 de seguridad.

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.

Módulo Cytomic Data Watch

Se trata de un módulo 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 los 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.

Módulo Cytomic Patch

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 excluir el parche problemático de su instalación en el parque del cliente.

Módulo Cytomic Encryption

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. Esta protección adicional es decisiva en casos de robo o pérdida de equipos, o cuando la empresa recicla dispositivos de almacenamiento sin borrar su contenido completamente. Cytomic Encryption 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 módulo 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.

Módulo Cytomic SIEMConnect for Partners

Centraliza en el SIEM del partner todas las detecciones, procesos y programas ejecutados en los dispositivos de sus clientes.

Para poder controlar la aparición de malware, los proveedores de servicios de seguridad necesitan un alto grado de visibilidad de la actividad desarrollada en los equipos de sus clientes. De esta forma, serán capaces de anticiparse a los problemas causados por las amenazas avanzadas que proliferan en el entorno corporativo. Cytomic SIEMConnect for Partners ayuda a los proveedores de servicios de seguridad con este objetivo, al incluir la funcionalidad siguiente:

- Anticipa posibles problemas de seguridad, localizando los programas ejecutados que todavía no han sido clasificados como goodware o malware, y obteniendo información sobre cómo han llegado hasta el equipo (vector de infección).
- Recibe alertas de IOAs (Indicators of Attack) y detecta actividad sospechosa, tal como modificaciones en el registro de Windows o instalación de controladores.
- Monitoriza la ejecución de software legítimo que a menudo es utilizado por atacantes para pasar desapercibidos dentro de la red del cliente, tales como herramientas de scripting o de acceso remoto.

El uso de Cytomic SIEMConnect for Partners simplifica la operativa del SOC del partner y le aporta los siguientes beneficios:

Visibilidad completa de todo lo que se ejecuta en los dispositivos de los clientes

Monitoriza y gestiona la seguridad. Detecta anomalías de forma continua en el entorno de ejecución propio de cada cliente.

Configuración centralizada

Consola de gestión centralizada (CYTOMIC Nexus) que permite establecer configuraciones de Cytomic SIEMConnect for Partners para los clientes del partner de forma sencilla y visual.

Sencillo de instalar, seguro y fácilmente escalable

Configura el servicio de descarga de telemetría una sola vez, e incorpora nuevos clientes sin tener que desplegar ni instalar ningún elemento adicional en sus infraestructuras. Seguridad en la descarga a través de conexiones seguras TLS (Transport Layer Security) desde la nube de Cytomic.

Control de costes de almacenamiento de tu SIEM

Filtra los eventos necesarios antes de que lleguen a la infraestructura del proveedor de servicios de seguridad para minimizar sus costes de almacenamiento.

Compatible con la mayoría de las soluciones SIEM existentes en el mercado

Descarga la telemetría en formato LEEF y CEF, compatible con las soluciones SIEM líderes del mercado, tales como Qradar, AlienVault, Splunk, Devo, etc. y natívamente con Arcsight.

Perfil de usuario de CYTOMIC Nexus

El usuario objetivo de CYTOMIC Nexus es el partner o el departamento técnico de grandes empresas que desean gestionar la seguridad de sus clientes y centros de trabajo de una forma simple y eficiente desde una única consola y con la máxima autonomía.

Tipos de usuarios de CYTOMIC Nexus

- **Resellers**: partners que compran licencias de productos de Cytomic y las revenden a sus clientes sin ofrecer un valor añadido.
- **Managed Service Provider (MSP)**: partners que venden productos de Cytomic a sus clientes y que además gestionan de forma proactiva su seguridad.
- **Mayorista**: partners que adquieren grandes volúmenes de licencias financiando la compra de las mismas. El mayorista distribuye posteriormente las licencias entre sus partners, y son éstos quienes tratan directamente con el cliente final. El mayorista mantiene licencias en stock, de manera que puede ofrecer una respuesta rápida a la demanda de licencias por parte de sus partners.
- **Departamentos de IT**: son grupos de trabajo que operan por lo general desde la sede central de las grandes compañías. Definen, mantienen y controlan las políticas de seguridad que se aplican en todos los centros de trabajo y departamentos de la compañía.

Capítulo 3

La consola de administración

CYTOMIC Nexus utiliza tecnología Web para ofrecer una consola de administración centralizada y alojada en la nube, orientada a facilitar al máximo su utilización.

CONTENIDO DEL CAPÍTULO

Beneficios de la consola web

La consola de administración, también llamada "consola web" o simplemente "consola", es la herramienta principal que se utiliza para asignar y gestionar los servicios de los clientes. Al tratarse de un servicio Web centralizado, posee una serie de características que influyen de forma positiva en la forma de trabajar con ella.

Única herramienta para la gestión completa de los productos

Con la consola web el usuario puede diseñar las políticas de seguridad de sus clientes, asignar las configuraciones de protección a los equipos de los usuarios de forma centralizada y personalizar sus servicios contratados. También permite generar listados detallados del estado de la seguridad y configurar su contenido.

Todas estas funcionalidades se ofrecen desde la misma consola web, lo que evita la complejidad de tener que utilizar diferentes herramientas de gestión de proveedores diferentes. Con la consola web diseñada por Cytomic, la gestión es centralizada, remota y única.

Gestión centralizada para todos los clientes y usuarios desplazados

La consola web de CYTOMIC Nexus está alojada en la nube, por lo que no es necesario realizar ninguna instalación adicional en las oficinas del usuario de la consola web ni de la de los clientes o centros de trabajo remotos, ni es necesario configurar accesos VPN o redireccionar puertos en los routers corporativos.

Al no necesitar de instalación, no conlleva tampoco un aumento de las inversiones en hardware, licencias de sistemas operativos o bases de datos, evitando también la gestión de mantenimientos / garantías para asegurar la operatividad 24/7 del servicio.

Gestión de la seguridad desde cualquier lugar y en cualquier momento

Al tratarse de un servicio cloud, el usuario de la consola web podrá gestionar los productos y la seguridad de los clientes y centros de trabajo desde cualquier lugar y en cualquier momento simplemente con un navegador compatible.

Requisitos de la consola web

Para acceder a la consola web de administración es necesario cumplir con el siguiente listado de requisitos:

- Contar con unas credenciales validas (usuario y contraseña).
- Un navegador compatible certificado.
- Conexión a Internet y comunicación por el puerto 443.

Navegadores certificados

Para acceder a la consola web CYTOMIC Nexus requiere el uso de un navegador web actualizado a la última versión de los proveedores siguientes:

- Chrome
- Internet Explorer
- Microsoft Edge
- Firefox

Otros navegadores no incluidos en el listado (Safari, Opera etc...) también pueden funcionar correctamente.

Acceso a la consola web

El acceso a CYTOMIC Nexus se realiza desde Cytomic Central (**https://central.cytomic.ai**), el punto de partida común par acceder a los servicios de Cytomic alojados en la nube.

Información de la cuenta y salida

Figura 3.1: Información del inicio de sesión, acceso al cierre de la consola web y a Cytomic Central

En la zona superior de la ventana se encuentra disponible en todo momento la información de la cuenta que accedió a la consola web así como los mecanismos para salir de la sesión:

- Regresa a la pantalla de Cytomic Central. Consulta el capítulo **La cuenta Cytomic** en la página **147** para obtener más información.
- **Nombre de usuario**: indica el usuario de la consola web que inicio la sesión en el servicio.
- **Salir**: cierra la sesión y muestra la pantalla de acceso a Cytomic Central.

Estructura general de la consola web

La consola web de CYTOMIC Nexus es una herramienta fácil de utilizar que permite gestionar de forma remota y centralizada los productos asignados a los clientes y la seguridad de los dispositivos.

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

Introducción

Al acceder a la consola web lo primero que se muestra es la ventana principal, correspondiente a la pestaña **Estado** del menú superior.

Esta ventana principal ofrece información resumida sobre el estado general de los clientes así como las licencias disponibles y que no han sido asignadas aún. Se divide en dos secciones:

- La zona de **Licencias** (**1**)
- La zona de **Monitorización** (**2**).

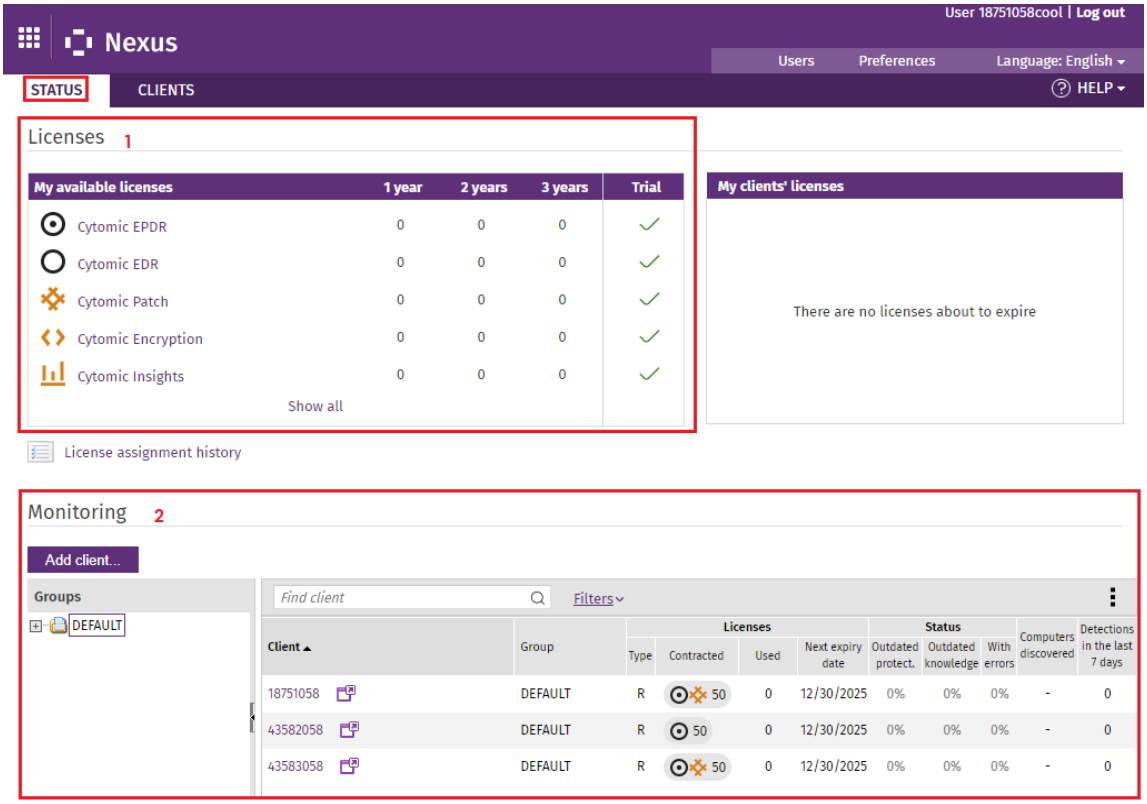

Figura 3.2: Ventana principal de la consola web

Menú superior

Figura 3.3: Menú superior

Es el menú principal de la consola web y permite navegar por las principales secciones del producto:

Estado

Visualiza de forma resumida el estado de los clientes. Dependiendo del modelo de licenciamiento elegido por el partner o por la gran cuenta, mostrará información sobre el tipo de licencias que puede comercializar o asignar a los clientes y centros de trabajo.

Haz clic en la pestaña **Estado** para:

- Mostrar información del tipo de licencias disponibles.
- Acceder al histórico de licencias asignadas.
- Monitorizar las licencias en proceso de asignación.
- Comprobar el estado de la protección desplegada en los equipos

Clientes

Permite administrar los clientes, productos, módulos y las licencias asignadas.

Utiliza la pestaña **Clientes** para:

- Dar de alta nuevos clientes.
- Ordenar clientes mediante agrupaciones.
- Asignar, modificar y renovar licencias.
- Agrupar mantenimientos.
- Crear configuraciones de seguridad y enviarlas a los equipos de usuario de los clientes.

Para obtener más información, consulta el capítulo ***Gestión de clientes*** *en la página* ***39****.*

Ayuda

Este menú proporciona:

- Acceso a la ayuda Web de CYTOMIC Nexus

http://nexus-documents.cytomic.ai/Help/v77000//Partners/es-es/index.htm

- Acceso a la Guía de administración de CYTOMIC Nexus.

http://nexus-documents.cytomic.ai/AdvancedGuide/Nexus-Manual-ES.pdf ,

- Información sobre novedades de CYTOMIC Nexus.

http://documents.managedprotection.pandasecurity.com/ReleaseNotes/v77000//Partners/es-es/ReleaseNotes.html

- Acceso al acuerdo de licencia.
- Información sobre la versión de CYTOMIC Nexus disponible.

Menú Otras opciones

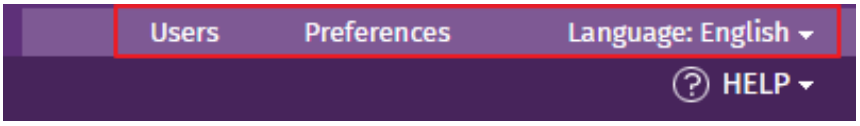

Figura 3.4: Menú Otras opciones

Usuarios

Crea usuarios y les asigna permisos de acceso a la consola web. Consulta el capítulo **Acceso y autorización en CYTOMIC Nexus** en la página **29**.

Preferencias

Establece configuraciones generales para algunos aspectos de la consola web:

Vistas por defecto

Determina la manera en que se muestran los clientes y sus equipos en la consola web.

Notificaciones por correo electrónico

Envía el día 1 de cada mes un informe sobre el número de licencias de los clientes que han caducado o van a caducar próximamente. Consulta el apartado **Aviso por correo de clientes a punto de caducar** en la página **62** para obtener más información.

Permiso de acceso para Cytomic

Autoriza al equipo técnico de Cytomic el acceso a la consola web del usuario, facilitando así la resolución de incidencias.

Idioma

Establece el idioma en el que se muestra la consola web. Los idiomas soportados son:

- Alemán
- Ingles
- Español
- Francés
- Italiano
- Portugués
- Sueco
- Polaco
- Japones
- Chino simplificado
- Chino tradicional

Servicios

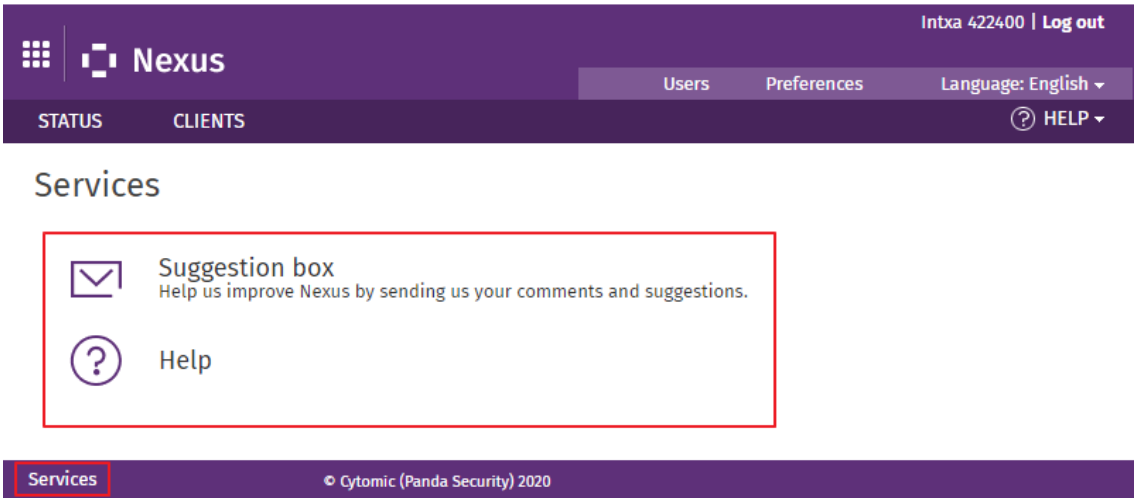

Figura 3.5: Servicios de CYTOMIC Nexus

Haz clic en el vínculo **Servicios** que encontrarás en la barra inferior de la consola web y selecciona:

- **Buzón de sugerencias**: envía sugerencias al equipo de Cytomic encargado de diseñar y desarrollar CYTOMIC Nexus.
- **Ayuda**: accede a la ayuda Web de CYTOMIC Nexus.

Ruta de navegación

La ruta de navegación muestra en todo momento el camino completo de la ventana donde se encuentra el usuario de la consola web.

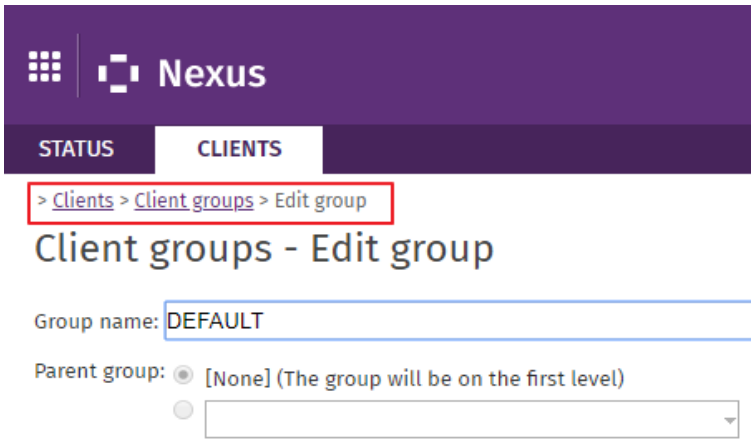

Figura 3.6: Ruta de navegación

Esta ruta está formada por los nombres de las ventanas recorridas hasta llegar a la actual, separadas por el símbolo ">".

Se utilizan hipervínculos para poder retroceder de forma directa a cualquier punto del camino explorado, sin tener que iniciar el recorrido desde el menú superior.

Elementos de configuración

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

- Desplegables de selección
- Combos de selección
- Botones
- Cuadros de texto
- Listados

Cuadros de texto

En muchos casos, la consola realiza un análisis del texto introducido para comprobar que los datos sean correctos (existencia del carácter "@" en cuadros de texto para la introducción de direcciones de correo, comprobación de datos numéricos, etc)

Listados

Para la presentación de listados, CYTOMIC Nexus utiliza tablas. Todas tienen una cabecera que permite establecer un criterio de ordenación:

Figura 3.7: Cabecera de tabla

Haciendo en una cabecera, se selecciona esa columna como referente ascendente de ordenación de la tabla. Volviendo a hacer clic, la ordenación será descendente.

En la parte inferior de las tablas se encuentra la herramienta de paginación.

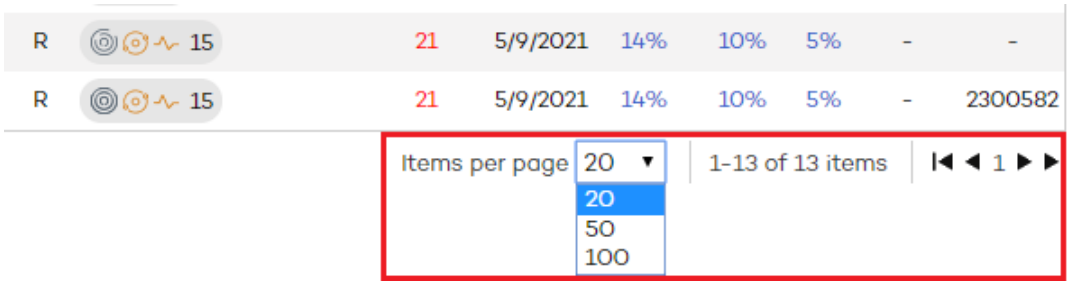

Figura 3.8: Herramienta de paginación

Dependiendo del tipo de tabla, la funcionalidad de esta herramienta varía:

- Selector del número de líneas por página
- Acceso directo a páginas específicas
- Avance de una página
- Retroceso de una página

- Avance hasta la última página
- Retroceso hasta la primera página

Capítulo 4

Acceso y autorización en CYTOMIC Nexus

En este capítulo se detallan los recursos implementados en CYTOMIC Nexus para controlar y supervisar las acciones realizadas por los usuarios de la consola web.

Esta supervisión y control se implementa en forma de dos recursos explicados a lo largo de este capítulo:

- Cuenta de usuario.
- Roles asignados a las cuentas de usuario.

CONTENIDO DEL CAPÍTULO

Concepto de cuenta de usuario

Es un recurso gestionado por CYTOMIC Nexus, formado por un conjunto de información que el sistema utiliza para regular el acceso de los usuarios a la consola web, y establecer las acciones

que éstos podrán realizar sobre los clientes y sus equipos administrados.

Las cuentas de usuario son utilizadas únicamente por los usuarios que acceden a la consola web de CYTOMIC Nexus. Cada usuario necesitará como mínimo una cuenta para acceder a la consola, aunque puede tener más de una con distintos niveles de acceso.

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 usuario que accede a la consola.
- **Contraseña de la cuenta**: asignada una vez creada la cuenta, regula el acceso a la consola de administración.
- **Permiso asignado**: establecido una vez creada la cuenta de usuario, indica las acciones que puede ejecutar en la consola web.
- **Visibilidad**: establece todos los grupos de clientes sobre los que podrá actuar el administrador con la cuenta de usuario creada.

El usuario principal

Es la primera cuenta de usuario que se crea a través del mail de bienvenida enviado por Cytomic. Esta cuenta tiene la siguiente estructura:

- **Nombre de la cuenta**: dirección de correo de contacto del usuario que contrató el servicio.
- **Contraseña de la cuenta**: establecida mediante el correo de activación.
- **Permiso asignado**: **Control total**, descrito en el apartado **Tipos de permisos**.
- **Grupos de clientes**: muestra la visibilidad del usuario de la consola web sobre los diferentes grupos de clientes.

Concepto de permiso

Es una configuración específica de nivel de acceso a la consola que se aplica a una o más cuentas de usuario. De esta forma, un técnico o comercial concreto está autorizado a ver o modificar determinados recursos de la consola, dependiendo del permiso asignado a la cuenta de usuario con la que accedió aCYTOMIC Nexus.

Una cuenta de usuario tiene un único permiso asignado aunque éste pueda estar asignado a una o más cuentas de usuario.

> *Los permisos que se detallan en este capítulo son también aplicables a la parte de la gestión que se realiza desde la consola de CYTOMIC Nexus sobre los productos de la familia Endpoint. Consulta el capítulo* ***Gestión de la configuración de la familia de productos Endpoint*** *en la página* ***73***

Estructura de un permiso

Un permiso está formado por los siguientes elementos:

- **Nombre del permiso**: resume brevemente el acceso a las características de la consola web que tiene las cuentas de usuario con el permiso asignado.
- **Grupos sobre los que tiene visibilidad**: restringe el acceso a determinados clientes. Para configurar esta restricción es necesario especificar las carpetas del árbol de grupos a las cuales la cuenta de usuario tendrá acceso.
- **Tipo de permiso**: determina las acciones concretas que la cuenta de usuario podrá ejecutar sobre los clientes.

¿Por qué son necesarios los permisos?

En un departamento 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 de clientes amplio para administrar, es muy posible que sea necesario organizar o segmentar el acceso a los clientes, aplicando alguno o todos los criterios mostrados a continuación:

Según el tamaño de los clientes a gestionar.

Clientes de tamaño medio/grande pueden necesitar técnicos asignados en exclusiva. De esta forma, los dispositivos de un determinado cliente asignado a un técnico en particular serán invisibles para los técnicos que administran los dispositivos de otros clientes.

Según el tipo de negocio del cliente

Pueden requerirse restricciones de acceso a ciertos clientes por el tipo de negocio que desarrollan o manejar información confidencial. En estos casos se suele requerir una asignación muy precisa de los técnicos que van a poder manipular los dispositivos de este tipo de clientes.

Según la tecnología utilizada por el cliente a gestionar.

Según la infraestructura desplegada en las oficinas del cliente, éste puede ser asignado a uno o varios técnicos expertos en esa tecnología: por ejemplo, los clientes que utilizan servidores de correo Exchange se asignan a un grupo de técnicos especialistas, y de la misma forma, otros clientes con dispositivos Android podrán ser asignados a otro grupo de técnicos.

Según el perfil o conocimientos del técnico.

Según las capacidades de la persona o de su función, se puede asignar un acceso de monitorización/solo lectura o, por el contrario, uno más avanzado que permita acceder a las consolas de los productos contratados por el cliente. Por ejemplo, es frecuente encontrar en departamentos de tamaño grande grupos de técnicos dedicados exclusivamente a configurar las soluciones de seguridad de los dispositivos de sus clientes. A su vez, trabajadores con un perfil más comercial asignan licencias de prueba (trial) a potenciales clientes para ampliar su cartera de clientes, o modifican los mantenimientos de los ya existentes, renovándolos cuando su fecha de finalización se aproxime.

Los criterios descritos 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 Nexus incluye un rol de **Control total** predefinido. A este rol pertenece la cuenta de administración creada por defecto, y con ella es posible realizar absolutamente todas las acciones disponibles en la consola web sobre todos los clientes.

Gestión de usuarios

Para gestionar los usuarios y sus permisos asignados haz clic en **Usuarios**, en el menú **Otras opciones**:

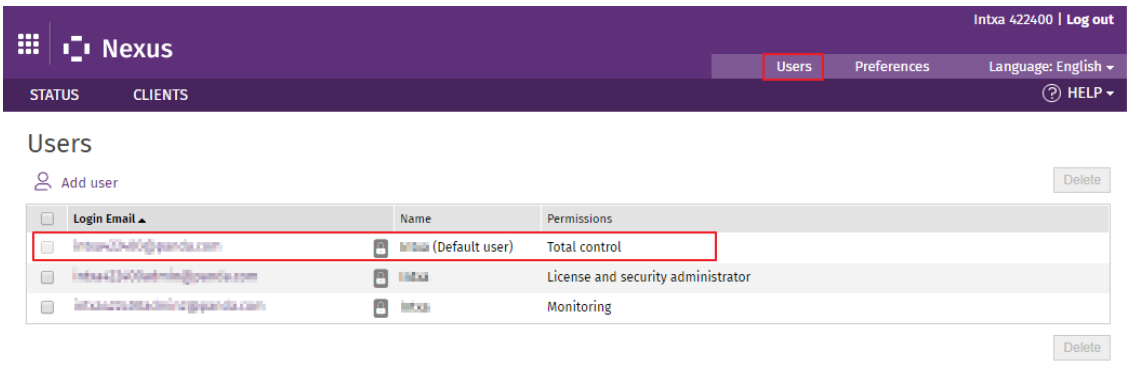

Figura 4.1: Listado de usuarios

Añadir usuarios

Para iniciar el proceso de creación de usuarios, sigue los pasos mostrados a continuación:

En el menú **Otras opciones** haz clic en **Usuarios**, haz clic en el vínculo **Añadir usuario** e introduce los datos necesarios:

- **Correo electrónico**: se utilizará como nombre de usuario.
- **Comentarios**: utiliza este campo si necesitas añadir información adicional.

- **Permisos**: selecciona el permiso que deseas asignar al usuario. Para más información consulta el apartado **Tipos de permisos**.
- **Grupos de clientes**: selecciona los grupos/subgrupos de clientes sobre los que podrá actuar el usuario. La cuenta de usuario con permiso de control total podrá actuar sobre todos los grupos.

> *Si creas un usuario con permiso sobre un grupo y todos sus subgrupos y después añades un nuevo subgrupo, el usuario tendrá permiso automáticamente sobre dicho subgrupo.*
> *Si creas un usuario con permiso solo sobre algunos de los subgrupos de un grupo, y después se añade un nuevo subgrupo, el usuario NO tendrá permiso automáticamente sobre dicho subgrupo.*

- Haz clic en **Añadir**. Se mostrará un mensaje informando del envío de un correo electrónico a la dirección que has especificado al crear el usuario.

Una vez creado, el usuario se mostrará en el listado de la ventana **Usuarios**.

Modificar los datos del usuario

En el menú **Otras opciones** haz clic en **Usuarios** y en el nombre del usuario. Se mostrará la ventana **Edición de usuario** donde podrás modificar:

- El texto del campo **Comentarios**.
- El tipo de permiso.
- El grupo al que pertenece el usuario.

> *En el caso del usuario principal o por defecto solo es posible modificar el contenido del campo **Comentarios**.*

Modificar la información de autorización de la cuenta de usuario

La modificación del nombre, contraseña, correo electrónico del usuario, y el estado de la autenticación en dos pasos se realiza desde Cytomic Central (**https://central.cytomic.ai**). Consulta el capítulo **La cuenta Cytomic** en la página **147**.

Borrar un usuario

Para borrar un usuario, sigue estos pasos:

- En el menú **Otras opciones** haz clic en **Usuarios** y marca la casilla del usuario que deseas borrar.
- Para borrar todos los usuarios utiliza la casilla situada en la cabecera de la tabla, junto a la columna **Email**.
- Haz clic en el botón **Borrar**.

> *En ningún caso es posible borrar el usuario por defecto ni el usuario activo, es decir, aquel con cuyas credenciales haya accedido a la consola web.*

Requerir verificación en dos pasos

Desde el momento en que se establece como requisito un segundo factor de autenticación, el usuario de la consola necesitará un dispositivo adicional y un programa generador de códigos, como por ejemplo Watchguard AuthPoint, para acceder a la consola.

Para establecer como requisito un segundo factor de autenticación a todos los usuarios que acceden a la consola de CYTOMIC Nexus:

- Selecciona el menú superior **Usuarios**. Se abrirá una ventana con el listado de usuarios creados en Partner Center.
- Haz clic en la casilla **Exigir tener activada la verificación en dos pasos para acceder a esta cuenta**. Si la cuenta de usuario que solicita la funcionalidad no tiene activada la verificación en dos pasos, se abrirá la ventana **Verificación en dos pasos** alertando de la situación. Consulta el apartado **Activar la verificación en dos pasos** .

Si un usuario ya tenía iniciada una sesión en la consola en el momento en que se establece el requisito de verificación en dos pasos, su sesión terminará para poder iniciar una nueva con el nuevo factor de autenticación.

Activar la verificación en dos pasos

Para activar la verificación en dos pasos en una cuenta de usuario de CYTOMIC Nexus:

- Descarga de forma gratuita la app WatchGuard AuthPoint compatible con Android en **https://play.google.com/store/apps/details?id=com.watchguard.authpoint** o iOS en **https://apps.apple.com/app/watchguard-authpoint/id1335115425**.
- Accede a Cytomic Central:
    - Escribe las credenciales de la empresa en **https://central.cytomic.ai**.
- Haz clic en el icono  situado en la parte superior derecha de la ventana. Se desplegará un menú.
- Haz clic en la opción **Configurar mi perfil**. Se abrirá la ventana **Panda Cuenta**.

- Haz clic en el panel izquierdo Inicio de sesión y en el enlace **Activar**. Se abrirá la ventana **Sincronización con la app de autenticación**.
- Si es la primera vez que utilizas la aplicación WatchGuard AuthPoint en tu dispositivo móvil, pulsa el botón **Activar**. Si ya la has utilizado anteriormente, pulsa en el icono del QR situado en la esquina superior derecha. Se abrirá la cámara de fotos del dispositivo móvil.

Figura 4.2: Escanear código QR

- Enfoca con la cámara el código QR que se muestra en la consola de CYTOMIC Nexus. Se añadirá una entrada nueva en WatchGuard AuthPoint y se empezarán a generar tokens cada 30 segundos.
- Escribe el código generado por WatchGuard AuthPoint en la consola de Partner Center para enlazar el dispositivo con la cuenta de usuario, y haz clic en el botón **Verificar**. Se abrirá una ventana con el mensaje **Se ha activado la verificación en dos pasos**.
- Haz clic en el botón **Aceptar**. A partir de este momento, el usuario de la consola deberá introducir la cuenta de correo, la contraseña y el token generado por WatchGuard AuthPoint en ese momento.

Tipos de permisos

En CYTOMIC Nexus se establecen cuatro permisos:

- Control total
- Administrador de licencias y seguridad
- Administrador de seguridad
- Monitorización (solo lectura)

En función del permiso que se asigne a un usuario, éste podrá realizar un mayor o menor número de acciones.

Las acciones que el usuario podrá llevar a cabo están relacionadas con diferentes aspectos de la configuración básica y avanzada de la protección. Estas acciones van desde la creación y modificación de sus propias credenciales de usuario hasta la configuración y asignación de perfiles a grupos y equipos, entre otras.

Control total

Este usuario tiene autorización para realizar todas las acciones disponibles en la consola web sobre todos los clientes. Este es el único permiso de la consola web que permite crear otros usuarios.

Gestión de usuarios, grupos y clientes

El usuario podrá:

- Crear, modificar y borrar cualquier usuario excepto borrar el usuario por defecto y el usuario activo.
- Crear, modificar y borrar cualquier grupo menos el grupo DEFAULT.
- Crear, modificar y borrar cualquier cliente.
- Asignar clientes a los grupos y moverlos entre grupos.

Gestión de Licencias

El usuario podrá:

- Modificar el tipo de asignación de licencias a cualquier cliente. Consulta el apartado **Asignar y modificar licencias** en la página **60**.
- Visualizar en el historial de licencias asignadas todas las asignaciones realizadas sobre cualquier cliente y vaciar el listado de asignaciones de dichos clientes.
- Asignar, modificar y borrar licencias de cualquier cliente.
- Asignar, modificar y borrar productos / servicios de cualquier cliente.

Gestión de perfiles

El usuario podrá:

- Acceder con permiso de control total a la consola web de cualquier cliente.
- Gestionar la actualización automática de los perfiles de cualquier cliente.
- Ver los perfiles de cualquier cliente y asignarlos.

Administrador de licencias y seguridad

Este usuario tiene el mismo acceso que un usuario con permiso **Control total** (autorización para realizar todas las acciones disponibles en la consola web) pero limitado a los clientes que tenga acceso. Este usuario no puede crear otros usuarios.

Gestión de usuarios, grupos y clientes

El usuario podrá:

- Modificar sus propias credenciales.
- Gestionar y eliminar los grupos sobre los que tenga acceso menos el grupo DEFAULT.

- Crear, borrar y modificar los clientes a los que tenga acceso.
- Utilizar el campo **Comentario** para introducir información adicional sobre los clientes. Además podrá ver otros datos sobre los que tenga permiso (nombre, teléfono de contacto, fax, etc.).
- Acceder con permiso de control total a las consolas Web de los clientes finales sobre los que tenga acceso.

Gestión de licencias

El usuario podrá:

- Modificar del tipo de asignación de licencias de los clientes que tenga acceso. Consulta el apartado **Asignar y modificar licencias** en la página **60**.
- Visualizar en el historial de licencias asignadas todas las asignaciones realizadas sobre los clientes que tenga acceso y vaciar el listado de asignaciones de dichos clientes.
- Asignar, modificar y borrar licencias de los clientes que tenga acceso.
- Asignar, modificar y borrar productos de los clientes que tenga acceso.
- Asignar, modificar y borrar servicios de los clientes que tenga acceso.

Gestión de perfiles

El usuario podrá:

- Acceder con permiso de control total a la consola web de los clientes a los que tenga acceso.
- Gestionar la actualización automática de los perfiles de los clientes a los que tenga acceso.
- Ver los perfiles de los clientes a los que tenga acceso y asignarlos.

Administrador de seguridad

El usuario poseedor de este permiso puede gestionar la seguridad de los clientes a los que tenga acceso pero no podrá gestionar sus licencias, únicamente podrá visualizarlas. Tampoco podrá crear usuarios en la consola web.

Gestión de usuarios, grupos y clientes

El usuario podrá:

- Modificar sus propias credenciales.
- Gestionar y eliminar los grupos sobre los que tenga acceso menos el grupo DEFAULT.
- Utilizar el campo **Comentario** para introducir información adicional sobre los clientes. Además podrá ver otros datos de los clientes sobre los que tenga permiso (nombre, teléfono de contacto, fax, etc).

Gestión de licencias

El usuario podrá:

- Visualizar en el historial de licencias asignadas las licencias asignadas a clientes que pertenezcan a grupos sobre los que tenga acceso. No podrá vaciar el listado de asignación de licencias.

Gestión de perfiles

El usuario podrá:

- Acceder con permiso de control total a las consolas Web de los clientes finales sobre los que tenga acceso.
- Gestionar la actualización automática de los perfiles de los clientes a los que tenga acceso.

Monitorización (solo lectura)

El usuario poseedor de permiso de monitorización no podrá crear, eliminar ni modificar información alguna en la consola web.

Gestión de usuarios, grupos y clientes

El usuario podrá:

- Modificar sus propias credenciales.
- Acceder a los grupos que se le asignen, ver los clientes de dichos grupos y sus correspondientes perfiles.
- Visualizar el contenido del campo **Comentario** además de otros datos de los clientes sobre los que tenga acceso (nombre, teléfono de contacto, fax, etc.).

Gestión de licencias

El usuario podrá:

- Visualizar la renovación automática de licencias a cualquier cliente de los grupos sobre los que tenga acceso.
- Visualizar en el historial de licencias asignadas las asignaciones realizadas a clientes que pertenezcan a grupos sobre los que tenga acceso, pero no vaciar el listado de asignaciones.

Capítulo 5

Gestión de clientes

Toda la funcionalidad ofrecida por CYTOMIC Nexus se construye en torno al concepto de Cliente, una entidad que representa a dos grupos de usuarios:

- Empresas que han contratado con el partner diferentes servicios de seguridad.
- Delegaciones, departamentos o centros de trabajo dentro de una gran compañía con la gestión de la seguridad delegada.

La entidad Cliente se utiliza para organizar toda la información así como facilitar su seguimiento, liberando recursos del departamento técnico para dedicarlos a tareas más productivas.

El modo de licenciamiento simplificado deCYTOMIC Nexusno permite gestionar clientes mediante la consola Web. Consulta el capítulo ***Gestión de productos y licencias*** *en la página* ***51*** *para obtener más información sobre los modos de licenciamiento disponibles y las capacidades de cada uno de ellos.*

CONTENIDO DEL CAPÍTULO

Crear y eliminar clientes

En este apartado se describe el proceso que debe seguir un usuario de CYTOMIC Nexus para registrar un cliente, asignándole una versión de evaluación o un producto completo. También se describe el proceso para eliminar clientes.

Permisos necesarios

Para poder crear y borrar clientes es necesario que la cuenta de usuario tenga asignado el permiso de control total o de administrador de licencias y seguridad.

*Consulta el apartado **Añadir usuarios** en la página **32** para saber más sobre cómo crear y borrar usuarios, modificar sus datos y asignarles permisos. Consulta el apartado **Tipos de permisos** en la página **35** para conocer los diferentes niveles de gestión posibles en función de los permisos asignados*

Crear clientes

Para crear clientes, se pueden utilizar dos vías:

- La opción **Registrar nuevo cliente** de la ventana **Clientes**.
- El botón **Añadir cliente** de la ventana **Estado** > **Monitorización**

Desde la opción Registrar nuevo cliente

- Haz clic en la pestaña **Clientes**, y a continuación en **Registrar nuevo cliente**.

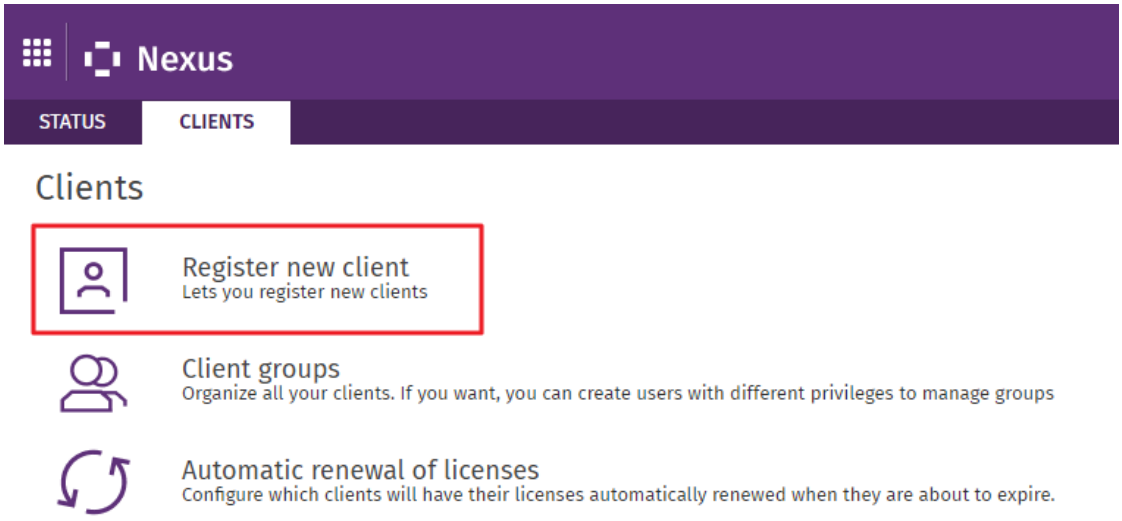

Figura 5.1: Registrar nuevo cliente

- En el formulario de registro, cumplimenta los campos necesarios para dar de alta al cliente y haz clic en el botón **Siguiente**.
- Selecciona el grupo en el que deseas incluir al nuevo cliente. En caso de que no haya ningún grupo configurado, selecciona el grupo por defecto (Default).
- Utiliza los desplegables para seleccionar:
  - **El tipo de licencias que deseas asignar al cliente**: licencias de tipo comercial o licencias de prueba.
  - **El producto de que se trate**.
  - **El periodo de validez de las licencias**: 1, 2 o 3 años.
  - **La cantidad de licencias a asignar**: si la cantidad supera el número de licencias disponibles se mostrará un aviso. .
  - **Módulos adicionales**: en función del producto seleccionado, es posible asignar licencias comerciales o de prueba de módulos que complementan la seguridad y prestaciones del producto elegido.

> *Toda la información sobre los módulos disponibles y sus características se encuentra en el apartado **Productos compatibles** en la página **15***

- Para finalizar el procedimiento haz clic en el botón **Añadir cliente**.

Desde el botón Añadir clientes

- En la sección **Monitorización** de la ventana **Estado**, haz clic en el botón **Añadir cliente**.

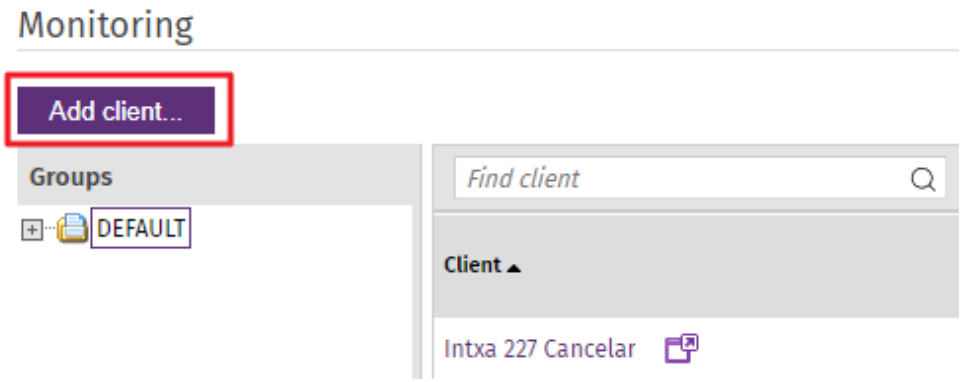

Figura 5.2: Añadir cliente

- Completa todos los campos necesarios del formulario de registro.
- Utiliza los desplegables para asignar licencias al cliente, tal y como se explica en el punto **Desde la opción Registrar nuevo cliente**.

Una vez finalizado el proceso se creará el mantenimiento del cliente, iniciándose así la cuenta atrás del periodo de validez de las licencias.

> *Si la asignación no se realiza de forma inmediata, se mostrará el siguiente texto en la pantalla de estado: **XX licencias en proceso de asignación**. **Ver detalles**. Al hacer clic en el link **Ver Detalles**, se mostrará el detalle de las asignaciones de licencias en curso.*

Una vez que se han asignado licencias al cliente, es posible modificarlas y asignarle otras de los diferentes productos y módulos de seguridad de Cytomic.

> *Para saber más sobre el proceso de gestión de licencias, consulta el capítulo **Gestión de productos y licencias** en la página **51***

Eliminar clientes

En la gestión diaria de los clientes, puede llegar un momento en que sea necesario eliminar alguno de ellos.

Consecuencias de la eliminación

Después de eliminar un cliente, no será posible:

- Recuperar sus datos pasados 90 días desde la fecha de borrado.
- Acceder de nuevo a la consola desde la que se gestionaban los servicios asignados al cliente.

Monitorización de los clientes

Para ver los clientes creados, selecciona el menú superior **Estado**. La información se encuentra en la sección **Monitorización**, y consta de dos partes principales:

- El árbol de grupos **(1)**
- El listado de clientes **(2)**
- La herramienta de filtrado **(3)**

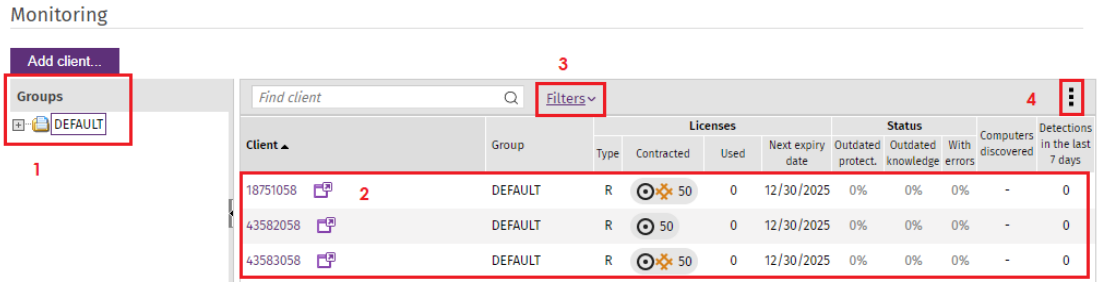

Figura 5.3: Monitorización de clientes

Para que el listado muestre también los clientes que han permanecidos inactivos durante los últimos 90 días, sigue estos pasos:

- Haz clic en **Filtros (3)**.
- Marca la casilla **Mostrar clientes sin servicios activos** y haz clic en el botón **Filtrar**.

Para mostrar solo los clientes pertenecientes a un grupo determinado, selecciona el grupo en el árbol.

Para mostrar todos los clientes de los subgrupos que pertenezcan al grupo seleccionado haz clic en el icono ⋮ **(4)** y activa la opción **Mostrar contenido de los subgrupos**.

El listado de clientes

El listado de clientes ofrece la siguiente información:

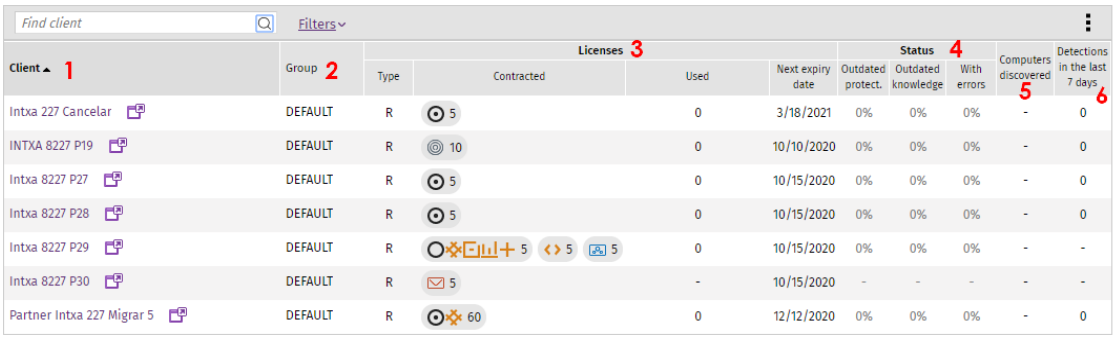

Figura 5.4: Información de listado de clientes

Para ver toda la información sobre el cliente, sitúa el cursor sobre el nombre del cliente y se mostrará una etiqueta con los datos.

Campo	Descripción
Cliente (1)	Nombre o identificador que asigna Cytomic al cliente en el momento del alta. Este identificador se le envía al cliente en el mail de bienvenida y se le solicita en sus comunicaciones con soporte técnico para la tramitación de incidencias. Icono de acceso a la consola del cliente si éste tiene habilitada la opción **Permitir a mi distribuidor acceder a mi consola** en su consola de producto. Consulta **Acceso a la consola del cliente** en la página **58**.
Modo de gestión	Indica si el producto es gestionado de forma centralizada o no. Para más información, consulta el capítulo **Gestión de la configuración de la familia de productos Endpoint** en la página **73**
Grupo (2)	Nombre del grupo al que pertenece el cliente.
Tipo	Indica si el cliente posee productos Trial o Release. Si dispone de ambos, se mostrará como Release.
Licencias (3)	• **Licencias contratadas**: productos o módulos contratados y número de licencias. • **Consumidas**: número de licencias asignadas a los equipos del cliente. • **Próxima fecha de caducidad**: fecha más cercana en la que caducarán algunas o todas las licencias del cliente. • **Protec. desactual.**: porcentaje de equipos de usuario con la protección

Campo	Descripción
	desactualizada
Estado (4)	Muestra mediante porcentajes el estado de la protección instalada en los equipos de los clientes: • **Conocimiento desac.**: % de equipos con el fichero de firmas desactualizado. • **Con errores**: % de equipos con el errores en software de seguridad instalado. • **Equipos descubiertos**: % de equipos detectados en la red pero sin software de seguridad instalado.
Detecciones últimos 7 días (6)	Detecciones realizadas en los últimos 7 días en: • Sistema de ficheros. • Correo electrónico. • Navegación Web. • Aplicaciones de mensajería instantánea. • Bloqueos realizados por el firewall.

Tabla 5.1: Información del listado de clientes

*Para acceder a la ventana de **Detalles del cliente**, haz clic en el nombre del cliente. Para más información, consulta el apartado **Detalles del cliente***

Filtrado de clientes

La herramienta de filtrado consiste en una serie de desplegables que restringen los resultados de la búsqueda en función de las opciones seleccionadas.

Para utilizar los filtros, haz clic en **Filtros** y utiliza los desplegables para seleccionar:

- **Producto**: elige de entre las opciones del desplegable el producto en base al cual acotarás la búsqueda.
- **Tipo de licencia**: licencias comerciales o de prueba.
- **Estado de licencias**:

- Licencias sin caducar.
- Licencias caducadas.
- Licencias que caducarán en el plazo de una semana, dos semanas o dos meses.
- Porcentaje total de licencias consumidas (con más del 80% consumidas o consumidas al 100%).

- **Licencias contratadas**: introduce un número de licencias a partir del cual acotar la búsqueda.
- **Modo de gestión de los productos**:
  - **Todos:** muestra todos los productos, sin distinción alguna por el modo de gestión.
  - **Productos sin gestión centralizada**: consulta el apartado **Configuraciones para los productos de seguridad** en la página **78**

Exportar la lista de clientes

- Para exportar la lista de clientes, haz clic en el icono y selecciona el formato que deseas:
  - **Exportar a excel**
  - **Exportar a csv**
- Para incluir la información de los clientes que dependen de grupos de segundo nivel superior en el árbol de clientes, selecciona **Mostrar contenido de los subgrupos**.

Detalles del cliente

- Para acceder a esta ventana, haz clic en el nombre del cliente allí donde aparezca con formato de vínculo.

La ventana **Detalles del cliente** muestra la siguiente información:

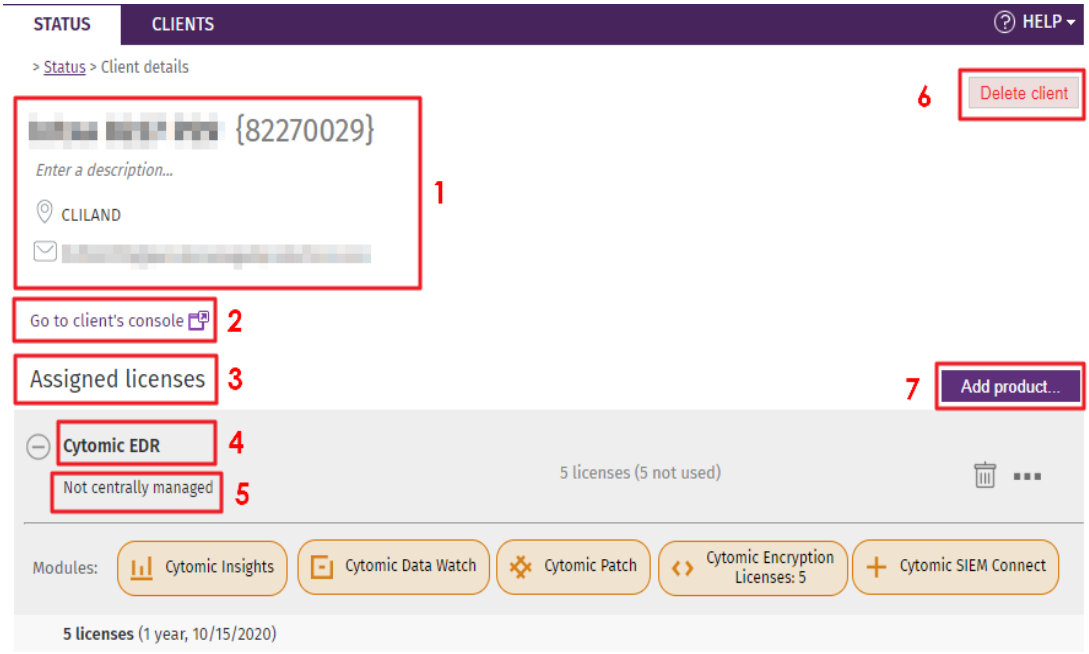

Figura 5.5: Detalles del cliente

- **Datos del cliente (1)**:
  - Nombre y descripción del cliente
  - Datos de contacto (fax, teléfono, correo electrónico, etc)
- **Acceso a la consola del cliente (2)**: para acceder a la consola, haz clic en el icono .
- **Licencias asignadas (3)**
- Utiliza y para desplegar o cerrar la información de detalle de cada línea del informe.
- **Producto contratado por el cliente (4)**: número de licencias contratadas y sin asignar.
- **Modelo de gestión del producto (5)**. Consulta el apartado **Modelos de gestión de servicios** en la página **54** .
- Botón para eliminar cliente (**6**).
- Botón para añadir producto (**7**).

Crear y administrar grupos de clientes

Por qué utilizar grupos de clientes

CYTOMIC Nexus permite agrupar los clientes para implementar dos características orientadas a facilitar la gestión de los clientes:

- Restringir la visibilidad de los usuarios de la consola web con respecto a los clientes que pueden gestionar.
- Agilizar la aplicación de los perfiles de configuración a los clientes gestionados.

Restringir la visibilidad de los usuarios de la consola web

Los departamentos técnicos con estructuras internas grandes y complejas, o que gestionan una gran cantidad de clientes pueden necesitar agruparlos para asignarlos a técnicos específicos que se encargarán de su gestión. Para obtener información sobre los distintos motivos que pueden llevar a segmentar los clientes en grupos, consulta el apartado **¿Por qué son necesarios los permisos?** en la página **31**

CYTOMIC Nexus permite limitar la visibilidad de los usuarios de la consola asignándoles determinados grupos de clientes. De esta manera, su acceso queda limitado a los clientes que pertenecen a los grupos asignados.

Aplicar perfiles de configuración

Mediante la asignación y el envío de perfiles, CYTOMIC Nexus permite aplicar configuraciones a grupos de clientes para ahorrar tiempo de gestión. Para obtener información sobre los perfiles de configuración soportados por CYTOMIC Nexus, consulta el capítulo **Gestión de la configuración de la familia de productos Endpoint** en la página **73** .

Crear grupos de clientes

Para crear un grupo de clientes, sigue los pasos que se detallan a continuación:

- Selecciona el menú superior **Clientes** y haz clic en **Grupos de clientes**.

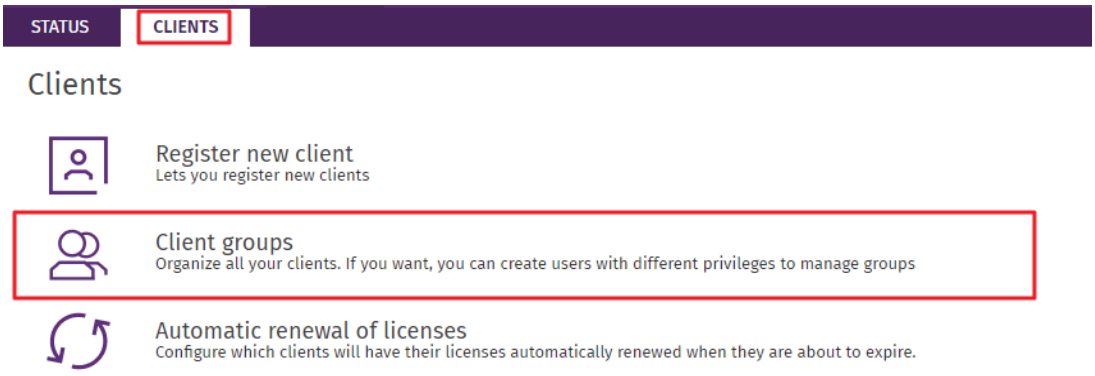

Figura 5.6: Crear grupos de clientes

- Haz clic en el enlace **Crear nuevo grupo** para acceder a la ventana **Grupos de clientes-Edición de grupo**. Rellena los campos mostrados a continuación:
  - **Nombre de grupo**: indica el nombre del nuevo grupo. Es posible crear grupos de clientes con el mismo nombre, siempre y cuando no compartan el mismo grupo "padre".

- **Padre del grupo**: indica el grupo del cual colgará el grupo a crear. Para que el grupo aparezca en el primer nivel del árbol, utiliza la opción **Ninguno (el grupo estará en el primer nivel)**. Para que el grupo dependa de alguno de los grupos ya existentes, selecciona el grupo a través del desplegable.

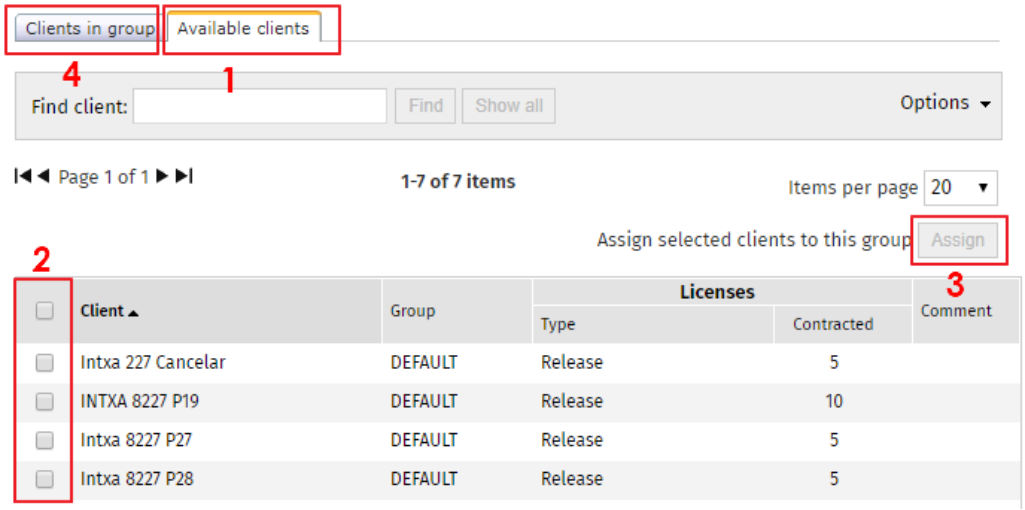

Figura 5.7: Controles para seleccionar los clientes que formarán parte del nuevo grupo

- Selecciona los clientes que formarán parte del grupo a crear: la pestaña **Clientes disponibles (1)** muestra un listado de los clientes que el administrador puede ver según los permisos asignados a su cuenta y que, además, no pertenecen al grupo que está editando. Junto a los clientes aparecen también el número de licencias que tienen contratadas, de qué tipo son así como el posible comentario que tengan asociado. Para seleccionar el cliente que se desea integrar en el grupo, marca la casilla correspondiente **(2)** situada junto al nombre del cliente. Si se trata de varios clientes, marca la casilla de cada uno de ellos.
- Haz clic en **Asignar** (**3**). Comprueba que los clientes seleccionados aparecen en la pestaña **Clientes integrantes (4)**.

Mover clientes de un grupo a otro

- Selecciona la pestaña **Clientes integrantes (4)** y selecciona el cliente o clientes que deseas trasladar marcando las casillas correspondiente.
- Utiliza el desplegable para seleccionar el grupo de destino y haz clic en el botón **Mover**.

Para comprobar si el grupo creado aparece en el nivel correspondiente dentro del árbol de grupos, regresa a la ventana principal **Grupos de clientes**.

Eliminar grupos de clientes

Para borrar algún grupo es necesario que dicho grupo esté vacío, es decir, que no incluya cliente ni subgrupo alguno. Selecciona el grupo y haz clic en **Borrar**.

Capítulo 6

Gestión de productos y licencias

CYTOMIC Nexus ofrece un conjunto de herramientas que proporcionan una gran autonomía al gestionar el tipo de servicio que mejor se adapta a las necesidades de los clientes. De esta manera, se agiliza la relación entre el departamento técnico de los partners, los clientes, y Cytomic a la hora de asignar productos, módulos y licencias.

Dependiendo del modo de licenciamiento, con CYTOMIC Nexus el usuario de la consola web podrá gestionar:

- Los productos asignados a sus clientes y su cambio y / o eliminación.
- La duración y el número de licencias asignadas de cada producto.
- Las renovaciones y cancelaciones del servicio.
- La asignación de versiones de prueba (trials).
- La aplicación de un modelo de gestión centralizada o sin centralizar a los servicios de los clientes.

Para poder gestionar y asignar productos y licencias, la cuenta de usuario utilizada para acceder a la consola web debe tener permisos de control total o de administrador de licencias y seguridad. Consulta el apartado ***Tipos de permisos*** *en la página* ***35****.*

CONTENIDO DEL CAPÍTULO

Conceptos básicos

Para poder utilizar de forma eficiente la gestión de productos y licencias es necesario tener en cuenta los conceptos mostrados a continuación:

- **Mantenimiento**: es la asignación de un número concreto de licencias de duración determinada de un producto o módulo a un cliente.
- **Producto**: solución de seguridad que pertenece al porfolio de Cytomic compatible con CYTOMIC Nexus, y por tanto gestionable por el departamento técnico.
- **Servicio**: es la agrupación de uno o más mantenimientos asociados a un mismo producto.
- **Módulo**: extensión de un producto que le añade funcionalidades adicionales.
- **Licencia**: cada producto de Cytomic puede ser utilizado / instalado en tantos dispositivos como número de licencias tenga asociado en el mantenimiento asignado al cliente.
- **Modelo de gestión**: los productos de Cytomic permiten la delegación completa de su gestión. De esta manera el cliente puede despreocuparse completamente de gestionar el servicio, incrementando de esta forma el valor de los productos de seguridad adquiridos.

Modelos de licenciamiento y funcionalidades disponibles

Dependiendo del modelo de licenciamiento elegido por el partner o por el departamento técnico de las grandes compañías, algunas funcionalidades de CYTOMIC Nexus involucradas en la gestión de clientes quedarán deshabilitadas en la consola web, quedando disponibles a través del comercial asignado:

Funcionalidad	Suscripción mensual	Suscripción anual	Modelo simplificado
Crear y eliminar clientes	Consola Web	Consola Web	Comercial asignado
Asignar licencias comerciales a clientes	Consola Web	Consola Web	Comercial asignado
Asignar licencias de prueba (trial) a clientes	Consola Web	Consola Web	Consola Web
Monitorizar el estado de los clientes	Consola Web	Consola Web	Consola Web
Filtrar y exportar clientes	Consola Web	Consola Web	Consola Web
Gestionar grupos de clientes	Consola Web	Consola Web	Consola Web

Tabla 6.1: Funcionalidades de gestión de clientes y licencias según el modelo de licenciamiento elegido

Productos y módulos disponibles en CYTOMIC Nexus

Productos disponibles

- Advanced EPDR
- Advanced EDR

Módulos disponibles

El usuario de la consola web puede asignar a los clientes módulos adicionales que amplían y complementan determinados aspectos de los productos.

Los módulos disponibles en CYTOMIC Nexus son:

- Cytomic Insights
- Cytomic Data Watch
- Cytomic Encryption
- Cytomic Patch
- Cytomic SIEMConnect for Partners

Por defecto los módulos se asocian al producto con el mismo número de licencias y la misma fecha de caducidad, aunque estos valores pueden cambiarse posteriormente.

Modelos de gestión de servicios

Modelos de gestión de servicios para productos de la familia endpoint

Al asignar un producto de la familia endpoint a un cliente es necesario elegir el modelo de gestión asociado:

- Sin gestión centralizada
- Gestión centralizada desde CYTOMIC Nexus

Sin gestión centralizada

El producto se configura individualmente desde la consola web del cliente. CYTOMIC Nexus no aplicará configuraciones centralizadas a ese producto.

Gestión centralizada desde CYTOMIC Nexus

Al producto del cliente se le aplican las configuraciones centralizadas asignadas desde CYTOMIC Nexus.

Para activar la gestión centralizada, es necesario cumplir ciertos requisitos. También es importante conocer y tener en cuenta las consecuencias que conlleva la gestión centralizada.

Para obtener más información sobre los requisitos necesarios para activar la gestión centralizada, consulta ***Requisitos para asignar configuraciones centralizadas*** *en la página* ***76****.*
Para obtener más información sobre el comportamiento de CYTOMIC Nexus con respecto a la gestión centralizada, consulta ***Configuraciones para los productos de seguridad*** *en la página* ***78****.*

Modelo de gestión por defecto asignado a los productos de seguridad

Asignar productos nuevos

Por defecto, se mostrarán como **Sin gestión centralizada**. Posteriormente, el usuario de la consola web podrá modificar el modelo de gestión.

Añadir una trial superior a un cliente que ya posee productos de seguridad gestionados de forma centralizada

la trial heredará el modelo de gestión centralizado del producto que ya poseía el cliente. Por tanto, la trial será gestionada de forma centralizada desde CYTOMIC Nexus.

Añadir una trial superior a un cliente que posee productos de seguridad sin gestión centralizada

La trial heredará el modelo de gestión centralizado del producto que ya poseía el cliente. En este caso, la trial no podrá ser gestionada de forma centralizada desde CYTOMIC Nexus.

*Consulta **Modelos de gestión de servicios para productos Cytomic***

Establecer y cambiar el modelo de gestión

El modelo de gestión se establece al asignar el producto al cliente en la consola CYTOMIC Nexus. Consulta **Añadir un producto a un cliente existente, caducado o eliminado**.

Para cambiar el modelo de gestión previamente establecido, consulta **Detalles del producto asignado**.

Gestión de productos y módulos

Asignar productos a clientes

Para que un cliente pueda disfrutar de los servicios ofrecidos por Cytomic es necesario que el usuario de la consola web le asigne previamente al menos un producto de una de las familias disponibles.

El proceso de asignación de productos/módulos varía en función de si se trata de un cliente nuevo o de uno ya existente:

- **Para clientes nuevos**: la asignación del producto forma parte del proceso de alta del cliente. Consulta el apartado **Crear y eliminar clientes** en la página **40**.
- **Para clientes existentes, caducados o eliminados antes de 90 días**: consulta el apartado **Añadir un producto a un cliente existente, caducado o eliminado**

> *Si el cliente al que deseas asignar licencias no se muestra en el listado, puede ser porque sus servicios no se hayan mostrado activos durante los últimos 90 días. Consulta el apartado* ***Monitorización de los clientes*** *en la página* ***43***

En el proceso de asignación de producto también se pueden agregar los módulos compatibles necesarios.

Añadir un producto a un cliente existente, caducado o eliminado

- En el menú superior **Estado** accede al detalle del cliente haciendo clic en su nombre desde la lista de la sección **Monitorización**.
- Si el cliente fue eliminado antes de 90 días o su producto esta caducado o eliminado seguirá apareciendo en CYTOMIC Nexus por si el usuario de la consola web quiere reasignar el producto.
- Haz clic en el botón **Añadir producto**.
- Selecciona las características del producto que se añadirá al cliente:

Campo	Descripción
Tipo de licencia	Utiliza el desplegable para seleccionar licencias de prueba (trial) o licencias comerciales.
Producto	Selecciona el producto a asignar al cliente.
Cantidad	Selecciona el número de licencias que deseas asignar.
Periodo	En el modelo de suscripción anual selecciona la duración de las licencias (1, 2 o 3 años). En caso de seleccionar un periodo no habilitado por Cytomic para su uso, se mostrará un aviso.
Módulos adicionales	Según el producto seleccionado se podrán asignar licencias de módulos adicionales. Exceptuando el módulo Cytomic Encryption, no es posible indicar el número de licencias deseadas de los módulos añadidos ya que será el mismo que el del producto principal.

Tabla 6.2: Campos para definir el tipo de producto a asignar al cliente

- Haz clic en el botón **Añadir**. Se mostrará una ventana para elegir el tipo de gestión a configurar: con gestión centralizada o sin gestión centralizada.

Como resultado del proceso el nuevo mantenimiento se mostrará en el detalle del cliente.

Detalles del producto asignado

Una vez asignado el producto al cliente, en la ventana **Detalles** del cliente se mostrará el nombre del producto y el modelo de gestión que tiene aplicado.

> *Consulta el apartado* ***Modelo de gestión por defecto asignado a los productos de seguridad***

Haz clic en ⊖ y ⊕ para desplegar o cerrar la información de detalle de cada línea del informe y en el botón ▪▪▪ (**3**) para acceder a las opciones del menú contextual:

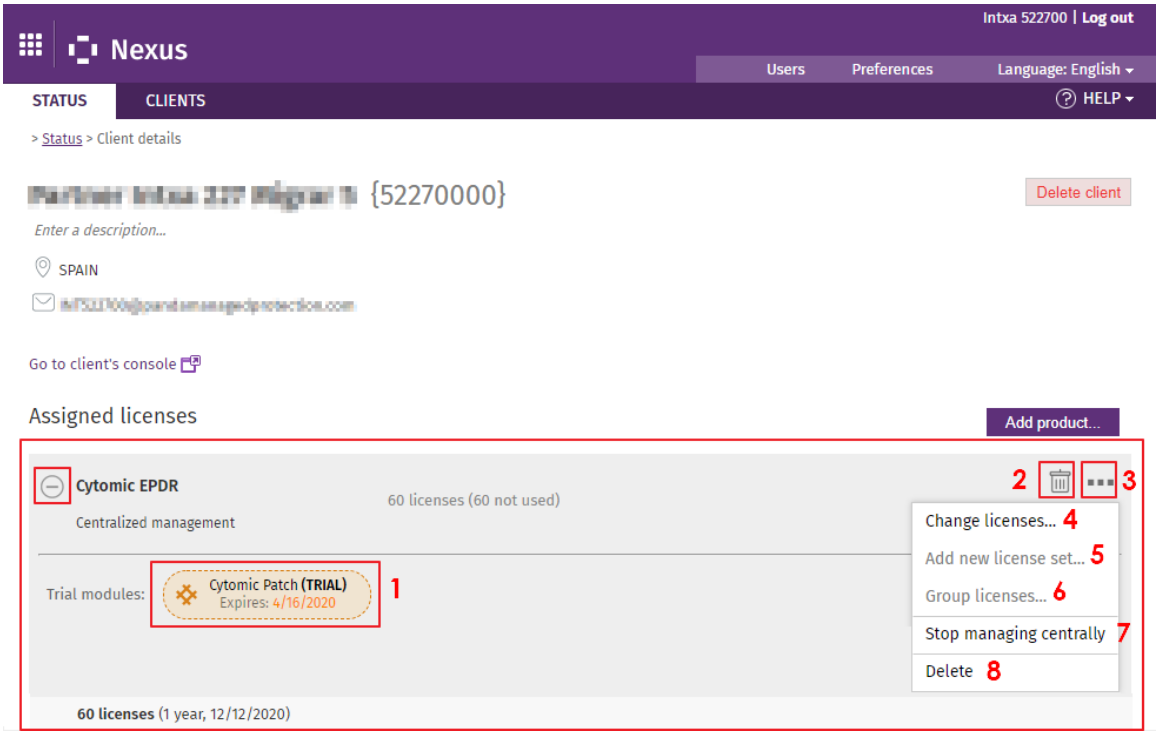

Figura 6.1: Detalles del producto asignado

- Módulos adicionales contratados (**1**): número de licencias contratadas, duración de las licencias y fecha de caducidad.
- Opciones del menú contextual (**3**):
  - Modificar licencias (**4**)
  - Dejar de gestionar/gestionar de forma centralizada (**7**)
  - Opción Borrar (**8**) para eliminar servicios.

Eliminar productos y módulos

Eliminar un producto

- Selecciona el menú superior **Estado**. En el listado de clientes, haz clic en el nombre del cliente para acceder a la ventana **Detalles del cliente**.
- Haz clic en el icono  del servicio a eliminar.
- Haz clic en **Eliminar servicio**. Los clientes perderán los servicios de protección de forma inmediata.

Eliminar módulos

- Selecciona el menú superior **Estado**. En el listado de clientes, haz clic en el nombre del cliente para acceder a la ventana **Detalles del cliente**.
- Haz clic en el icono  situado en la parte derecha de la ventana y selecciona **Modificar licencias**. Accederás a la ventana con la información de todas las licencias que tiene el cliente.
- Desactiva la casilla del módulo a eliminar y haz clic en **Eliminar**. Los clientes perderán los servicios de protección de forma inmediata.

Impacto de la eliminación de productos y módulos

Al eliminar un producto, también se eliminan sus módulos asociados si los hubiere, por lo que el cliente dejará de tener acceso al servicio.

Al eliminar únicamente los módulos asociados al producto, el servicio se mantiene pero se retira el acceso a los módulos.

Acceso a la consola del cliente

Requisitos para acceder a la consola del cliente

El cliente debe activar la opción **Permitir a mi distribuidor acceder a mi consola** en su consola de producto. Esta opción está activada por defecto. En caso de no ser así, el cliente debe seguir los pasos mostrados a continuación en la consola de administración de su producto:

- Selecciona el menú superior **Configuración** y haz clic en el menú lateral **Usuarios**.
- En la pestaña **Usuarios** haz clic en la opción **Permitir a mi distribuidor acceder a mi consola.**

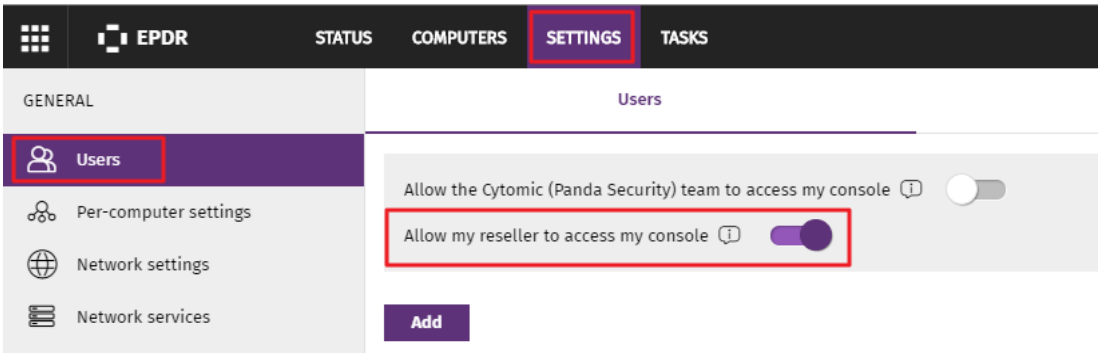

Figura 6.2: Acceso a la opción Permitir a mi distribuidor acceder a mi consola desde la consola del cliente

Acceso a la consola del cliente desde CYTOMIC Nexus

- Selecciona el menú superior **Estado**.
- En el listado **Monitorización** haz clic en el icono situado junto al nombre del cliente. Se mostrará la ventana Cytomic Central con los productos contratados por el cliente.
- Selecciona el producto de seguridad del cliente a gestionar. Se mostrará la consola de administración del cliente.

El acceso a la consola del cliente se realiza mediante la cuenta utilizada para acceder a la consola de CYTOMIC Nexus. El acceso se realiza con el rol Control total asignado.

Gestión de licencias

En la zona **Licencias** accesible desde el menú superior **Estado,** se muestra la información relativa a las licencias. Esta información varía dependiendo del modelo de licenciamiento acordado con Cytomic:

- **Modelo de suscripción mensual**: indica las licencias de los productos que se pueden asignar a los clientes, tanto comerciales como de prueba (trial). En este modelo, la duración de las licencias no está establecida de antemano ya que es el usuario de la consola web el que marca el final del servicio cuando retira de forma manual las licencias de los clientes.
- **Modelo de suscripción anual**: indica el tipo de licencias y qué productos se pueden asignar a los clientes: licencias de 1, 2, 3 años o de prueba (trial).
- **Modelo de licenciamiento simple**: no reporta ningún tipo de información ya que las licencias se gestionan vía telefónica a través del comercial asignado.

El panel de licencias permite saber qué licencias asignadas a los clientes están caducadas o próximas a caducar y además, para ofrecer un mayor control, CYTOMIC Nexus proporciona un historial de licencias asignadas a sus clientes.

Asignar y modificar licencias

La asignación y/o modificación del número de licencias de un producto a un cliente se puede producir en varios momentos diferentes dentro de su ciclo de vida:

- **En la asignación del producto al cliente**: es necesario indicar el número de licencias y su tipo para completar la asignación del producto al cliente. Consulta el apartado **Asignar productos a clientes**.
- **Cuando el número de equipos instalados en el cliente supera el número de licencias asignadas**: el usuario de la consola web podrá incrementar de forma manual el número de licencias asignadas.
- **Cuando el cliente retira equipos de la red**: el usuario de la consola web podrá reducir el número de licencias asignadas al cliente de forma manual.

Asignación de licencias de prueba (trial)

CYTOMIC Nexus facilita el upsell y crossell de productos, así como la captación de nuevos clientes mediante la asignación de licencias de prueba. Las licencias de prueba ofrecen al cliente toda la funcionalidad del producto durante un periodo de tiempo limitado; una vez terminado, el acceso al producto quedará deshabilitado automáticamente.

Para dar licencias de prueba a un cliente es necesario asignarle un nuevo producto con licencia de tipo **Licencia de prueba**. Consulta el apartado **Asignar productos a clientes**.

A la hora de asignar licencias de prueba es necesario tener en cuenta las siguientes consideraciones:

- La duración del periodo de prueba es de 1 mes y no se puede modificar.
- El número de licencias asignadas por cada cliente es 100.
- No se permite asignar un producto en pruebas si el cliente tuvo ese mismo producto en pruebas o con licencia comercial en los 3 últimos meses.

Renovar licencias

El proceso de renovación de licencias extiende por una cantidad de tiempo las licencias de los productos asignados al cliente. Esta renovación puede hacerse de forma anticipada (manual) o de forma automática. A continuación se explican ambos métodos de renovación de licencias.

Renovación anticipada (manual) de licencias anuales

Cuando el usuario de la consola web tiene conocimiento de la finalización próxima de las licencias de un cliente, puede iniciar el proceso de renovación anticipada de licencias para evitar que los equipos queden desprotegidos.

> ⚠ *Solo se permite renovar de forma anticipada los productos cuya fecha de caducidad es menor a 1 año.*

Para renovar anticipadamente un mantenimiento:

- En el menú superior **Estado** haz clic en el nombre del cliente dentro de la sección **Monitorización** para acceder a la ventana **Detalles del cliente**.
- Haz clic en el menú de contexto ▮▮▮ y selecciona **Modificar licencias** en el menú de contexto. Accederás a la ventana desde la que podrás elegir el producto cuyas licencias hay que renovar.
- En el campo **Renovar por** indica la duración de las licencias que serán asignadas al producto cuando éste caduque y haz clic en el botón **Modificar**.

Una vez completado el procedimiento el mantenimiento será modificado con la nueva fecha de finalización.

Renovación automática de licencias

CYTOMIC Nexus permite renovar automáticamente las licencias de los productos y módulos asignados a los clientes. De esta manera la gestión se simplifica al no tener que controlar diariamente qué clientes tienen productos con licencias a punto de caducar para iniciar una renovación manual / anticipada.

A la hora de configurar el proceso, el usuario de la consola web solo podrá elegir renovar automáticamente el producto principal. Cuando llegue la fecha de renovación se renovará el producto, y si éste tiene algún servicio adicional o módulo asociado, éstos también se renovarán automáticamente.

Configurar la renovación automática de licencias

En el menú superior, haz clic en la pestaña **Clientes** y luego en **Renovación automática de licencias**. Accederás a la ventana **Renovación automática**, que muestra **La zona de búsqueda** y **El listado de clientes**:

La zona de búsqueda

Localiza de forma rápida los clientes a configurar la renovación automática. Haz clic en **Opciones** > **Mostrar filtro** para desplegar las opciones de búsqueda. Si se utilizan varios criterios de búsqueda se aplicará un AND lógico.

Campo	Descripción
Buscar cliente	Filtra el listado por el nombre del cliente. Admite búsquedas parciales y no se distinguen mayúsculas y minúsculas.

Campo	Descripción
Grupo	Filtra el listado por el grupo al que pertenece el cliente. Admite búsquedas parciales y no se distinguen mayúsculas y minúsculas

Tabla 6.3: Opciones de búsqueda en el listado de renovación automática

El listado de clientes

Muestra un listado de todos los clientes indicando si son compatibles o no con la funcionalidad y si lo son, permite establecerla. Se muestra la información mostrada a continuación:

Campo	Descripción
Cliente	Muestra el nombre del cliente y un enlace para acceder a la ventana **Detalles del cliente.** Consulta el apartado **Detalles del cliente** en la página **46** para obtener más información. Bajo el nombre del cliente, se muestra el nombre del producto, el número de licencias contratadas y fecha de la caducidad de licencias más próxima. Al situar el cursor sobre el nombre de producto o número de licencias, obtendrás información adicional.
Grupo	Muestra el grupo al que pertenece el cliente.
Producto	Permite indicar mediante un desplegable el comportamiento de la funcionalidad de renovación automática: • **No disponible**: el producto no es compatible con la funcionalidad. • **Do not automatically renew**: The client's licenses will be renewed early/manually. • **Con lic. de 1 año**: al caducar las licencias asignadas al cliente, éstas se renovarán automáticamente por 1 año. • **Con lic. de 2 años**: al caducar las licencias asignadas al cliente, éstas se renovarán automáticamente por 2 años. • **Con lic. de 3 años**: al caducar las licencias asignadas al cliente, éstas se renovarán automáticamente por 3 años.

Tabla 6.4: Opciones de búsqueda en el listado de asignación automática

Aviso por correo de clientes a punto de caducar

Para evitar el acceso diario a la consola web con el fin de comprobar si hay algún cliente que va a caducar en fechas próximas, CYTOMIC Nexus enviará un correo electrónico de advertencia al

usuario de la consola web. Este correo electrónico se envía el día 1 de cada mes y contiene una lista de los clientes que han caducado o van a caducar próximamente junto a su número de licencias. Esta información también está disponible en la zona de licencias de la pantalla **Estado**, en la sección **Licencias de mis clientes**.

En el mensaje de correo electrónico enviado se incluye una hoja de cálculo con los siguientes datos:

- Licencias adicionales necesarias para renovaciones (en caso de que se disponga de stock suficiente para renovar todas las licencias de sus clientes).
- Clientes con licencias próximas a caducar.

Para activar el envío del correo sigue los pasos mostrados a continuación:

- Haz clic en **Preferencias**, en el menú de **Otras opciones**. Se mostrará la ventana de preferencias.
- En la sección **Notificaciones por correo electrónico** habilita la opción **Enviar un correo electrónico con las licencias que van a caducar en los próximos 60 días** y rellena los campos siguientes:
    - Asunto del mensaje
    - **Dirección de correo**: para enviar el mensaje a varios destinatarios, sepáralos con el carácter ";"

Modificar licencias y productos asignados

Durante la gestión diaria de sus clientes, el usuario de la consola web puede necesitar modificar las licencias de los productos asignados, o incluso mejorar el producto asignado para adaptar el servicio que ofrece a las necesidades cambiantes de los clientes.

A la hora de modificar un producto o su número de licencias se aplican las siguientes restricciones:

- No se permiten reducciones del número de licencias ejecutadas de forma individual. Solo se permiten reducciones del número de licencias si se realizan junto a una renovación anticipada dentro de los 3 últimos meses de la duración de las licencias. Consulta el apartado **Renovación anticipada (manual) de licencias anuales** para obtener más información.

> ⚠ *La reducción y modificación de la duración de licencias se aplica de forma instantánea al cliente.*

- Solo se permite el cambio de producto a uno superior dentro de la familia a la que pertenece.

Mejorar el producto y/o incrementar el número de licencias comerciales

Para incrementar el número de licencias y mejorar el producto asignado sigue los pasos mostrados a continuación:

- Selecciona el menú superior **Estado** y en el panel de clientes haz clic en el cliente a modificar.
- Pasa el ratón por encima del icono ■■■ del producto a modificar y elige la opción **Modificar licencias**. Se mostrará una ventana con las características del mantenimiento actual.
- Modifica el producto, número de licencias y acceso a módulos y haz clic en el botón **Modificar**. Se indicarán los nuevos consumos de licencias.

Modificar licencias de prueba (conversión de trial a comercial)

Con CYTOMIC Nexus es posible convertir una licencia de prueba en una comercial e incluso cambiar de un producto en pruebas a otro. Se aplican las siguientes restricciones a la hora de modificar licencias de prueba:

- No se permite cambiar el número de licencias de prueba establecido por producto (consulta el apartado **Asignación de licencias de prueba (trial)**) ni su duración.
- **Cambio del producto en pruebas a otro producto en pruebas**: no se permite el paso de un producto en pruebas a otro.
- **Cambio de un producto en pruebas a un producto comercial**: se permite cambiar el tipo de licencia a comercial, seleccionar servicios adicionales y el número y duración de las licencias.

Modificar el modelo de gestión de Panda Systems Management

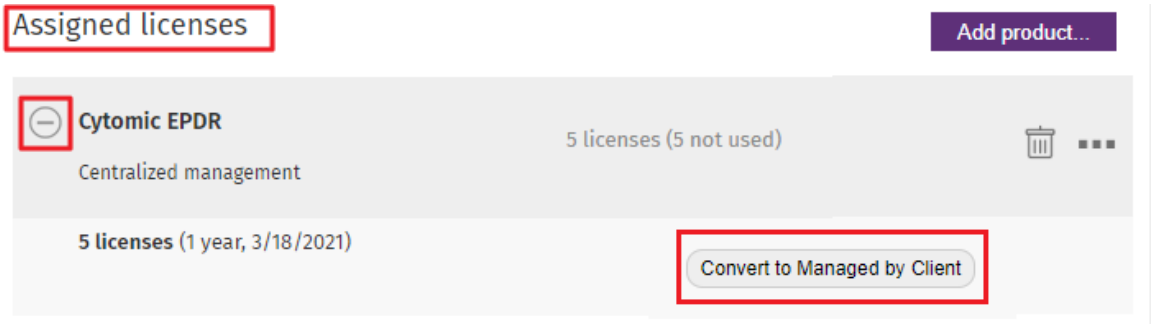

Figura 6.3: Información sobre licencias asignadas al producto

Modificar el modo de gestión de los productos de seguridad

> *Consulta el apartado **Consecuencias de modificar el modo de gestión** para ver un resumen de los efectos en la configuración de seguridad del cliente al cambiar el modelo de gestión de sus productos.*

Para gestionar centralizadamente el producto de seguridad del cliente:

- Consulta **Requisitos para asignar configuraciones centralizadas** en la página **76**.
- Selecciona el menú superior **Estado** y en el panel de clientes haz clic en el cliente a modificar.
- En la ventana **Detalle del cliente**, haz clic en el menú contextual ▮▮▮.
- Selecciona **Gestionar de forma centralizada**. Se mostrará un mensaje advirtiendo de los cambios que acarrea este modelo de gestión y un enlace para obtener más información. Si estás seguro de aplicar el cambio, haz clic en el botón **Sí**.

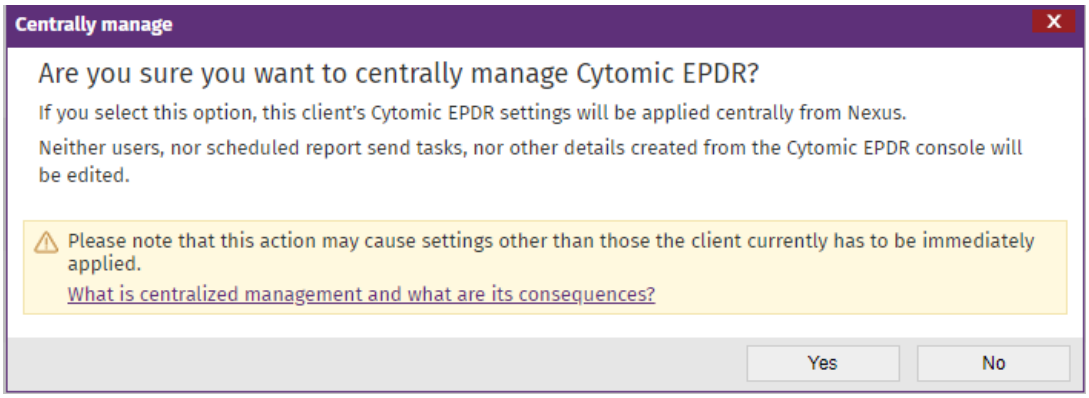

Figura 6.4: Gestionar el producto de forma centralizada

Para dejar de gestionar el producto de forma centralizada:

- En el listado de clientes haz clic en el nombre del cliente.
- En la ventana **Detalle del cliente**, haz clic en el menú contextual ▮▮▮.
- Selecciona **Dejar de gestionar de forma centralizada** y selecciona **Sí**.

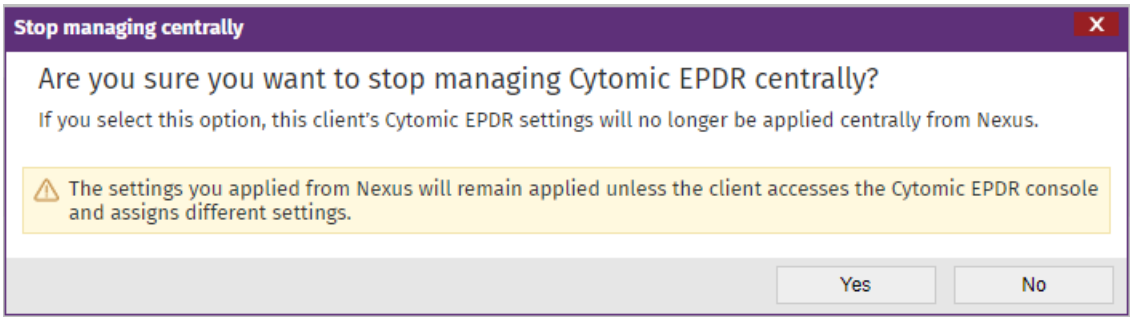

Figura 6.5: Dejar de gestionar el producto de forma centralizada

Consecuencias de modificar el modo de gestión

Cuando se modifica el modo de gestión de un cliente, es posible que se apliquen de forma inmediata configuraciones a los productos del cliente diferentes a las que tenía previamente asignadas. Por ello, es importante conocer las consecuencias del cambio de modelo de gestión.

Gestión centralizada desde CYTOMIC Nexus:

- Al producto del cliente se le aplican las configuraciones de forma centralizada desde CYTOMIC Nexus.

> *Para conocer en detalle cómo interactúan entre sí las configuraciones establecidas por el cliente y por el usuario de CYTOMIC Nexus, consulta el capítulo* ***Gestión de la configuración de la familia de productos Endpoint*** *en la página 73*

Sin gestión centralizada:

- La configuración del producto se realiza únicamente desde la consola web del producto del cliente.
- Las configuraciones previamente aplicadas desde CYTOMIC Nexus permanecen en vigor mientras el administrador de la red no las cambie desde la consola del producto.

Gestionar equipos desprotegidos

Cuando un cliente no dispone de licencias suficientes para proteger todos sus equipos, algunos de ellos quedarán desprotegidos. Esto implica que su protección no se actualizará y que la información procedente de estos equipos no será tenida en cuenta a efecto de las estadísticas, informes y análisis realizados por CYTOMIC Nexus.

Los equipos afectados por esta situación revertirán automáticamente a su estado de protegido en el momento en que el cliente disponga de las licencias suficientes, para lo cual el usuario de la consola web deberá realizar alguna de las acciones siguientes:

- Si hay nuevos equipos en la red sin proteger por no disponer el cliente de licencias sin asignar, el usuario de la consola web deberá modificar el número de licencias para añadir los nuevos equipos del cliente. Consulta el apartado **Modificar licencias y productos asignados**.
- Si hay equipos previamente protegidos en la red del cliente con licencias cuya duración ha terminado, el usuario de la consola web deberá renovar los mantenimientos afectados.

Visualizar los equipos caducados en la consola web

Para ver los equipos de los clientes sin licencias es necesario exportar el listado de clientes:

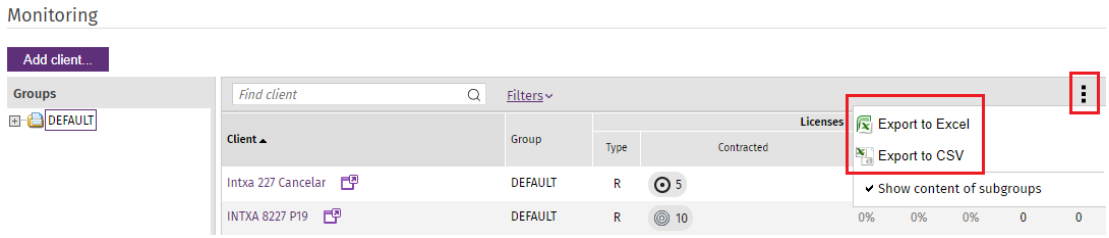

Figura 6.6: Exportar listado de clientes

- En la sección **Monitorización** del menú superior **Estado**, haz clic en el menú de contexto y selecciona el formato en el que quieres exportar el listado: Excel o .CSV.
- Abre el informe. Los equipos con licencia caducada se muestran en la columna **Equipos sin licencia**.

Obtener un listado por correo de los equipos caducados

Consulta el apartado **Aviso por correo de clientes a punto de caducar** para obtener información de cómo configurar el envío de un correo con los clientes con productos caducados o a punto de caducar.

Visualizar el estado de las licencias

La zona de licencias

La zona de licencias es lo primero que se muestra al usuario al acceder a la consola web de CYTOMIC Nexus.

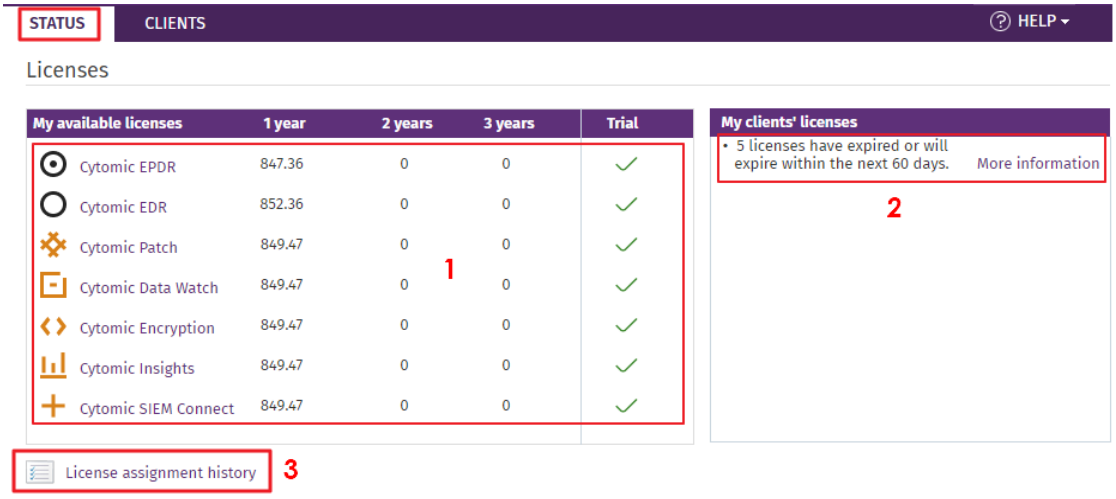

Figura 6.7: Zona de licencias

La información se organiza en las siguientes áreas:

Mis licencias disponibles (1)

Muestra las licencias disponibles de los diferentes productos, incluyendo:

Campo	Descripción
Nombre del producto	Haz clic en el producto para acceder a su información detallada.
Duración de las licencias	Dependiendo del modelo de licenciamiento elegido este panel mostrará la siguiente información: • **Modelo de licenciamiento mensual**: mostrará los productos que disponibles para su venta. • **Modelo de licenciamiento anual**: mostrará el tipo de licencias (1, 2 o 3 años) y los productos disponibles para su venta. • **Modelo de licenciamiento simple**: este panel no mostrará información relevante.
Trial	Indica si CYTOMIC Nexus admite la asignación de licencias de tipo trial para ese producto.

Tabla 6.5: Campos del listado Mis licencias disponibles

Licencias de mis clientes (2):

Informa sobre el número de licencias de los clientes que están caducadas o próximas a estarlo. Incluye:

- Avisos relacionados con las licencias asignadas a los clientes.
- Vínculo **Más información**: haz clic en él para generar el informe de licencias caducadas.

Licencias en proceso de asignación (3)

Indica el número de licencias que no han sido asignadas de forma inmediata. Haz clic en el vínculo **Ver detalles** para más información.

Historial de licencias asignadas (4)

CYTOMIC Nexus proporciona un historial que permite ver todas las asignaciones de licencias que ha hecho.

Licencias en proceso de asignación

Al asignar licencias a los clientes, si la asignación no se realiza de forma inmediata visualizarás el texto **XX licencias en proceso de asignación**. Ver detalles en la zona de licencias. Al hacer clic en el vínculo **Ver detalles**, accederás a la ventana **Licencias en proceso de asignación**, que muestra la siguiente información:

Campo	Descripción
Tipo	Nombre del producto cuyas licencias están en proceso de asignación.
Periodo del servicio	Duración de las licencias (1, 2 o 3 años).
Cantidad	Número de licencias en proceso de asignación.
Cliente	Nombre del cliente al que se han asignado las licencias. Al hacer clic en el nombre, se accederá a la ventana **Detalles del cliente** en la página **46**.
Grupo	Grupo al que pertenece el cliente.

Tabla 6.6: Campos de la ventana Licencias en proceso de asignación

Historial de licencias asignadas

El historial de asignación de licencias lleva el control de todas las operaciones que han involucrado una modificación de las licencias asignadas a los clientes.

Para acceder al historial, selecicona el menú superior **Estado** y haz clic en el enlace **Historial de licencias asignadas**.

La ventana **Historial de licencias asignadas** se divide en dos áreas fundamentales:

- La zona de búsqueda
- El listado de licencias asignadas

La zona de búsqueda

En la zona de búsqueda, se muestran los siguientes campos:

Campo	Descripción
Opciones > Mostrar filtro	Muestra todos los campos de búsqueda.
Buscar	Introduce el nombre de cliente, grupo o usuario de la consola web cuyas asociaciones de licencias quieres visualizar. La búsqueda no tiene en cuenta las mayúsculas y minúsculas y permite realizar búsquedas parciales por subcadenas.
Tipo de asignación	Selecciona en el desplegable el tipo de asignación que se utilizó para asignar las licencias al cliente. Consulta la tabla **Tipos de asignación de licencias utilizadas** .
Producto	Selecciona el producto de las licencias asignadas a buscar.
Fecha desde	Haz clic en el icono para desplazarte por el calendario hasta la fecha a partir de la cual quieres buscar las licencias.
Fecha hasta	Haz clic en el calendario para desplazarte hasta la fecha límite de búsqueda de las licencias.
Mostrar todos	Muestra todos los clientes a los que se han asignado licencias sin importar los criterios de búsqueda establecidos.
Exportar a	Exporta el listado en formato excel o CSV.
Limpiar historial	Borra todos los registros del historial. Esta información no podrá ser recuperada.

Tabla 6.7: Criterios de filtrado en la zona de búsqueda

Tipos de asignación disponibles:

Campo	Descripción
Asignación manual	Consulta el apartado **Asignar y modificar licencias**.

Campo	Descripción
Renovación	Consulta el apartado **Renovación anticipada (manual) de licencias anuales**.
Renovación automática	Consulta el apartado **Renovación automática de licencias**.
Cambio de servicio	Consulta el apartado **Modificar licencias y productos asignados**.
Cancelación de servicio	Consulta el apartado **Eliminar productos y módulos**.

Tabla 6.8: Tipos de asignación de licencias utilizadas

El listado historial de licencias asignadas

En esta zona se muestran los datos resultantes de aplicar el filtro especificado en la zona de búsqueda. La información se distribuye en las siguientes columnas:

Campo	Descripción
Fecha	Día y hora en que se registró la operación.
Producto	Nombre del producto sobre el que se realizó la operación.
Periodo	Duración de las licencias sobre las que se realizó la operación
Número de licencias	Numero de licencias afectadas por la operación registrada.
Cliente	Nombre del cliente que resultó afectado por la operación.
Grupo	Grupo al que pertenece el cliente afectado por la operación.
Asignado por	Cuenta usuario de la consola web que efectuó la operación.
Tipo asignación	Tipo de operación registrada: • **Manual**: las licencias fueron asignadas desde la consola web de forma manual por el administrador. Consulta el apartado **Asignar y modificar licencias**. • **Auto-renovaciones**: las licencias se renovaron de forma automática.

Campo	Descripción
	Consulta el apartado **Renovación automática de licencias** • **Cancelaciones de mantenimientos, servicios y clientes**: Consulta el apartado **Eliminar productos y módulos** y **Eliminar clientes** en la página **42**. • **Cambio de servicio**: Consulta el apartado **Modificar licencias y productos asignados**. • **Renovación de mantenimiento**: Consulta el apartado **Renovar licencias**.

Tabla 6.9: Campos del listado Historial de licencias asignadas

Capítulo 7

Gestión de la configuración de la familia de productos Endpoint

CYTOMIC Nexus ofrece capacidades avanzadas para gestionar la seguridad de los clientes que hayan adquirido productos que pertenecen a la familia Endpoint:

- Configurar el funcionamiento de todos los productos de seguridad instalados en los clientes.
- Personalizar el aspecto de la consola del cliente, modificando los colores y logotipos para potenciar la imagen de marca.
- Minimizar el tiempo de gestión, agilizando la asignación de configuraciones al aprovechar las características avanzadas de herencia implementadas en Cytomic.

CONTENIDO DEL CAPÍTULO

Consola web de CYTOMIC Nexus y Consola web del cliente

La configuración centralizada de productos abre la posibilidad de que una configuración establecida por el partner colisione con la configuración previamente establecida por el cliente. Para resolver este tipo de situaciones se establecen prioridades de configuraciones, que dependen de su origen (consola donde fueron creadas):

- Las configuraciones que establece el partner se crean y envían siempre desde la consola web de CYTOMIC Nexus.
- Las configuraciones que establece el administrador de la red se crean siempre desde la consola web del cliente.

El acceso de forma individual a la consola del cliente por parte del partner y la posterior creación de configuraciones quedan fuera de la dinámica de gestión centralizada de configuraciones tratada en esta sección. Por esta razón, no se tendrá en cuenta esta posibilidad al describir las prioridades de la configuraciones creadas por el partner y por el usuario.

Configuración centralizada de productos

Las funcionalidades de CYTOMIC Nexus con respecto a los productos que pertenecen a la familia Endpoint instalados en los clientes son:

- Crear y asignar/mostrar los perfiles de configuración de los productos de seguridad a uno, varios o todos los clientes administrados por el usuario de la consola web.

- Configurar de forma avanzada el aspecto de la consola que se muestra al cliente para adaptarla a los colores y a la imagen de marca.
- Asignación y envío ágil de configuraciones a los clientes mediante el árbol de equipos, aprovechando las características implementadas de herencia.
- Integración con el sistema de permisos de CYTOMIC Nexus: el árbol de clientes se adapta, limitando la información mostrada en función de la visibilidad del permiso asociado a la cuenta del usuario de la consola web. También se limita la modificación de las configuraciones en función del permiso y de la visibilidad de la cuenta.

Productos y módulos compatibles

Muchos de los conceptos necesarios para manejar CYTOMIC Nexus son heredados de la plataforma Cytomic, por lo que ya son conocidos por el usuario de la consola web y pueden utilizarse como referencia las guías de administración de cada producto administrado.

A continuación se enumeran los productos de seguridad compatibles con CYTOMIC Nexus, y se indica el enlace para obtener su guía asociada:

Producto / módulo	Guía del producto
Advanced EPDR	Guía de administración de Advanced EPDR. **https://info.cytomicmodel.com/resources/guides/EPDR/latest/es/EPDR-guia-ES.pdf**
Advanced EDR	Guía de administración de Advanced EDR. **https://info.cytomicmodel.com/resources/guides/EDR/latest/es/EDR-guia-ES.pdf**
Cytomic Encryption	Guía de administración del producto instalado.
Cytomic Data Watch	Guía de administración del producto instalado.
Cytomic Patch	Guía de administración del producto instalado.
Cytomic SIEMConnect for Partners	Guía de infraestructura. **https://info.cytomicmodel.com/resources/guides/SIEMConnect/es/SIEMCONNECT-Manual-ES.PDF** Manual de descripción de eventos.

Producto / módulo	Guía del producto
	https://info.cytomicmodel.com/resources/guides/SIEMConnect/es/SIEMCONNECT-ManualDescripcionEventos-ES.pdf

Tabla 7.1: Productos compatibles con CYTOMIC Nexus y guía de administración asociada

Requisitos para asignar configuraciones centralizadas

Para que el usuario de la consola web de CYTOMIC Nexus pueda asignar configuraciones a los productos de seguridad instalados en sus clientes, es necesario que se cumplan los siguientes requisitos:

- El usuario de la consola web de CYTOMIC Nexus ha creado previamente el cliente y le ha asignado un producto de seguridad. Consulta el apartado **Productos y módulos compatibles**.
- El usuario de la consola web de CYTOMIC Nexus ha establecido el modo de gestión centralizada al producto. Consulta **Asignar productos a clientes** en la página **55**
- El usuario de la consola web de CYTOMIC Nexus tiene visibilidad y permisos suficientes para asignar configuraciones a ese cliente o grupo de clientes. Consulta el capítulo **Acceso y autorización en CYTOMIC Nexus** en la página **29** para obtener más información sobre los permisos en CYTOMIC Nexus.
- La versión del producto de seguridad instalado el cliente es la 3.50 o posterior. Para encontrar esta información en la consola del cliente, selecciona la opción de novedades del producto en el menú de configuración general.
- El cliente tiene activada la opción **Permitir a mi distribuidor acceder a mi consola**. Esta opción está activada por defecto, pero si no es así, el cliente deberá seguir los pasos mostrados a continuación en la consola de administración de su producto:
    - En el menú superior **Configuración**, haz clic en el menú lateral **Usuarios** y en la pestaña **Usuarios**.
    - Haz clic en la opción **Permitir a mi distribuidor acceder a mi consola**.

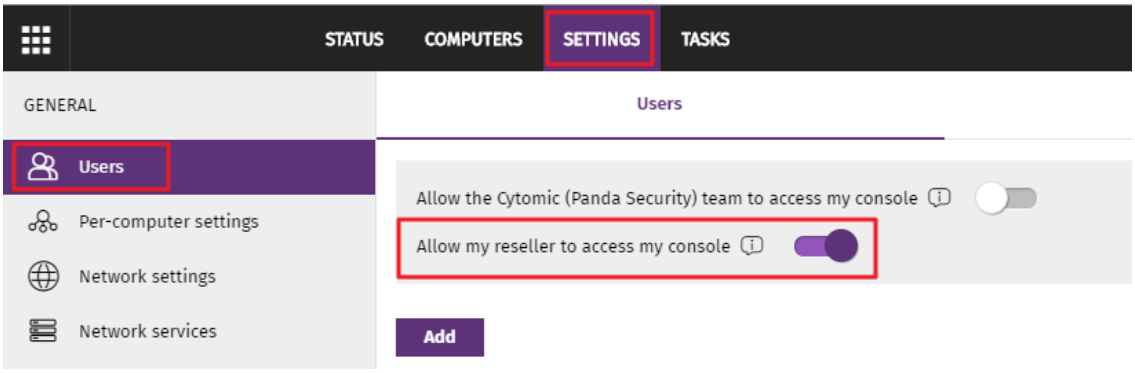

Figura 7.1: Acceso a la opción Permitir a mi distribuidor acceder a mi consola desde la consola Cytomic del cliente

Acceso a la gestión de configuraciones

- En el menú superior **Clientes** haz clic en el botón **Configuración de los productos de los clientes**. Se abrirá una nueva pestaña con el mismo aspecto de la consola de que utiliza el propio cliente para administrar sus productos.

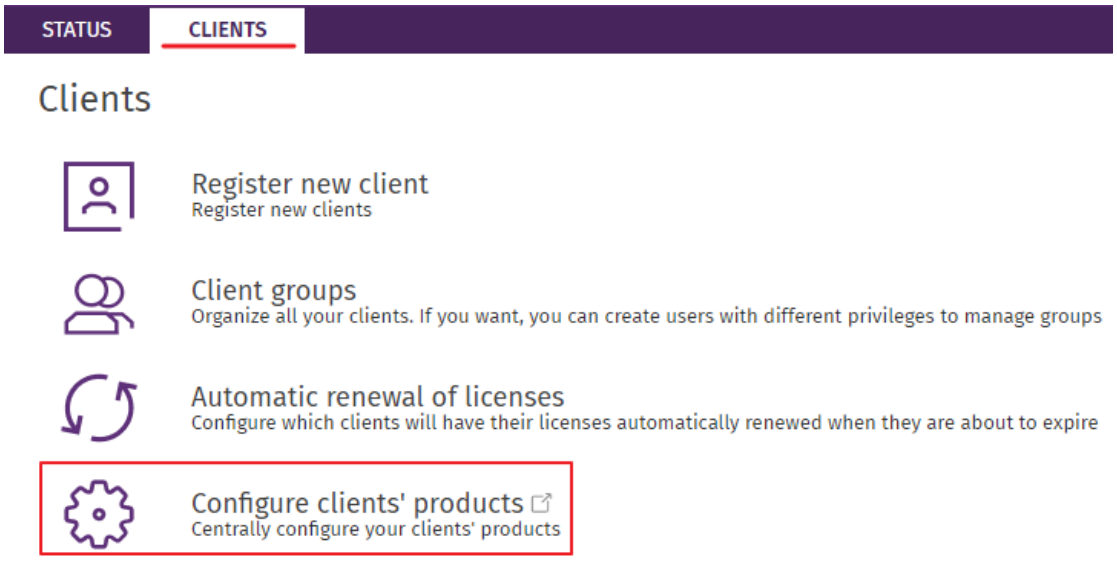

Figura 7.2: Acceso a la configuración de productos

- Selecciona el menú superior **Configuración**. Se mostrarán dos pestañas en el panel lateral: **Clientes** y **Administración**.
- Haz clic en la pestaña **Configuración** para modificar el funcionamiento de las características del producto de seguridad instalado en el cliente y sus módulos.
- Haz clic en la pestaña **Administración** para gestionar el aspecto de la consola del cliente y la información de telemetría que recibirá el proveedor de servicios de seguridad a través del producto Cytomic SIEMConnect for Partners.

Configuraciones para los productos de seguridad

Gestión de configuraciones

Para obtener información de cómo crear, borrar o modificar configuraciones consulta el capítulo "**Gestión de configuraciones**", apartado "**Crear y gestionar configuraciones**" de la guía de administración asociada al producto.

Clases de configuraciones soportadas en CYTOMIC Nexus

Dependiendo del producto instalado en el cliente, algunas o todas las configuraciones establecidas por el usuario de la consola web tendrán efecto en el software de seguridad instalado en los equipos del cliente. Para configurar un determinado perfil, consulta el capítulo indicado en la tabla **Configuraciones disponibles** correspondiente a la guía de administración del producto asociado.

CYTOMIC Nexus soporta las configuraciones de los productos de la familia Endpoint mostradas a continuación:

Configuración	Descripción
Ajustes por equipo	Configura el comportamiento del software de seguridad instalado en el equipo del usuario: • Visualización del icono en la bandeja del sistema. Consulta el capítulo "**Configuración remota del agente**", apartado "**Configuración de la visibilidad del agente**" de la guía de administración del producto. • Actualización del software de seguridad instalado. Consulta el capítulo "**Actualización del software cliente**", apartado "**Actualización del motor de protección**" de la guía de administración del producto. • Configuración de la seguridad ante manipulaciones no deseadas del software de seguridad (anti-tampering) y protección del equipo en modo arranque seguro. Consulta el capítulo "**Configuración remota del agente**", apartado "**Configuración de contraseña y anti-tampering**" de la guía de administración del producto. • Gestión de la copia de seguridad transparente de los ficheros almacenados en el equipo del usuario (Shadow Copies). Consulta el capítulo "**Configuración remota del agente**", apartado "**Configuración de Shadow Copies**" de la guía de administración del producto.

Configuración	Descripción
Control remoto	Permite al administrador establecer una conexión remota desde la consola del producto contratado por el cliente a los equipos de la red, con el fin de comprobar su estado o para iniciar tareas de resolución de problemas. Consulta el capítulo "**Herramientas de resolución**", apartado "**Control remoto de los equipos**" de la guía de administración del producto.
Estaciones y servidores	Determina el comportamiento del software de seguridad ante las amenazas y establece las reglas de acceso a los recursos de red permitidos por el administrador para minimizar la superficie de ataque de los equipos. Consulta el capítulo "**Configuración de estaciones y servidores**" de la guía de administración del producto.
Indicadores de ataque (IOA)	Detecta ataques informáticos dirigidos, con los que los hackers tratan de romper las defensas de seguridad mediante el despliegue de múltiples acciones coordinadas entre sí. Estas acciones se distribuyen a lo largo de períodos de tiempo extensos, y utilizan múltiples estrategias y vectores de infección simultáneos. Consulta el capítulo "**Configuración de indicadores de ataque**" de la guía de administración del producto.
Indicadores de ataque avanzados	Realiza un seguimiento detallado de las aplicaciones que se ejecutan en los equipos, para detectar comportamientos sospechosos. Los eventos generados por las aplicaciones instaladas en los equipos se analizan para determinar si constituyen un ataque. Esta configuración solo es aplicable a equipos con sistema operativo Windows. Consulta el capítulo "**Configuración de indicadores de ataque**" de la guía de administración del producto.
Bloqueo de programas	Contribuye a incrementar la seguridad en los equipos Windows de la red al permitir bloquear la ejecución de los programas que se consideren peligrosos o no compatibles con la actividad desarrollada en el cliente. Consulta el capítulo **"Configuración del bloqueo de programas"** de la guía de administración del producto.
Software	Evita inconvenientes y retrasos al usuario cuando la protección

Configuración	Descripción
autorizado	avanzada impide la ejecución de los programas desconocidos para la inteligencia de Cytomic hasta que se completa su clasificación. Consulta el capítulo "**Configuración de software autorizado**" de la guía de administración del producto.
Dispositivos móviles	Determina el comportamiento del software de seguridad ante las amenazas en smartphones y tablets compatibles con el sistema operativo Android e iOS. Consulta el capítulo **"Configuración de seguridad para dispositivos móviles"** de la guía de administración del producto
Gestión de parches	Mantiene actualizado el sistema operativo y las aplicaciones instaladas, automatizando la instalación de los parches de seguridad publicados por los proveedores del software. • Consulta **Parchear selectivamente equipos de clientes administrados por una única consola Cytomic** • Consulta el capítulo **Cytomic Patch (Actualización de programas vulnerables)** de la guía de administración del producto.
Data Control	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. Consulta el capítulo **Cytomic Data Watch (supervisión de información sensible)** de la guía de administración del producto.
Cifrado	Cifra el contenido de los medios de almacenamiento interno de los equipos para 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 sin borrar su contenido. Consulta el capítulo **Configuración de Full Encryption** de la guía de administración del producto.

Configuración	Descripción
Cytomic SIEMConnect for Partners	Establece una configuración unificada para recibir toda la telemetría generada en los equipos del proveedor de servicios de seguridad. Para obtener información sobre la configuración del módulo consulta el apartado **Configuración Cytomic SIEMConnect for Partners**.

Tabla 7.2: Configuraciones disponibles

Configuraciones editables por el cliente

Por defecto, los clientes no pueden modificar ni borrar las configuraciones enviadas por los partners. Sin embargo, CYTOMIC Nexus permite establecer configuraciones como editables, autorizando su modificación de forma limitada a los clientes que las reciben.

Las configuraciones modificables por el cliente son:

- **Estaciones y servidores**: permite al cliente añadir nuevas exclusiones a la lista definida por el partner, pero no permite modificarla ni eliminarla.
- **Software autorizado**: permite al cliente añadir nuevas reglas de software autorizado a la lista definida por el partner, pero no permite modificarla ni borrarla.

Marcar configuraciones como editables

Para acceder a las configuraciones editables gestionadas desde CYTOMIC Nexus:

- En el menú superior selecciona **Clientes** y haz clic en **Configuración de los productos de los clientes**. Se abrirá una nueva pestaña en el navegador.
- En el menú superior selecciona **Configuración** y haz clic en la pestaña **Clientes** del panel lateral.

Para marcar las configuraciones de **Estaciones y servidores** como editables:

- Haz clic en el panel lateral **Estaciones y servidores**. Se mostrarán las configuraciones creadas.
- Selecciona la configuración que se va a establecer como editable y accede a la sección **General**.
- Selecciona la opción de **Exclusiones editables por el cliente** y haz clic en el botón **Guardar**. La configuración se mostrará con la etiqueta **Exclusiones editables por el cliente**

Para marcar reglas de **Software autorizado** como editables:

- Haz clic en el panel lateral **Software autorizado**. Se mostrarán las configuraciones creadas.
- Selecciona la configuración que se va a establecer como editable.

- Selecciona la opción de **Configuración modificable por el cliente** y haz clic en **Guardar**. La configuración se mostrará con la etiqueta **Configuración modificable por el cliente**.

Cambio de una configuración de editable a no editable y viceversa

Si el partner cambia el estado de la configuración de editable a no editable, las exclusiones o reglas añadidas por el cliente se ocultarán y dejarán de aplicarse.

Si el partner cambia el estado de la configuración de no editable a editable, se restaurarán las exclusiones o reglas añadidas por el cliente y volverán a aplicarse.

Ninguno de estos cambios afecta a las reglas y exclusiones añadidas por el partner, que permanecerán siempre visibles, aunque atenuadas, y en funcionamiento mientras se conserve la configuración.

Parchear selectivamente equipos de clientes administrados por una única consola Cytomic

Como normal general, el proveedor de servicios asigna una consola Cytomic independiente a cada cliente para gestionar los productos de seguridad que ha contratado. Si por el contrario, un proveedor de servicios gestiona la seguridad de varios clientes desde una misma consola Cytomic, puede ocurrir que algunos de sus clientes tengan contratado Cytomic Patch y otros no. En este caso, para evitar que la tarea de instalación de parches que el proveedor de servicios envía desde la consola de CYTOMIC Nexus se ejecute en todos los equipos sin distinción, es necesario crear en la consola de Cytomic configuraciones de gestión de parches diferenciadas que determinen si los parches se instalarán en el equipo o no.

Para configurar Cytomic Patch y permitir o no la instalación de parches en los equipos de los clientes:

- En la consola de Cytomic crea una configuración para los equipos de los clientes que tienen licencia de Cytomic Patch.
- En la consola de Cytomic crea otra configuración para los equipos de los clientes que NO tienen licencia de Cytomic Patch.
- En la configuración de los equipos que sí tienen licencia de Cytomic Patch, selecciona **Instalar parches** en el desplegable **Instalación de parches**.
- En la configuración de los equipos que NO tienen licencia de Cytomic Patch selecciona **No instalar parches** en el desplegable **Instalación de parches**.
- En la consola de CYTOMIC Nexus crea una única tarea de instalación de parches que tenga como destinatario la consola que contiene equipos de varios clientes.

Para obtener más información acerca de cómo crear tareas de instalación de parches en CYTOMIC Nexus consulta **Configurar una tarea de Cytomic Patch (4)** en la página **136**.

Para obtener más información acerca de la configuración de Cytomic Patch en la consola de Cytomic consulta el capítulo **Cytomic Patch(Actualización de programas vulnerables)**, apartado

Configuración del descubrimiento de parches sin aplicar de la Guía de administración del producto de seguridad contratado.

Configuración Cytomic SIEMConnect for Partners

Para activar la configuración haz clic en el control deslizante **Enviar los siguientes eventos a mi SIEM** e indica los grupos de eventos que recibirás en el SIEM de entre toda la telemetría generada por los equipos asignados a la configuración.

Configuración de los grupos

El flujo de telemetría enviado a Cytomic está formado por los eventos relevantes que se registran al ejecutar programas en los equipos de los clientes. Estos eventos se agrupan según su tipo, y cada grupo puede habilitarse o deshabilitarse de forma individual para seleccionar unicamente aquellos eventos que el MSSP tenga interés en recibir.

Grupo	Descripción
Detecciones de amenazas (Malware, PUPS, Exploits)	Alertas de malware / PUP, Exploit y bloqueo por políticas avanzadas.
Carga y ejecución de ejecutables PE y scripts	Carga y ejecución de ficheros ejecutables binarios y no binarios (scripts).
Comunicaciones	Eventos de apertura y uso de sockets.
Acceso a datos	Acceso a datos contenidos en ficheros y en el registro de Windows.
Creación y modificación de ejecutables PE y scripts	Creación y modificación de ficheros ejecutables binarios y scripts.
Accesos al registro de Windows	Eventos relacionados con acceso al registro de Windows.
Eventos del sistema	Eventos relacionados con el acceso a dispositivos, motor WMI e inicios y finales de sesión.
Indicios de threat hunting (Sólo para clientes con Cytomic Orion)	Alertas generadas por las reglas de Threat Hunting en Orion.

Tabla 7.3: Agrupaciones de los eventos disponibles para el partner

Para obtener más información sobre el significado y la definición de los eventos enviados al SIEM del proveedor de servicios consulta el Manual de descripción de eventos en ***ttps://info.cytomicmodel.com/resources/guides/SIEMConnect/es/SIEMCONNECT-ManualDescripcionEventos-ES.pdf***

Configuración del formato de evento

- Haz clic en el enlace **Cambiar formato de envío** en la parte inferior de la pantalla. Se mostrará la ventana **Selecciona el formato en el que quieres que se envíen los eventos a tu SIEM**.
- Selecciona la opción Formato LEEF o Formato CEF y haz clic en el botón **Guardar**. La nueva configuración se aplicará de forma inmediata.

Dado que el MSSP va a recibir todos los eventos en un único servidor SIEM, todos los eventos se recibirán en el mismo formato. De esta forma, cuando el usuario de la consola CYTOMIC Nexus cambia el formato de evento en una configuración, el resto de configuraciones creadas compartirán esa elección.

Configuración por defecto

La configuración por defecto desactiva todos los grupos y el control deslizante **Enviar los siguientes eventos a mi SIEM**, por lo que inicialmente el partner no recibe ningún evento de sus clientes.

Asignar y enviar configuraciones

Asignar configuraciones

CYTOMIC Nexus permite asignar configuraciones a los clientes con productos que pertenecen a la familia Endpoint. Para ello, utiliza dos métodos: la asignación directa de configuraciones y la asignación indirecta. Las configuraciones se aplicarán automáticamente al grupo **Todos** de la consola del cliente.

Consulta los apartados ***Asignación / envío manual de configuraciones*** *y* ***Asignación / envío indirecto de configuraciones: herencia***

Enviar configuraciones

Con esta funcionalidad el usuario de la consola de CYTOMIC Nexus envía configuraciones a la consola del producto de sus clientes pero sin aplicarla al grupo Todos del cliente. Esta configuración podrá ser asignada posteriormente por el administrador de la consola del cliente y/o por el usuario de la consola web de CYTOMIC Nexus que accede a dicha consola, de forma directa y cuando lo necesite.

*Para más información, consulta el apartado **Tipos de asignación / envío de configuraciones**.*

Tipos de asignación / envío de configuraciones

Asignación / envío manual de configuraciones

La asignación directa de configuraciones a clientes puede realizarse desde el propio perfil de configuración o desde el listado de configuraciones.

Asignar / enviar desde el propio perfil de configuración:

- Seleccionael menú superior **Configuración**, pestaña **Clientes**. En el panel lateral, selecciona el tipo de configuración que quieres asignar.
- En el panel de la derecha se muestran el listado de grupos de clientes y las configuraciones ya existentes del tipo seleccionado.
- Haz clic en la configuración que deseas asignar o crea una nueva y haz clic en el campo de texto **Destinatarios**.
- **Para asignar una configuración**: en la sección **Asignar al grupo Todos de los siguientes clientes**, haz clic en el icono ⊕ y selecciona en el árbol de clientes el cliente o grupo de clientes al que quieres asignar la configuración.
- **Para enviar una configuración**: en la sección **Mostrar en la consola de los siguientes clientes**, haz clic en el icono ⊕ y selecciona en el árbol de clientes el cliente o grupo de clientes al que quieres enviar la configuración.
- Haz clic en el botón **Añadir**.

Los clientes o grupos de clientes se mostrarán en la caja de texto **Grupos de clientes** en la ventana **Destinatarios** y la nueva configuración se enviará de forma inmediata a la consola de los clientes.

En el caso de las configuraciones asignadas, si alguno de los nodos hijos del nodo elegido tiene otra configuración asignada por el usuario de la consola web, se mostrará una ventana de advertencia preguntando que configuración prevalecerá: la previamente asignada o la nueva.

Asignar desde el listado de configuraciones (Drag&Drop)

Selecciona la configuración y arrástrala hasta el cliente o grupo de clientes a asignar. La configuración se asignará automáticamente a la consola del cliente o grupo de clientes, y el grupo de clientes se añadirá en el campo **Grupos de clientes** de la ventana **Destinatarios** de la configuración.

Asignación / envío indirecto de configuraciones: herencia

CYTOMIC Nexus implementa los mismos mecanismos de herencia que se incluyen en los productos de la familia Endpoint instalados en sus clientes. De esta forma, el usuario de la consola web puede asignar o enviar de forma indirecta configuraciones a ramas completas del árbol de clientes, sin necesidad de configurar cada uno de sus nodos (clientes o grupos de clientes) de forma individual.

Para obtener más información sobre esta funcionalidad y los tipos de herencia soportados en CYTOMIC Nexus consulta el capítulo "**Gestión de configuraciones**", apartado "**Asignación indirecta de configuraciones: las dos reglas de la herencia**" de la guía de administración del producto.

Visualizar las configuraciones asignadas

Las configuraciones de los productos que pertenecen a la familia Endpoint son visibles al acceder al menú superior **Configuración**, pestaña **Clientes**. La ventana contiene los siguientes elementos:

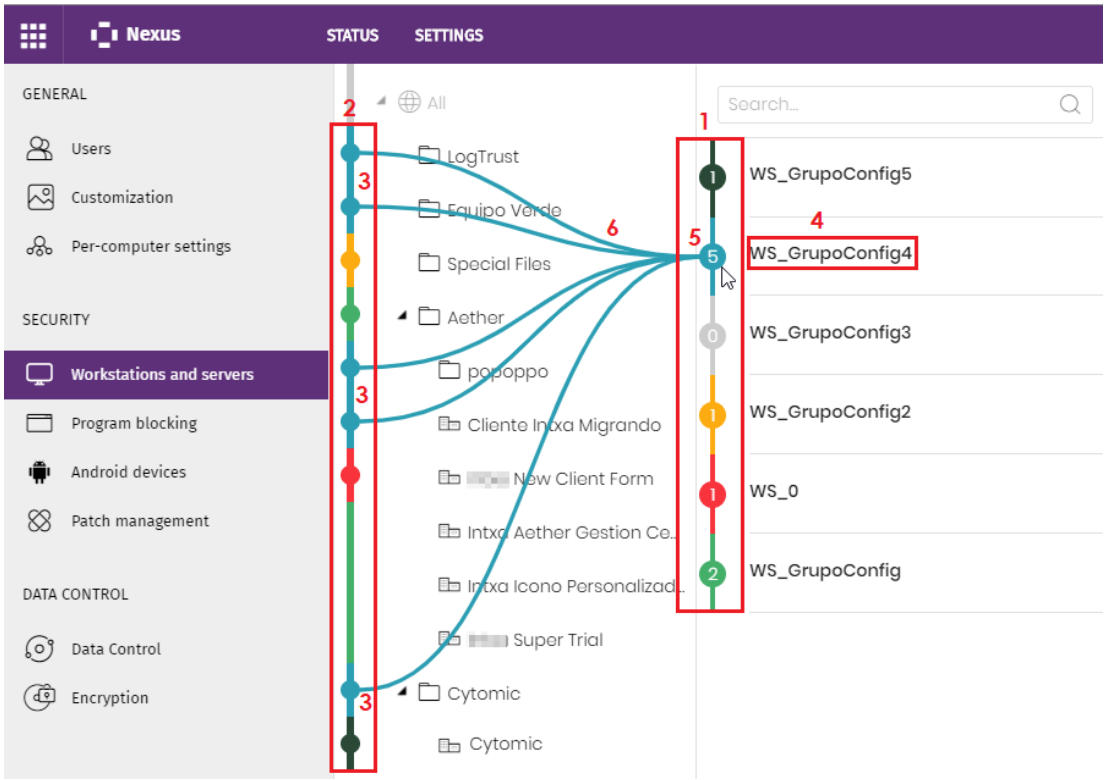

Figura 7.3: Visualizar las configuraciones asignadas

- **Panel lateral izquierdo**: muestra los tipos de configuración posibles.
- **Panel derecho**: indica qué configuraciones se corresponden con el tipo seleccionado y a qué grupos de clientes afectan. Este panel incluye:
    - **Barra vertical de configuraciones (1)**: utiliza un sistema de colores para representar las configuraciones existentes. En cada configuración se detalla el número de nodos del árbol de clientes a los que está asignada.
    - **Barra vertical del árbol de grupos de clientes (2)**: señala mediante el color la sección del árbol de clientes afectada por la configuración debido a la herencia.

Cuando se crea y asigna una configuración, CYTOMIC Nexus ejecuta los siguientes pasos:

- Muestra la configuración dentro del listado de configuraciones disponibles **(4).**
- Crea una sección en la barra vertical de configuraciones y le asigna un color **(5)**. La sección muestra en su interior la cantidad de nodos a los que se ha asignado la configuración. Si la configuración no tiene nodos asignados mostrará el número "0".
- Utiliza el mismo color de la configuración para señalar en la barra vertical del árbol de clientes la sección afectada por la configuración **(3)**. Si la sección de la barra vertical de configuraciones abarca varios nodos del árbol de clientes, todos los nodos estarán afectados por la configuración del color asociado.
- Muestra la relación entre una configuración y los nodos a los que afecta en el árbol de clientes mediante líneas **(6)** visibles al pasar el cursor sobre las secciones de ambas barras verticales. El color de las líneas es el asignado a la configuración.
- Si la barra del árbol de clientes muestra números asociados a alguna de sus secciones, quiere decir que estas secciones están contraídos y que hay nodos hijos ocultos que tienen excepciones de configuración.

Figura 7.4: Visualizar configuraciones de nodos con excepciones

La cifra indicada **(1)** se corresponde con el número de nodos hijos ocultos que tienen asignadas configuraciones específicas. Al situar el cursor sobre el número del cuadrado, se mostrarán las líneas del color correspondiente a las configuraciones específicas asignadas **(2)**.

Para desplegar la barra vertical de grupos de clientes y mostrar los nodos ocultos, haz doble clic en el cuadrado.

Impacto de la asignación / envío de configuraciones en el cliente

En la consola del cliente conviven configuraciones creadas por el propio cliente con las enviadas por el usuario de la consola de CYTOMIC Nexus. Por esta razón, CYTOMIC Nexus establece ciertas reglas para resolver las situaciones donde se detectan colisiones o sustituciones de configuraciones entre los dos orígenes posibles. La prioridad de una configuración viene establecida por su propietario, que queda determinado por la consola que creó o modificó esa configuración:

- Las configuraciones creadas por el cliente en su consola tienen como propietario el cliente.
- Las configuraciones creadas en CYTOMIC Nexus y enviadas de forma centralizada al cliente, tienen como propietario CYTOMIC Nexus.
- Las configuraciones creadas y enviadas por la consola web de CYTOMIC Nexus, y posteriormente modificados sus destinatarios en la consola del cliente, tienen propietario compartido.

Las reglas implementadas son:

- **Configuraciones de propietario CYTOMIC Nexus**: estas configuraciones se identifican visualmente en la consola del cliente con el color verde y con la etiqueta "Partner Center". Desde la consola web de CYTOMIC Nexus se pueden borrar y también modificar (sincronizar). El cliente no puede borrar estas configuraciones de forma directa, ni tampoco modificarlas, aunque sí puede añadir nuevos destinatarios o eliminar los que hubiera añadido previamente, pasando a ser una configuración de propietario compartido. Si la configuración está asignada al grupo **Todos** de la consola del cliente, el cliente no puede eliminar esta asignación de forma directa. Consulta el apartado **Causas e implicaciones para el cliente al cambiar el modo de gestión**.
- **Configuraciones de propietario el cliente**: la consola web de CYTOMIC Nexus no puede acceder ni ver estas configuraciones, de modo que tampoco puede borrarlas ni modificarlas.
- **Configuraciones de propietario compartido**: la consola web de CYTOMIC Nexus puede modificarlas (sincronizarlas) respetando los destinatarios que haya agregado el cliente, pero no puede borrarlas. El cliente no puede modificarlas ni borrarlas excepto añadir o retirar destinatarios, al igual que las configuraciones de propietario CYTOMIC Nexus. Al igual que las configuraciones de propietario CYTOMIC Nexus, éstas se identifican visualmente con el color verde en la consola del cliente y con la frase "Partner Center".

Crear configuraciones en la consola de los clientes

Cuando el usuario de la consola web de CYTOMIC Nexus asigna una configuración a uno o más clientes, se convierte en el propietario de esa configuración. La configuración se envía a la consola de cada cliente y se asocia al grupo **Todos** de su árbol de equipos para intentar garantizar que se aplica a todos los equipos de la red. No obstante, si el cliente ha establecido una configuración manual en alguno de los nodos de su árbol de equipos, ésta prevalecerá sobre la configuración heredada del grupo **Todos**, y, por lo tanto, ninguno de los descendientes de ese grupo la recibirá.

Cuando el usuario de la consola web de CYTOMIC Nexus envía o asigna una configuración, ésta se muestra en el listado de configuraciones disponibles en la consola de los clientes con las siguientes particularidades:

- Todas las configuraciones enviadas o asignadas por la consola web de CYTOMIC Nexus a los clientes son configuraciones de solo lectura para éstos, y se identifican mediante la etiqueta "Partner Center" en color verde en el listado de configuraciones del cliente. De esta manera se diferencian del resto de configuraciones creadas por el administrador de la red del cliente.
- El cliente solo puede añadir o suprimir destinatarios a una configuración de solo lectura, pasando a ser de propietario compartido. No obstante, el cliente sí puede copiar esta configuración y modificar la copia a su gusto, ya que será el propietario de la copia.
- Los cambios efectuados en la consola web de CYTOMIC Nexus sobre una configuración enviada o asignada previamente a los clientes se sincronizan de forma automática en la consola de los clientes. Esta sincronización es unidireccional, en sentido del CYTOMIC Nexus hacia el cliente. Estos cambios se reflejan en la consola del cliente de forma inmediata y se propagan a sus dispositivos en tiempo real o en un plazo máximo de 15 minutos, dependiendo de la configuración de la opción **Activar la comunicación en tiempo real**. Consulta el capítulo "**Configuración remota del agente**", apartado "**Configuración de la comunicación en tiempo real**" en la guía de administración del producto asociado.
- En el caso de configuraciones de propietario compartido, el cliente no podrá desasignar el grupo **Todos** de forma directa.

Borrar configuraciones de la consola del cliente

Las reglas que regulan el borrado centralizado de configuraciones desde la consola web de CYTOMIC Nexus son:

- El usuario de la consola web de CYTOMIC Nexus solo puede borrar de las consolas de sus clientes las configuraciones de su propiedad, es decir, las que él ha enviado previamente y que no han sido modificadas por el cliente (propietario compartido).
- Las configuraciones que tienen como propietario la consola web de CYTOMIC Nexus borradas se eliminan también de las consolas de los clientes, pero las configuraciones de propiedad compartida no se borrarán. Por ejemplo, si se elimina una configuración o se

mueve de grupo a un cliente en la consola web de CYTOMIC Nexus, la configuración ya no se mostrará en la consola del cliente. Sin embargo, si el cliente añadió algún destinatario adicional a la configuración, ésta no se eliminará de forma centralizada de la consola del cliente aunque ya no se esté utilizando.

- Las configuraciones propiedad del cliente sustituidas por las del usuario de la consola web de CYTOMIC Nexus no se borran y se conservan en la consola del cliente.
- Después de borrar una configuración desde la consola web de CYTOMIC Nexus, el cliente siempre termina el proceso con una configuración asignada al grupo **Todos** de su consola. Esta configuración puede estar asignada desde la consola web de CYTOMIC Nexus si hay otra configuración que se aplica mediante la herencia o, si no hay configuración en CYTOMIC Nexus disponible para ese cliente, se mantiene la configuración actual del cliente pasado éste a ser su propietario.

Cambiar al cliente de grupo

Al cambiar a un cliente de grupo en la consola web de CYTOMIC Nexus se ejecutan las acciones siguientes:

- Todas las configuraciones propiedad del usuario de la consola web asignadas a los clientes que se mueven del grupo original se eliminarán del listado de configuraciones disponibles del cliente.
- En el listado de configuraciones de los clientes que se mueven de grupo se mostrarán las configuraciones asignadas al grupo nuevo.

Causas e implicaciones para el cliente al cambiar el modo de gestión

Las causas por las cuales un cliente puede dejar de recibir configuraciones centralizadas de su partner son:

- Cuando el cliente deja de autorizar a CYTOMIC Nexus el acceso a su consola (Consulta **Requisitos para asignar configuraciones centralizadas**).
- Cuando se elimina el cliente desde la consola web de CYTOMIC Nexus al terminar su relación contractual.
- Cuando se cambia el modo de gestión en el producto desde la consola web de CYTOMIC Nexus. Consulta **Detalles del producto asignado** en la página **57**.

En estos casos, todas las configuraciones en propiedad de la consola web de CYTOMIC Nexus o copropietarias, excepto las asociadas al módulo Cytomic SIEMConnect for Partners, pasan a ser propiedad del cliente:

- Dejarán de mostrar la etiqueta “Partner Center" en el listado de configuraciones de la consola del cliente.

- Dejarán de ser de solo lectura para el cliente.
- Los cambios en las configuraciones de la consola web de CYTOMIC Nexus no se sincronizarán en la consola del cliente.

Modelo de gestión elegido y Cytomic SIEMConnect for Partners

Puesto que la configuración de Cytomic SIEMConnect for Partners no afecta a la configuración del producto de seguridad instalado en el cliente, el modelo de gestión elegido no tiene ningún efecto.

Consecuencias de la restauración de la relación CYTOMIC Nexus/cliente

Si tras una situación de ruptura se recupera la relación CYTOMIC Nexus/cliente, CYTOMIC Nexus asignará al cliente las configuraciones correspondientes al grupo del que va a formar parte.

Permisos y visibilidad del usuario de la consola web

Visibilidad del árbol de clientes

El árbol mostrará solo los clientes visibles para el usuario de la consola web, según el nivel de visibilidad sobre los clientes establecido en su permiso. En el caso de que el usuario de la consola web tenga visibilidad sobre un grupo de clientes pero no sobre un nodo intermedio, éste se mostrará sin clientes.

En el árbol de clientes de la consola web se mostrarán solo los clientes que han autorizado a CYTOMIC Nexus el acceso a su consola y han sido configurados como clientes con gestión centralizada en la consola de CYTOMIC Nexus.

Para autorizar al CYTOMIC Nexus el acceso a la consola, en la consola del producto de la familia Endpoint del cliente es necesario seleccionar el menú **Configuración**, hacer clic en **Usuarios** en el menú lateral y marcar la casilla **Permitir a mi distribuidor acceder a mi consola**.

Modificar configuraciones

El tipo de permiso asignado a la cuenta de usuario con la que se accede a la consola de CYTOMIC Nexus autoriza a quien accede a ver únicamente o a modificar configuraciones.

Para obtener más información sobre la cuenta de usuario y los diferentes permisos, consulta el capítulo ***Acceso y autorización en CYTOMIC Nexus*** *en la página* ***29****.*

Para modificar una configuración, se deben cumplir los requisitos siguientes:

- El usuario de la consola web debe disponer de permiso de control total, administrador de licencias y seguridad o administrador de seguridad. Las cuentas de usuario con permiso de monitorización no pueden modificar configuraciones.

- El usuario de la consola web que realiza la modificación debe tener visibilidad sobre todos los clientes a los que se ha asignado la configuración. Si existe algún cliente sobre el que el usuario no tenga visibilidad, no se podrá modificar la configuración. Como alternativa, el usuario podrá:
    - Asignar/retirar o enviar la configuración a los clientes sobre los que sí tiene visibilidad.
    - Crear una nueva configuración copiando la anterior, modificarla a su gusto y asignarla o enviarla a los clientes sobre los que sí tiene visibilidad.

*Consulta el apartado **Asignar configuraciones***

Borrar configuraciones

Solo se puede borrar una configuración cuando ésta no tiene ningún cliente asignado. Para dejar de asignar una configuración a los clientes, la cuenta de usuario ha de tener visibilidad sobre ellos.

Personalización de la consola del cliente (Co-Branding)

CYTOMIC Nexus permite cambiar el aspecto de la consola de los productos de seguridad asignados a los clientes para reforzar su presencia e imagen de marca:

- Cambio de la paleta de colores de la consola.
- Cambio del logotipo de la consola.
- Cambio del nombre de la protección instalada en los equipos por uno genérico.
- Cambio del icono de la protección instalada en los equipos por uno genérico.

Acceso a la configuración de la personalización

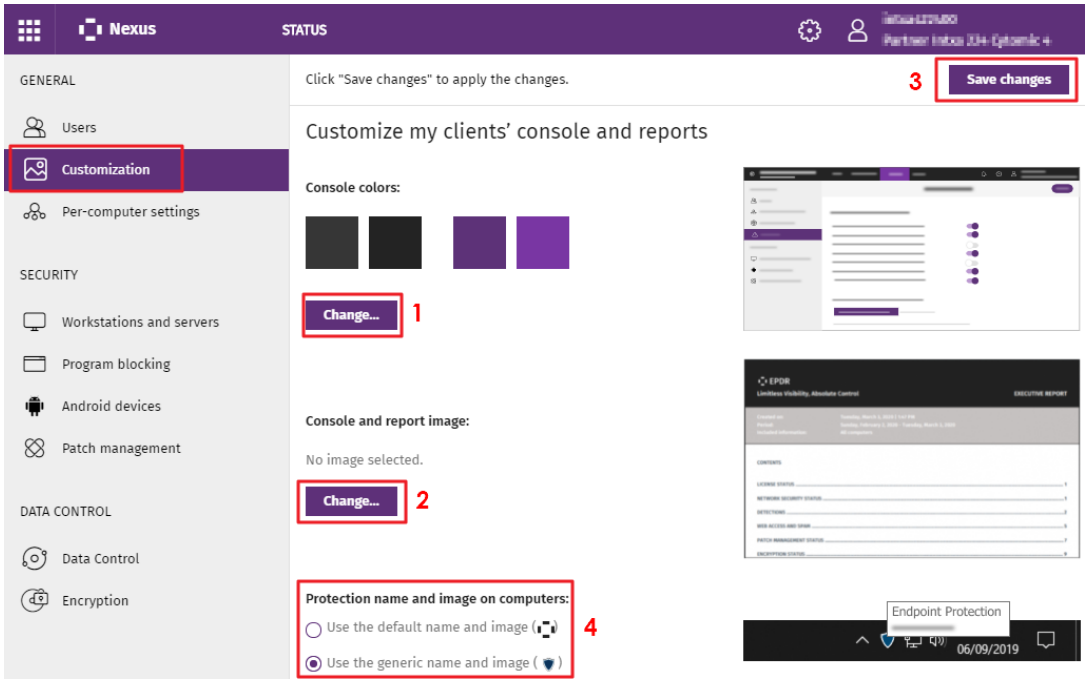

Figura 7.5: Acceso a la funcionalidad de personalización de productos que pertenecen a la familia Endpoint

Para cambiar el aspecto de la consola de los clientes que pertenecen a la familia Endpoint sigue los pasos mostrados a continuación:

- Selecciona el menú superior **Clientes** y haz clic en **Configuración de los productos de los clientes**. Se abrirá una nueva pestaña en el navegador.
- Haz clic en el menú superior **Configuración**, pestaña **Administración**, panel lateral **Personalización**. Se abrirá la ventana **Personalizar consola de mis clientes**.

Modificar el aspecto de la consola

- Haz clic en el botón **Cambiar (1)** para elegir una paleta de colores alternativa entre las 8 posibles.

Modificar la imagen que se mostrará en la consola y en los informes

- Haz clic en el botón **Cambiar (2)** para cargar un logotipo nuevo que sustituirá a la imagen del producto en la consola del cliente. Esta imagen tiene que tener un formato compatible: jpeg, o png a una resolución de 128x48 pixels y de un tamaño menor a los 10 Kbytes.
- Una vez terminada la configuración, haz clic en el botón **Guardar cambios (3)**. Los cambios se aplicaran en la consola del cliente de forma inmediata.

Modificar el icono y el nombre de la protección en los equipos

- Haz clic en **Utilizar la imagen y el nombre genérico (4)**.

Consecuencias de la modificación:

- El nombre del agente será Panda Endpoint Protection.
- El icono del agente será el genérico (escudo).

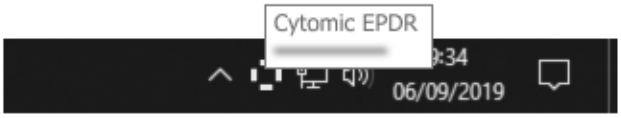

Figura 7.6: Imagen y nombre genérico de la protección

- Una vez terminada la configuración haz clic en el botón **Guardar cambios (3)**. Los cambios se aplicaran de forma inmediata y serán visibles en:
    - Todas las ventanas mostradas por el agente en los equipos del cliente, tanto durante el proceso de instalación como en el funcionamiento posterior.
    - La barra de inicio rápido de los equipos del cliente.
    - La consola local.

> *Los productos instalados en los equipos del cliente, se mostrarán sin el indicativo "Cytomic". Por ejemplo, Panda Endpoint Protection se mostrará como "Endpoint Protection".*

Estado de la seguridad de los clientes

CYTOMIC Nexus ofrece dos grandes grupos de herramientas que permiten al partner monitorizar el estado de la seguridad en los equipos de sus clientes:

- El panel de seguridad, con información sobre el estado global de la protección instalada en el parque informático de los clientes.
- Listados con información sobre el estado de la protección instalada en los equipos de los clientes y las amenazas detectadas en ellos; información global sobre los usuarios que acceden a las consolas de los clientes, datos sobre indicadores de ataque encontrados y distribución de los riesgos detectados.

Las herramientas de visualización y monitorización determinan en tiempo real el estado de la seguridad del parque informático de los clientes y el impacto de las brechas de seguridad que se puedan producir, lo que facilita la adopción de las medidas de seguridad apropiadas.

Widgets del panel de seguridad

El panel de seguridad muestra mediante widgets el estado de la seguridad del parque informático de los clientes. Además, la herramienta de filtrado disponible facilita la búsqueda rápida y directa de los equipos que reúnen determinadas características.

Acceso al panel de seguridad

Para acceder al panel de seguridad, selecciona el menú superior **Estado** y **Seguridad**  . Se mostrarán los contadores relativos a la seguridad de los equipos administrados por los clientes sobre los que tiene visibilidad la cuenta de usuario utilizada para acceder a la consola partner.

> *Para obtener más información sobre la cuenta de usuario y los diferentes permisos consulta el capítulo* ***Acceso y autorización en CYTOMIC Nexus*** *en la página* ***29****.*

Filtros disponibles desde el panel de seguridad

La herramienta de filtrado incorporada al panel de seguridad, facilita la búsqueda rápida y directa de equipos de clientes que reúnen determinadas características.

Los filtros establecidos en el panel de seguridad seleccionan los datos que se muestran en los widgets. Al hacer clic en una serie de un widget, la configuración del filtro elegido en el panel de seguridad se aplicará también a los datos mostrados en el listado **Estado de protección de los clientes**, junto al filtro de la serie seleccionada.

> *El funcionamiento de los filtros del panel de seguridad es el mismo que en el listado de estado de protección de los clientes. Para más información, consulta* ***Listados disponibles***

Desde el listado **Estado de la protección de los clientes** el partner puede acceder al dashboard de seguridad de la consola del producto de cada cliente, y a sus correspondientes listados sobre el estado de la protección de los equipos con todos los filtros seleccionados aplicados.

Para acceder a la herramienta de filtrado del panel de seguridad, haz clic en el desplegable **Filtros**, situado en la esquina superior izquierda del panel.

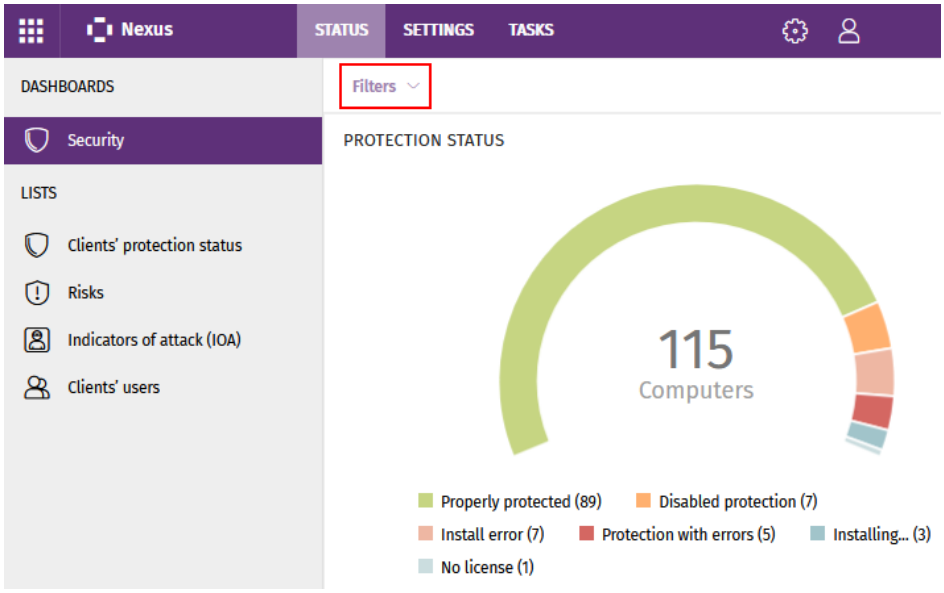

Figura 7.7: Selección de filtros del módulo de seguridad

A continuación se detallan los widgets, áreas y zonas activas incorporadas, así como los filtros disponibles.

Estado de protección

El widget representa en porcentaje y de forma gráfica los equipos de los clientes que comparten un mismo estado. Se muestra el número de equipos de los clientes en los que la protección funciona correctamente y aquellos con errores y problemas en la instalación o en la ejecución de la 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.*

En la parte inferior del widget se indica, si los hubiera:

- El número de equipos de los clientes que están en modo **Contención de ataque RDP**. Haz clic en el mensaje para acceder al listado de **Estado de la protección de los clientes**, filtrado por los equipos que están en modo **Contención de ataque RDP**.
- El número de equipos de los clientes que están aislados. Haz clic en el mensaje para acceder al listado de **Estado de la protección de los clientes**, filtrado por los equipos aislados.
- El número de equipos no administrados descubiertos. Haz clic en el mensaje para acceder al listado de **Estado de la protección de los clientes,** donde se muestra el número de

equipos no administrados descubiertos en el parque informático de los clientes, ordenados de mayor a menor.

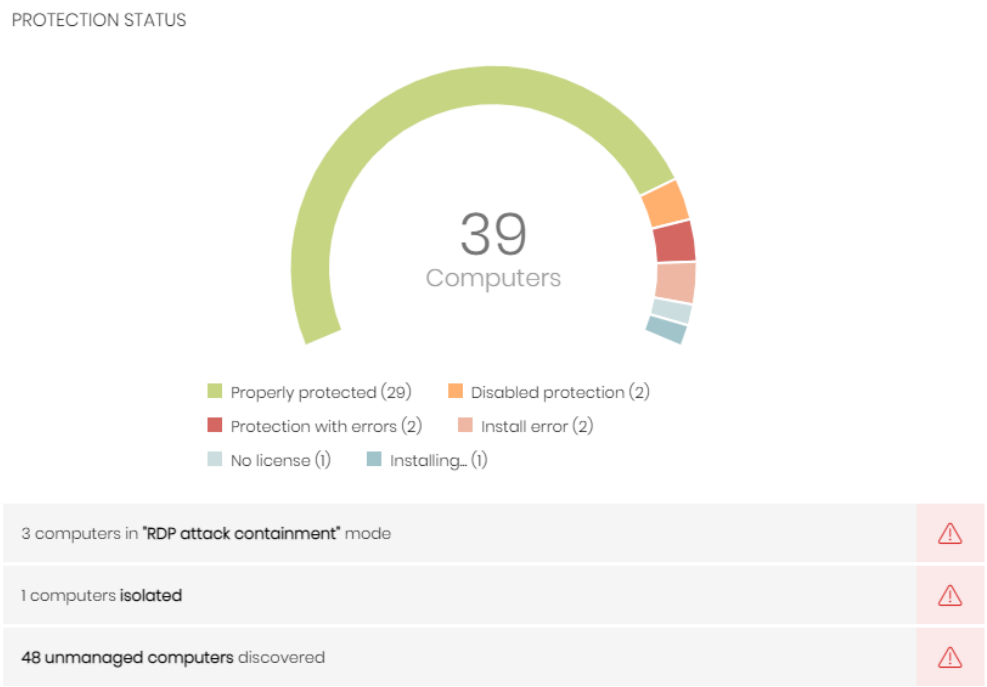

Figura 7.8: Panel Estado de protección

Descripción de las series

Serie	Descripción
Correctamente protegido	Número de equipos de los clientes en los que la protección se instaló sin errores y su ejecución no presenta problemas.
Protección desactivada	Número de equipos de los clientes que tienen la protección antivirus o la protección avanzada desactivada (la protección avanzada está disponible en función del producto contratado por el cliente y del sistema operativo instalado en el dispositivo).
Protección con error	Número de equipos de los clientes con la protección instalada pero que no responden a las peticiones desde los servidores de Cytomic.
Error instalando	Número de equipos de los clientes en los que la instalación de la protección no se pudo completar.

Serie	Descripción
Sin licencia	Número de equipos de los clientes sin protección, debido a que el número de licencias es insuficiente o a que no se les asignó ninguna licencia de las disponibles.
Instalando	Número de equipos de los clientes en los que la protección se encuentra en proceso de instalación.

Tabla 7.4: Descripción de las series de Estado de protección

Filtros establecidos desde el panel

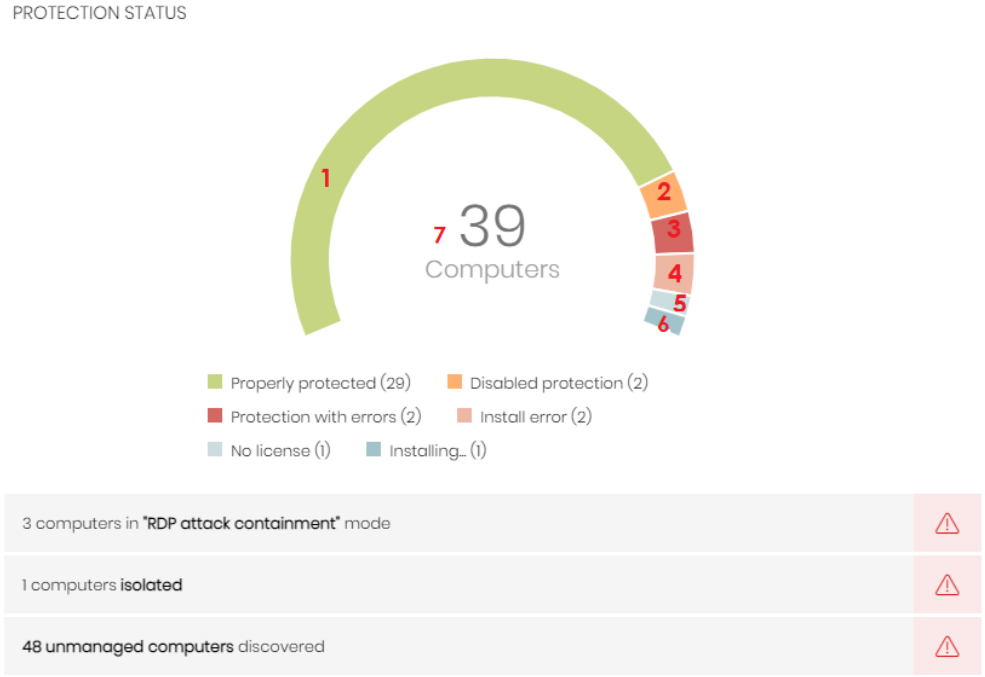

Figura 7.9: Zonas activas del panel Estado de protección

Al hacer clic en alguna de las zonas del widget, accederás al listado **Estado de la protección de los clientes**, con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de protección = Correctamente protegido.
(2)	Estado de protección = Protección desactivada.

Zona activa	Filtro
(3)	Estado de protección = Protección con error.
(4)	Estado de protección = Error instalando.
(5)	Estado de protección = Sin licencia.
(6)	Estado de protección = Instalando
(7)	Sin filtro.

Tabla 7.5: Definición de filtros del listado Estado de protección de los clientes

Equipos sin conexión

Muestra los equipos de los clientes 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.

En la parte inferior del widget se indica, si lo hubiera, el número de equipos que han tenido algún tipo de problema de conexión con los servidores de conocimiento de Cytomic.

Figura 7.10: Panel Equipos sin conexión

Descripción de las series

Zona activa	Filtro
> 3 días	Número de equipos que no enviaron su estado en los últimos 3 días.
> 7 días	Número de equipos que no enviaron su estado en los últimos 7 días.

Zona activa	Filtro
> 30 días	Número de equipos que no enviaron su estado en los últimos 30 días.

Tabla 7.6: Definición de los filtros del listado Equipos sin conexión

Filtros establecidos desde el panel

Figura 7.11: Zonas activas del panel Equipos sin conexión

Al hacer clic en alguna de las zonas del widget, accederás al listado **Estado de la protección de los clientes**, con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 3 días.
(2)	Última conexión = Hace más de 7 días.
(3)	Última conexión = Hace más de 30 días.

Tabla 7.7: Definición de los filtros del listado Equipos sin conexión

Protección desactualizada

El panel muestra:

- El número de equipos de los clientes cuya última versión del fichero de firmas instalada difiere en más de 3 días del fichero publicado por Cytomic
- El número de equipos de los clientes cuya versión del motor de protección difiere en más de 7 días del publicado por Cytomic.

En ambos casos, estos equipos pueden ser vulnerables frente a los ataques de amenazas.

- El número de equipos de los clientes que están pendientes de reinicio para completar la actualización de la protección.

Figura 7.12: Panel Protección desactualizada

Descripción de las series

El panel muestra el porcentaje y el número de equipos vulnerables por estar desactualizados, divididos en tres conceptos: protección, conocimiento y pendientes de reinicio. El porcentaje es visible al situar el cursor sobre las barras de la gráfica.

Serie	Descripción
Protección	Desde hace 7 días el equipo tiene un motor de protección instalado que es 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 7.8: Descripción de la serie Protección desactualizada

Filtros establecidos desde el panel

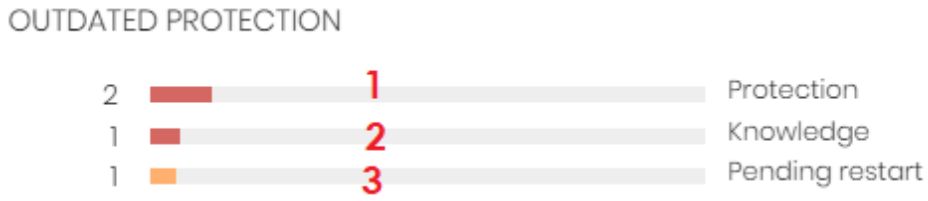

Figura 7.13: Zonas activas del panel Protección desactualizada

Al hacer clic en alguna de las zonas del widget, accederás al listado **Estado de la protección de los clientes**, con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Protección actualizada = No.

Zona activa	Filtro
(2)	Conocimiento = No.
(3)	Protección actualizada = Pendiente de reinicio.

Tabla 7.9: Definición de los filtros del listado Equipos con protección desactualizada

Listados del panel de seguridad

Los listados de seguridad contienen los datos utilizados para generar los widgets, y muestran con un algo grado de detalle la información de la actividad relativa a la protección de los equipos de la red.

Acceso al panel de seguridad de los clientes

- Selecciona el menú superior **Estado** y **Seguridad**  .
- Selecciona el menú superior **Clientes** y haz clic en **Configuración de los productos de los clientes**. Se abrirá una pestaña nueva en el navegador.
- En la pestaña nueva, selecciona el menú superior **Estado**. Se mostrarán los listados disponibles:
    - **Estado de la protección de los clientes**: indica las amenazas detectadas en cada cliente del partner realizadas por los distintos módulos de protección, y si éstos están actualizados o no.
    - **Riesgos**: muestra la distribución de los riesgos detectados en los equipos de cada cliente del partner. Consulta el capítulo "Evaluación de riesgos" de la guía de administración del producto.
    - **Indicadores de ataque (IOA) detectados**: resume los indicadores de ataque encontrados en la red de cada cliente del partner. Un IOA es una secuencia de acciones poco frecuentes encontradas en los eventos generados por los equipos del cliente con alta probabilidad de pertenecer a un ataque informático. Por lo general, se trata de ataques en fase temprana o en fase de explotación. En su mayoría, estos ataques no utilizan malware, ya que los atacantes suelen utilizar las propias herramientas del sistema operativo para ejecutarlos y así ocultar su actividad.
    - **Resultado de la instalación de parches**: muestra el resultado de la instalación de actualizaciones de programas y sistemas operativos en los equipos gestionados por el partner.

- **Usuarios de los clientes**: ofrece información global sobre los usuarios que acceden a la consola de administración de los clientes gestionados por el partner. Se especifica qué usuario ha accedido a la consola y en qué momento, si se ha modificado la contraseña de acceso y si ha sido necesario utilizar el doble factor de verificación (2FA).

Monitorización y acceso según el permiso asociado a la cuenta de usuario

Para obtener más información sobre la cuenta de usuario y los diferentes permisos consulta el capítulo ***Acceso y autorización en CYTOMIC Nexus*** *en la página* ***29****.*

En la ventana **Estado** solo se mostrarán los clientes sobre los que tenga visibilidad la cuenta de usuario utilizada. La visibilidad se define a nivel de permiso al crear la cuenta de usuario. Consulta **Acceso y autorización en CYTOMIC Nexus** en la página **29**.

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.

- **Nombre del listado (1)**: identifica el tipo de datos que se muestran en el listado.
- **Exportar (2)**: genera un fichero Excel con el contenido del listado.
- **Botón de herramientas de filtrado y búsqueda (3)**: al hacer clic se despliega un panel con las herramientas de filtrado. Una vez configuradas haz clic en el botón **Filtrar (6)**.
- **Bloque de controles de filtrado y búsqueda (4)**: filtra los datos mostrados en el listado.
- **Criterio de ordenación (5)**: 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.

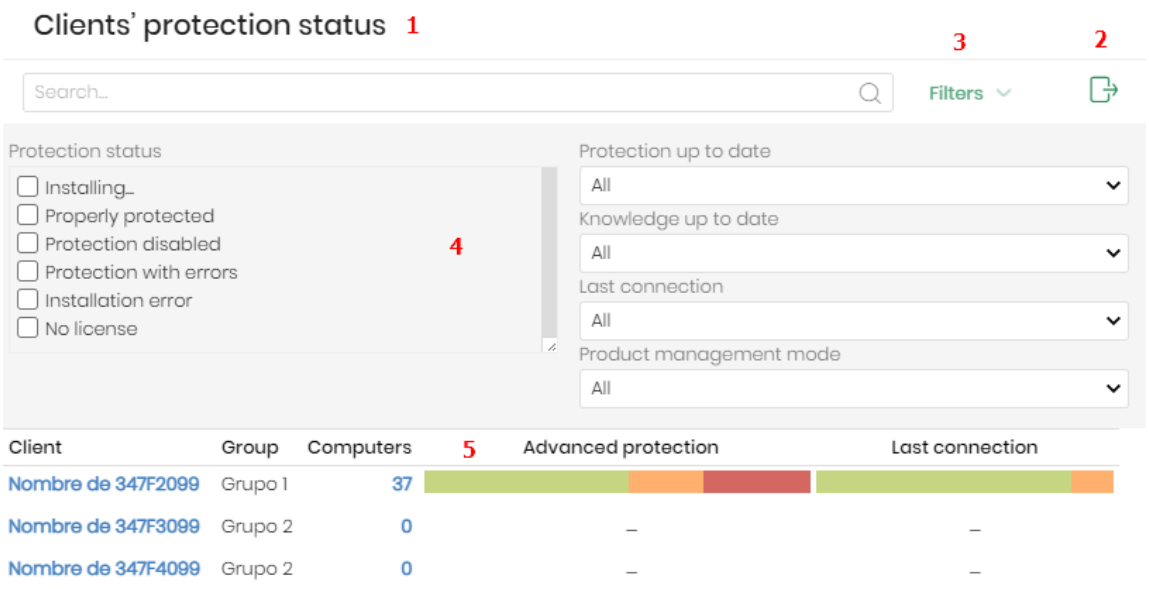

Figura 7.14: Partes de un listado

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

Icono	Descripción
25 rows	Selector del número de filas mostradas por página.
1 to 25 of 67	Intervalo de registros mostrados del total disponible.
«	Retroceso a la primera página.
‹	Retroceso a la página anterior a la actual.
1 2 3	Acceso directo por número de páginas.
›	Avance a la siguiente página.
»	Avance a la última página.

Tabla 7.10: Herramientas de paginación

Listados disponibles

Estado de protección de los clientes

Muestra el estado de la protección de los clientes e incorpora filtros que permiten localizar aquellos clientes con equipos que no estén protegidos.

Este listado permite acceder de forma rápida a diferentes secciones dentro de la consola de administración del cliente.

Al situar el cursor sobre cualquiera de las barras de colores, se muestra una etiqueta con la información de detalle:

- Número de equipos que pertenecen a cada serie.
- Porcentaje sobre el total de equipos en la red del cliente.
- Enlace **Ir a la consola del cliente**.

Campo	Descripción	Valores
Cliente	Nombre o identificador del cliente. Al hacer clic en el nombre del cliente se abre su consola, mostrando la ventana **Estado** y su dashboard de seguridad.	Cadena de caracteres
Grupo	Nombre del grupo al que pertenece el cliente.	Cadena de caracteres
Equipos no administrados descubiertos	Numero total de equipos no administrados descubiertos en el parque informático del cliente. Al hacer clic en el número de equipos, se abre la consola del cliente con el listado **Equipos no administrados descubiertos** con los filtros seleccionados aplicados (enlace disponible para usuarios de la consola de CYTOMIC Nexus con permiso superior al de solo lectura).	Numérico
Equipos administrados	Número total de equipos del cliente con productos que pertenecen a la familia Endpoint instalados. Al hacer clic en el número de equipos se abre la consola del cliente con el listado **Estado de protección de los equipos** con los filtros	Numérico

Campo	Descripción	Valores
	seleccionados aplicados (enlace disponible para usuarios de la consola de CYTOMIC Nexus con permiso superior al de solo lectura).	
Protección avanzada	Barra con sectores de colores que indica el estado de la protección avanzada en los equipos administrados del cliente.	• **Rojo**: equipos con error en la protección, protección desactivada, error de instalación y sin licencias. • **Verde**: equipos con la protección correcta o instalando. • **Guión** [-]: el cliente no tiene contratada la funcionalidad.
Antivirus	Barra con sectores de colores que indica el estado de la protección antivirus en los equipos administrados del cliente.	• **Rojo**: equipos con error en la protección, protección desactivada, error de instalación y sin licencias. • **Verde**: equipos con la protección correcta o instalando. • **Guión** [-]: el cliente no tiene contratada la funcionalidad.
Protección actualizada	Barra con sectores de colores que indica el estado de actualización de la protección	• **Rojo**: equipos con la protección sin

Campo	Descripción	Valores
	instalada en los equipos administrados del cliente.	actualizar. • **Naranja**: equipos pendientes de reinicio para completar la actualización. • **Verde**: equipos con la protección actualizada.
Conocimiento	Barra con sectores de colores que indica si el fichero de firmas descargado en los equipos administrados del cliente coincide con la última versión publicada o no.	• **Rojo**: conocimiento sin actualizar. • **Verde**: conocimiento actualizado.
Última conexión	Barra con sectores de colores que indica la fecha del último envío sobre el estado de los equipos administrados del cliente a la nube de Cytomic.	• **Verde**: menos de 3 días. • **Naranja**: más de 3 días. • **Naranja**: más de 7 días. • **Rojo**: Más de 30 días.

Tabla 7.11: Campos del listado de protección de los clientes para productos que pertenecen a la familia Endpoint

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Cliente	Nombre de la cuenta del cliente al que pertenece el servicio.	Cadena de caracteres
Identificador	Identificador asignado por Cytomic al cliente al darle de alta. Es necesaria su utilización en la	Cadena de caracteres

Campo	Descripción	Valores
	tramitación de incidencias y para el contacto del cliente con soporte técnico.	
Grupo	Nombre del grupo al que pertenece el cliente.	Cadena de caracteres
Gestión centralizada	Indica si el producto es gestionado de forma centralizada o no. Para más información, consulta el capítulo **Gestión de la configuración de la familia de productos Endpoint**	• **Sí**: gestión centralizada • **No**: sin gestión centralizada
Licencias consumidas	Número total de licencias consumidas por el cliente.	Numérico
Equipos no administrados descubiertos	Numero total de equipos no administrados descubiertos en el parque informático del cliente.	Numérico
Equipos administrados	Número total de equipos del cliente con productos que pertenecen a la familia Endpoint instalados.	
Protección avanzada - Instalando	Número de equipos del cliente que se encuentran en el estado.	Numérico
Protección avanzada - Correctamente protegido	Número de equipos del cliente que se encuentran en el estado.	Numérico
Protección avanzada - Protección desactivada	Número de equipos del cliente que se encuentran en el estado.	Numérico
Protección avanzada -	Número de equipos del cliente que se encuentran en el estado.	Numérico

Campo	Descripción	Valores
Protección con error		
Protección avanzada - Error instalando	Número de equipos del cliente que se encuentran en el estado.	Numérico
Protección avanzada - Sin licencia	Número de equipos del cliente que se encuentran en el estado.	Numérico
Antivirus - Instalando	Número de equipos del cliente que se encuentran en el estado.	Numérico
Antivirus - Correctamente protegido	Número de equipos del cliente que se encuentran en el estado.	Numérico
Antivirus - Protección desactivada	Número de equipos del cliente que se encuentran en el estado.	Numérico
Antivirus - Protección con error	Número de equipos del cliente que se encuentran en el estado.	Numérico
Antivirus - Error instalando	Número de equipos del cliente que se encuentran en el estado.	Numérico
Antivirus - Sin licencia	Número de equipos del cliente que se encuentran en el estado.	Numérico
Protección actualizada	Número de equipos del cliente que se encuentran en el estado.	Numérico
Protección desactualizada	Número de equipos del cliente que se encuentran en el estado.	Numérico
Protección	Número de equipos del cliente que se	Numérico

Campo	Descripción	Valores
pendiente de reinicio	encuentran en el estado.	
Conocimiento actualizado	Número de equipos del cliente que se encuentran en el estado.	Numérico
Conocimiento desactualizado	Número de equipos del cliente que se encuentran en el estado.	Numérico
Última conexión - Hace menos de 3 días	Número de equipos que se conectaron por última vez a la nube de Cytomic en el intervalo de tiempo indicado.	Numérico
Última conexión - Entre 3 y 30 días	Número de equipos que se conectaron por última vez a la nube de Cytomic en el intervalo de tiempo indicado.	Numérico
Última conexión - Más de 30 días	Número de equipos que se conectaron por última vez a la nube de Cytomic en el intervalo de tiempo indicado.	Numérico

Tabla 7.12: Campos del fichero exportado del listado de protección de los clientes con productos que pertenecen a la familia Endpoint

Herramienta de filtrado

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS • iOS

Campo	Descripción	Valores
Modo de gestión de los productos	Indica si el producto es gestionado de forma centralizada o no.	• Todos • Sin gestión centralizada • Gestionados de forma centralizada
Protección actualizada	El módulo de la protección instalado en el equipo es la última versión publicada.	• Todos • Actualizados • Pendientes de reinicio • Desactualizados
Conocimiento actualizado	El fichero de firmas descargado en el equipo es la última versión publicada.	• Todos • Actualizado • Desactualizados
Última conexión	Fecha del último envío del estado del cliente 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
Conexión con servidores de conocimiento	Indica el resultado de la última conexión del equipo con los servidores de conocimiento de Cytomic.	• Todos • Correcta • Con problemas

Campo	Descripción	Valores
Estado de protección	Estado de la protección seleccionado.	• Instalando • Correctamente protegido • Protección desactivada • Protección con error • Error instalando • Sin licencia
Estado de aislamiento	Estado del proceso de aislamiento en el que se encuentra el equipo.	• No aislado • Aislado • Aislando • Dejando de aislar
Modo Contención de ataque RDP	Indica si el equipo se encuentra en modo Contención de ataque RDP.	• Todos • No • Sí

Tabla 7.13: Campos de filtrado para el listado de Estado de la protección de clientes con productos Cytomic

Listado de Riesgos por cliente

Este listado muestra el nivel de los riesgos detectados en los equipos de cada cliente del partner.

> *Para más información, consulta el capítulo "Evaluación de riesgos"de la guía de administración del producto.*

Al situar el cursor sobre las barras de colores de la gráfica de distribución de riesgos, se muestra una etiqueta con la información de detalle:

- Número de equipos que pertenecen a cada nivel de riesgo.
- Porcentaje sobre el total de equipos del cliente.
- Enlace **Ir a la consola del cliente**.

Campo	Descripción	Valores
Cliente	Nombre o identificador del cliente. Al hacer clic en el cliente se abre su consola, mostrando la ventana **Estado** del módulo de evaluación de riesgos.	Cadena de caracteres
Grupo	Nombre del grupo al que pertenece el cliente.	Cadena de caracteres
Equipos	Número total de equipos del cliente en los que se han detectado riesgos. Al hacer clic se abre la consola del cliente, mostrando el listado **Riesgos por equipo**.	Numérico
Riesgo por equipo	Gráfica de distribución de los riesgos detectados en los equipos del cliente durante la evaluación de riesgos. Al situar el cursor sobre las barras de colores, se muestra una etiqueta con información detallada. Al hacer clic en el porcentaje que se muestra en la etiqueta, se accede al listado **Riesgos por equipo** de la consola del cliente, filtrado por el riesgo correspondiente.	• **Rojo**: número de equipos que se encuentran en nivel de riesgo Crítico. • **Naranja**: número de equipos que se encuentran en nivel de riesgo Alto. • **Amarillo** : número de equipos que se encuentran en nivel de riesgo Medio. • **Verde**: numero de equipos con riesgos sin impacto en la seguridad.

Tabla 7.14: Campos del listado Riesgos por cliente

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Cliente	Nombre de la cuenta del cliente al que pertenece el servicio.	Cadena de caracteres
Identificador	Identificador asignado por Cytomic al cliente al darle de alta. Es necesaria su utilización en la tramitación de incidencias y para el contacto del cliente con soporte técnico.	Cadena de caracteres
Grupo	Nombre del grupo al que pertenece el cliente.	Cadena de caracteres
Equipos con riesgos críticos	Número de equipos que se encuentran en nivel de riesgo crítico.	Numérico
Equipos con riesgos altos	Número de equipos que se encuentran en nivel de riesgo alto.	Numérico
Equipos con riesgos medios	Número de equipos que se encuentran en nivel de riesgo medio.	Numérico
Equipos sin riesgo	Número de equipos con riesgos sin impacto en la seguridad.	Numérico

Tabla 7.15: Campos del fichero exportado del listado Riesgos por cliente

Herramienta de filtrado

Campo	Descripción	Valores
Buscar cliente	Filtra los clientes según su nombre o grupo.	Cadena de caracteres
Tipo de equipo	Filtra los equipos según su clase.	• Estación • Portátil • Servidor • Dispositivo móvil
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows

Campo	Descripción	Valores
		• Linux • macOS • Android • iOS
Nivel de riesgo	Nivel de riesgo asignado.	• Critico • Alto • Medio • Sin riesgo

Tabla 7.16: Campos de filtrado para el listado Riesgos por cliente

Indicadores de ataque (IOA) detectados

Muestra el número total de indicadores de ataque detectados hasta el presente en los equipos de los clientes, tanto sin han sido revisados como si no, y el número de indicadores que no han sido revisados por el administrador o por el partner.

Este listado permite acceder de forma rápida a diferentes secciones dentro de la consola de administración del cliente.

Campo	Descripción	Valores
Cliente	Nombre o identificador del cliente. Al hacer clic se abre la consola del cliente con la ventana **Estado**, mostrando su dashboard de seguridad.	Cadena de caracteres
Grupo	Nombre del grupo al que pertenece el cliente.	Cadena de caracteres
Equipos	Número total de equipos del cliente con productos Cytomic instalados. Al hacer clic se abre la consola del cliente con la ventana **Equipos**, mostrando un listado de sus equipos de la familia Endpoint.	Numérico
Indicadores de	Número total de indicadores de ataque detectados en los equipos del cliente.	Numérico

Campo	Descripción	Valores
ataque (IOA) detectados	Al hacer clic se abre la consola del cliente con el listado Indicadores de ataque (IOA) y con el filtro **Estado** establecido a **Todos**, mostrando el histórico de IOAs detectados en el cliente.	
Indicadores de ataque (IOA) pendientes	Número de indicadores de ataque detectados en los equipos del cliente que todavía no fueron revisados. Al hacer clic se abre la consola del cliente con el listado Indicadores de ataque (IOA) y con el filtro **Estado** establecido a **Pendiente**, mostrando los IOAs que el administrador o el partner del cliente todavía no ha revisado o resuelto.	Numérico
Última detección	Fecha de aparición del último indicador de ataque.	Fecha

Tabla 7.17: Campos del listado Indicadores de ataque

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Cliente	Nombre o identificador del cliente.	Cadena de caracteres
Grupo	Nombre del grupo al que pertenece el cliente.	Cadena de caracteres
Equipos	Número total de equipos del cliente con productos Cytomic instalados.	Numérico
Indicadores de ataque (IOA) detectados	Número total de indicadores de ataque detectados en los equipos del cliente.	Numérico
Indicadores de ataque (IOA) pendientes	Número de indicadores de ataque detectados en los equipos del cliente que todavía no fueron revisados.	Numérico

Campo	Descripción	Valores
Última detección	Fecha de aparición del último indicador de ataque.	Fecha

Tabla 7.18: Campos del fichero exportado del listado Indicadores de ataque

Herramienta de filtrado

Campo	Descripción	Valores
Estado	• **Archivado**: el IOA ya no requiere atención por parte del administrador al tratarse de un falso positivo o por haberse completado las tareas de resolución. • **Pendiente**: el IOA no ha sido investigado por el administrador.	Enumeración
Riesgo	Importancia del impacto del IOA detectado.	• Crítico • Alto • Medio • Bajo • Desconocido
Indicador de ataque (IOA)	Nombre de la regla que detecta el patrón de eventos que genera el IOA. Únicamente se muestran los nombres de las reglas de los IOAs mostrados en el listado.	Enumeración
Acción	Tipo de acción ejecutada por el software de protección instalado en el equipo.	• Informado • Ataque bloqueado
Táctica	Categoría de la táctica de ataque que generó el IOA, mapeado según la especificación MITRE. Únicamente se muestran en el desplegable las tácticas asociadas a los IOAs mostrados en el listado.	Enumeración
Técnica	Categoría de la técnica de ataque que generó el IOA, mapeado según la especificación MITRE. Únicamente se muestran en el desplegable las	Enumeración

Campo	Descripción	Valores
	técnicas asociadas a los IOAs mostrados en el listado.	
Última detección	Periodo en el que detectaron los indicadores de ataque.	• Últimas 24 horas • Últimos 7 días • Último mes

Tabla 7.19: Campos de filtrado para el listado Indicadores de ataque (IOA)

Resultado de la instalación de parches

El usuario de la consola de CYTOMIC Nexus solo tendrá acceso a los datos correspondientes a aquellos clientes sobre los que disponga de visibilidad.

Este listado resume el historial de instalación de parches de cada cliente, y muestra el estado final de cada parche que se ha intentado instalar en cada equipo del cliente. De esta forma:

- Si se intentó instalar un mismo parche varias veces en un equipo pero no se consiguió, solo se registrará la última vez que se intento instalar.
- Si se intentó instalar un mismo parche varias veces en un equipo y finalmente se consiguió instalar, solo se registrará una vez como instalación correcta.
- Si un parche se instala correctamente en 2 equipos, se mostrará como 2 instalaciones correctas.

Campo	Descripción	Valores
Cliente	Nombre o identificador del cliente.	Cadena de caracteres
Grupo	Nombre del grupo al que pertenece el cliente.	Cadena de caracteres
Gestión de parches	Indica si el cliente tiene contratado Cytomic Patch o no.	Cadena de caracteres

Campo	Descripción	Valores
Equipos que requieren reinicio	Indica el número de equipos del cliente que están pendientes de reinicio para completar la instalación o desinstalación de parches.	Numérico
Resultado de la instalación de parches	Barra con sectores de colores que indica el último resultado de la instalación de los parches en los equipos de los clientes.	• **Verde**: número de parches instalados. • **Amarillo**: número de parches que requieren un reinicio del equipo para su instalación. No se tienen en cuenta los parches que requieren un reinicio del equipo para su desinstalación, con lo que este número podría no coincidir con el campo **Equipos que requieren reinicio**. • **Naranja**: número de parches con error en su instalación. • **Rojo**: número de parches con error en su descarga. • **Gris**: el cliente no tiene ningún equipo con los criterios seleccionados.

Tabla 7.20: Campos del listado Resultado de la instalación de parches

Campos mostrados en el fichero exportado

El fichero exportado contiene el registro de las operaciones realizadas en cada equipo de cada cliente con una licencia de Cytomic Patch asignada. Se registra la instalación y desinstalación de parches, así como los errores. Solo se registra la última operación de cada tipo en cada equipo.

Campo	Descripción	Valores
Cliente	Nombre o identificador del cliente.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	• Estación • Portátil • Servidor

Campo	Descripción	Valores
Equipo	Nombre del equipo	Cadena de caracteres
Dirección IP	Dirección IP del equipo	Numérico
Dominio	Dominio al que pertenece el equipo	Cadena de caracteres
Descripción		Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Grupo	Nombre del grupo al que pertenece el equipo.	Cadena de caracteres
Fecha	Fecha de la última operación realizada con el parche	Fecha
Programa	Nombre del programa o versión del sistema operativo involucrado en el proceso de parcheo.	Cadena de caracteres
Versión	Numero de versión del programa involucrado en el proceso de parcheo.	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)

Campo	Descripción	Valores
		• 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
Instalación	Estado del parche involucrado en la operación realizada.	• Instalado • Requiere reinicio • El parche ya no es requerido • Desinstalado (requiere reinicio) • Error
Error de instalación	Especifica el tipo de error en la operación realizada.	• Error en la instalación • Error en la desinstalación • Error en la descarga
URL de descarga	URL para descargar el parche de forma	Cadena de

Campo	Descripción	Valores
	individual.	caracteres
Código de resultado	Código resultado de la operación realizada. Puede indicar el éxito o el motivo del fracaso de la operación. Consulta la documentación del proveedor para interpretar el código de resultado.	Numérico
Nombre de la tarea	Nombre de la tarea asociada a la operación en el equipo.	Cadena de caracteres
Fecha de lanzamiento de la tarea	Fecha para la que se programa la ejecución de la tarea asociada al equipo.	Fecha
Fecha de inicio de la tarea	Fecha de comienzo de ejecución de la tarea asociada al equipo.	Fecha
Fecha de finalización de la tarea	Fecha en que finaliza la ejecución de la tarea asociada al equipo.	Fecha

Tabla 7.21: Campos del fichero exportado del listado Resultado de la instalación de parches

Herramienta de filtrado

Campo	Descripción	Valores
Buscar	Filtra por el nombre del cliente o grupo al que pertenece.	Cadena de caracteres
Mostrar	Muestra todos los clientes o solo aquellos que tienen contratado Cytomic Patch	• Todos los clientes • Sólo clientes con gestión de parches
Fecha	Intervalo de fechas en el que se registró la operación de Cytomic Patch en los equipos del cliente.	• Últimas 24 horas • Últimos 7 días

Campo	Descripción	Valores
		• Último mes
Plataforma	Filtra según el sistema operativo instalado en los equipos del cliente.	• Todos • Windows • Linux • macOS
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Instalación	Filtra por el resultado de la instalación de parches en los equipos del cliente.	• Instalado • Requiere reinicio • Error de descarga • Error de instalación
Criticidad	Filtra por la importancia del parche instalado en los equipos del cliente.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad)

Tabla 7.22: Campos de filtrado para el listado Resultado de la instalación de parches

Listado Usuarios de los clientes

Ofrece información global sobre los usuarios que acceden a la consola de administración de los clientes gestionados por el partner. Este listado resulta muy útil cuando se trata de redes muy amplias, ya que especifica qué usuario ha accedido a la consola y cuándo lo ha hecho. Además, se informa acerca de la modificación de la contraseña de acceso a la consola y si ha sido necesario utilizar el doble factor de verificación.

Para que los usuarios del cliente se muestren en el listado, es necesario que el partner tenga acceso a la consola del cliente. En la consola del cliente haz clic en ***Configuración****, menú lateral* ***Usuarios*** *y marca la casilla* ***Permitir a mi distribuidor acceder a mi consola****.*

Campo	Descripción	Valores
Cliente	Nombre o identificador del cliente.	Cadena de caracteres
Grupo	Nombre del grupo al que pertenece el cliente.	Cadena de caracteres
Usuario	Nombre y apellido del usuario. Si el usuario no ha introducido su nombre y apellido, se mostrará el indicativo de la dirección de correo anterior a la @. Ejemplo: si el usuario es *mi.usuario@gmail.com* , se mostrará *mi.usuario* Al hacer clic se abre la consola del cliente con la ventana **Usuarios** (no disponible si el usuario que accede a la consola de CYTOMIC Nexus tiene permiso de solo lectura).	Cadena de caracteres
Email	Dirección de correo electrónico del usuario. Al hacer clic se abre la consola del cliente con la ventana **Usuarios** (no disponible si el usuario que accede a la consola de CYTOMIC Nexus tiene permiso de solo lectura).	Cadena de caracteres
Rol	Rol asignado a la cuenta de usuario.	Cadena de caracteres

Campo	Descripción	Valores
Estado	Indica si la cuenta de usuario está activada o bloqueada.	Cadena de caracteres
2FA requerido	Indica si es necesario utilizar el doble factor de verificación (2FA) para acceder a la consola de administración. Al hacer clic se abre la consola del cliente con la ventana**Seguridad**, donde se puede activar o desactivar el requerimiento de 2FA (no disponible si el usuario que accede a la consola de CYTOMIC Nexus tiene permiso de solo lectura).	Cadena de caracteres
2FA activado	Indica si el usuario tiene activado el doble factor de verificación (2FA).	Cadena de caracteres
Contraseña cambiada	Informa sobre el día y la hora en que se modificó la contraseña de acceso a la consola de administración por última vez.	Cadena de caracteres
Último acceso	Indica el día y hora en que el usuario accedió por última vez a la consola de administración.	Numérico

Tabla 7.23: Campos del listado Usuarios de los clientes

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Cliente	Nombre o identificador del cliente.	Cadena de caracteres
Grupo	Nombre del grupo al que pertenece el cliente.	Cadena de caracteres
Usuario	Nombre y apellido del usuario. Si el usuario no ha introducido su nombre y apellido, se mostrará el indicativo de la dirección de correo anterior a la @. Ejemplo: si el usuario es *mi.usuario@gmail.com* , se mostrará *mi.usuario*	Cadena de caracteres

Campo	Descripción	Valores
Email	Dirección de correo electrónico del usuario.	Cadena de caracteres
Rol	Rol asignado a la cuenta de usuario.	Cadena de caracteres
Estado	Indica si la cuenta de usuario está activada o bloqueada.	Cadena de caracteres
2FA requerido	Indica si es necesario utilizar el doble factor de verificación (2FA) para acceder a la consola de administración.	Cadena de caracteres
2FA activado	Indica si el usuario tiene activado el doble factor de verificación (2FA).	Cadena de caracteres
Contraseña cambiada	Informa sobre el día y la hora en que se modificó la contraseña de acceso a la consola de administración por última vez.	Cadena de caracteres
Último acceso	Indica el día y hora en que el usuario accedió por última vez a la consola de administración.	Numérico

Tabla 7.24: Campos del listado Usuarios de los clientes

Herramienta de filtrado

Campo	Descripción	Valores
Buscar cliente	Filtra los clientes según su nombre.	Cadena de caracteres
Buscar grupo	Filtra los clientes por grupos.	Cadena de caracteres
Buscar usuario	Filtra los usuarios según el contenido del campo **Usuario** o **Email**.	Cadena de caracteres
Email	Filtra los usuarios según su correo electrónico.	Cadena de caracteres

Campo	Descripción	Valores
Estado	Estado de la cuenta de usuario.	• Todos • Activado • Bloqueado
2FA requerido	Filtra en función de si es necesario 2FA para acceder a la consola de administración.	• Todos • No • Sí
2FA activado	Filtra en función de si 2FA está activado o no.	• Todos • No • Sí
Contraseña cambiada	Filtra según el tiempo en que se modificó la contraseña de acceso a la consola por última vez.	• En cualquier momento • Hace más de un mes • Hace más de dos meses • Hace más de tres meses • Hace más de cuatro meses • Hace más de cinco meses • Hace más de seis meses • Hace más de un año
Último acceso	Filtra según el tiempo en el que se accedió a la consola de administración por última vez.	• En cualquier momento • Hace menos de un mes • Hace menos

Campo	Descripción	Valores
		de dos meses • Hace menos de tres meses • Hace más de un mes • Hace más de tres meses • Hace más de seis meses • Hace más de un año

Tabla 7.25: Campos de filtrado para el listado Usuarios de los clientes

Tareas

Una tarea es un recurso implementado en CYTOMIC Nexus que permite añadir dos características nuevas a la ejecución de un proceso: la repetición y el aplazamiento de su inicio.

- **Repetición**: configura la tarea para ejecutarla de forma puntual o repetida a lo largo del tiempo.
- **Aplazamiento**: configura la tarea para ejecutarla en el momento en que se define (tarea inmediata), o aplazada en el tiempo (tarea programada).

CONTENIDO DEL CAPÍTULO

Introducción al sistema de tareas

Productos de seguridad compatibles

El usuario de la consola de CYTOMIC Nexus puede definir y enviar tareas de forma centralizada a los productos de seguridad de sus clientes que que pertenecen a la familia Endpoint:

- Advanced EDR (solo para tareas de instalación de parches)
- Advanced EPDR

Acceso al sistema de tareas

- Selecciona el menú superior **Clientes**.
- Haz clic en **Configuración de los productos de los clientes**. Se abrirá una pestaña nueva en el navegador.
- Selecciona el menú superior **Tareas**. Se abrirá una ventana con el listado de tareas configuradas.

Secuencia completa para lanzar una tarea

El proceso para lanzar una tarea consta de los pasos siguientes:

- **Crear y configurar la tarea**: establece los clientes afectados, las características de la tarea, el momento en que será lanzada y el número de veces que se ejecutará. Una vez creada la tarea, ésta se enviará a los clientes incluidos como destinatarios. Al recibir la tarea en la consola del cliente, ésta se mostrará con la etiqueta "CYTOMIC Nexus", y se le asignará el grupo **Todos** para que se ejecute en todo el parque informático. Las tareas enviadas por CYTOMIC Nexus no pueden ser modificadas por el cliente, a no ser que la relación que une a CYTOMIC Nexus con el producto del cliente se rompa.
- **Publicar la tarea**: cuando se publica una tarea en CYTOMIC Nexus, ésta se introduce en el programador de procesos de los productos contratados por los clientes que la han recibido.
- **Ejecutar la tarea**: el programador lanza el proceso en los equipos del cliente cuando se alcanzan las condiciones especificadas en la definición de la tarea.
- **Recoger los resultados**: CYTOMIC Nexus recopila y consolida los resultados generados por todos los equipos de los clientes que ejecutaron la tarea.

Tipos de procesos ejecutados por una tarea

CYTOMIC Nexus puede ejecutar como tarea los procesos siguientes:

- Análisis y desinfección de ficheros: consulta **Configurar una tarea de análisis (4)**.
- Instalar parches: actualizaciones del sistema operativo y de los programas instalados en los equipos de los clientes. Consulta **Configurar una tarea de Cytomic Patch (4)**.

Resumen de los permisos asociados a la gestión de tareas

- Los usuarios de la consola con permisos de sólo lectura no pueden crear, copiar, eliminar, cancelar ni publicar tareas.
- Todos los usuarios pueden ver el listado de tareas configuradas, independientemente de su visibilidad asignada.

- Para publicar, eliminar o cancelar una tarea es necesario que el usuario tenga visibilidad sobre todos los clientes asignados a la tarea.
- Solo se pueden añadir o eliminar destinatarios de una tarea si el usuario tiene visibilidad sobre ellos.

Crear una tarea

Permisos requeridos

- Usuarios de la consola con alguno de los permisos siguientes:
    - Control total
    - Administrador de licencias y seguridad
    - Administrador de seguridad
- Visibilidad sobre los clientes que se asignarán a la tarea.

Crear una tarea

Seleccionael menú superior **Tareas**. Se abrirá una ventana con un listado que contiene todas las tareas creadas y su estado.

Haz clic en el botón **Añadir tarea** y elige el tipo de tarea en el desplegable. Se abrirá la ventana **Nueva tarea** con los datos de la tarea, distribuidos en varias zonas:

- **Información general (1)**: nombre y descripción de la tarea.
- **Destinatarios (2)**: equipos que recibirán la tarea. Consulta **Destinatarios de la tarea (2)**.
- **Programación (3)**: momento en el que se lanzará la tarea.
- **Configuración (4)**: acciones a ejecutar por la tarea. Esta sección varía según el tipo de tarea y se detalla en la documentación asociada al módulo relacionado.

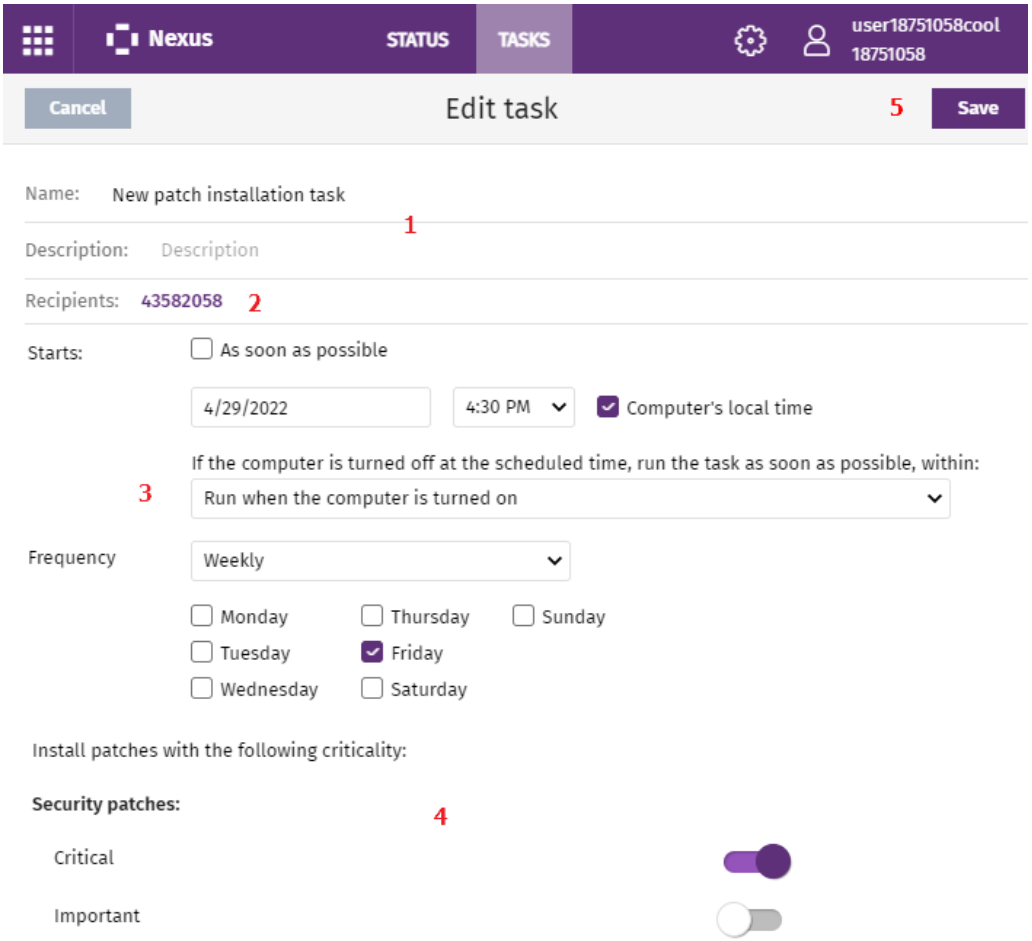

Figura 7.15: Crear una tarea

Destinatarios de la tarea (2)

Establece los clientes o grupos de clientes que recibirán la tarea.

- En la ventana **Editar tarea**, haz clic en el enlace **Destinatarios (No se ha asignado a ningún destinatario)**. Se abrirá la ventana **Destinatarios**.

> *Para acceder a la ventana de selección de clientes, es necesario guardar previamente la tarea. Si la tarea no ha sido guardada, se mostrará una ventana de advertencia.*

- Haz clic en el icono . Se abrirá la ventana **Añadir clientes**.
- Selecciona el cliente o grupo de clientes que recibirán la tarea y haz clic en el botón **Añadir** situado al final de la ventana. Se abrirá la ventana **Destinatarios** con la selección realizada.

- Por defecto, la tarea se asigna a todos los equipos y dispositivos de los clientes o grupos de clientes seleccionados. Para seleccionar los tipos de equipos y dispositivos a los que se desea asignar la tarea, haz clic en el enlace **Todos los tipos de equipos**.
- En la ventana **Tipo de dispositivo**, selecciona el tipo de equipos del cliente que recibirán la tarea: **Estación**, **Portátil**, **Servidor** o **Dispositivo móvil**.

  No todos los tipos de equipos pueden recibir todos los tipos de tareas:

Tipo de tarea	Estación	Servidor	Portátil	Dispositivo móvil
Análisis	X	X	X	X
Instalación de parches	X	X	X	

Tabla 7.26: Tareas aplicables a cada tipo de equipo o dispositivo

- Utiliza el botón  para agregar clientes o grupos de clientes, y  para eliminarlos.
- En la ventana **Tareas**, utiliza el botón **Ver equipos** para verificar los equipos que recibirán la tarea.

Configurar tareas

Programación horaria y repetición de la tarea (3)

Se establece mediante tres parámetros:

- **Empieza**: marca el inicio de la tarea.

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 cuando 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. Utiliza la casilla **Hora local del dispositivo** para lanzar la tarea a la hora del equipo o dispositivo. Si la casilla no está seleccionada, la tarea se lanzará a la hora establecida en el servidor de CYTOMIC Nexus.
Equipo apagado	Si el equipo está apagado o inaccesible, la tarea no se podrá lanzar. El

Valor	Descripción
	sistema de programación de tareas permite establecer la caducidad de la tarea en función del intervalo de tiempo definido por el administrador, desde 0 (la tarea caduca de forma inmediata si el equipo no está disponible) a infinito (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 o no es accesible. • **Dar un margen de x**: define 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 sino que se espera de forma indefinida a que el equipo esté accesible para lanzar la tarea. Si el valor seleccionado es menor que la frecuencia de ejecución se mostrará una advertencia en rojo.

Tabla 7.27: Programación y repetición de una tarea

- **Tiempo máximo de ejecución** (disponible solo en tareas de tipo Análisis programado): indica el tiempo máximo que la tarea puede tardar en completarse, transcurrido el cual la tarea se cancelará con error si no ha terminado.

Valor	Descripción
Sin límite	La duración de la ejecución de la tarea no está definida, pudiéndose extender 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.

Tabla 7.28: Tiempo de ejecución de una tarea

- **Frecuencia**: establece un intervalo de repetición cada día, semana, mes o año tomando como referencia la fecha indicada en el campo Empieza:

Valor	Descripción
Ejecución única	La tarea se ejecuta de forma puntual a la hora indicada en el campo **Empieza**.

Valor	Descripción
Diaria	La tarea se ejecuta todos los días a la hora indicada en el campo **Empieza**.
Semanal	Selecciona las casillas para establecer la ejecución de la tarea en los días de la semana elegidos, a la hora indicada en el campo **Empieza**.
Mensual	Elige una de las opciones: • Ejecutar la tarea un día concreto de cada mes. Si se eligen los días 29, 30 o 31 y el mes no tiene esos días, la tarea se ejecuta el último día del mes. • Ejecutar la tarea el primer, segundo, tercer, cuarto o ultima día de la semana de cada mes.

Tabla 7.29: Establecer la frecuencia de una tarea

Configurar una tarea de análisis (4)

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**: se realiza un análisis profundo del equipo. El análisis incluye a todos los dispositivos de almacenamiento conectados al equipo. Completar esta tarea puede requerir horas.
	• **Áreas críticas**: se realiza un análisis rápido del equipo. Completar esta tarea requiere minutos. Se incluye:
	  • %WinDir%\system32
	  • %WinDir%\SysWow64
	  • Memoria
	  • Sistema de arranque
	  • Cookies
	• **Elementos específicos**: se indican 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.

Valor	Descripción
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 de seguridad analiza los programas instalados en el equipo del usuario de forma estática, sin ejecutarlos, con lo que se reducen las posibilidades de detectar ciertos tipos de amenazas. Para mejorar el ratio de detección en este tipo de análisis, CYTOMIC Nexus puede utilizar algoritmos heurísticos. El software de seguridad tratará como sospechoso a un programa únicamente si éste ha sido detectado mediante la protección heurística.
Analizar archivos comprimidos	Descomprime y analiza los archivos empaquetados.
Excluir del análisis los siguientes archivos	• **No analizar los archivos excluidos para las protecciones permanentes**: los archivos cuya ejecución ha sido permitida por el administrador no serán analizados. Tampoco lo serán 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**: escribe el nombre de los archivos que no se analizarán, separados por comas. • **Carpetas**: escribe el nombre de las carpetas que no se analizarán, separados por comas.

Tabla 7.30: Configurar una tarea de análisis

Configurar una tarea de Cytomic Patch (4)

Las opciones de instalación de parches configuran los parámetros del módulo de Cytomic Patch para actualizar los componentes de los equipos de los clientes.

*Si necesitas modificar la configuración de Cytomic Patch asignada a los equipos de los clientes para permitir la instalación o no de parches en ellos, consulta el capítulo **Cytomic Patch(Actualización de programas vulnerables)**, apartado **Configuración del descubrimiento de parches sin aplicar** de la Guía de administración del producto.*

Valor	Descripción
Parches de seguridad	Indica el nivel de criticidad de los parches a instalar: • Crítica • Importante • Moderada • Baja • No clasificado • Otros parches (no de seguridad) • Service Pack
Instalar parches de los siguientes productos	Utiliza las casillas de selección del árbol de productos para indicar qué productos recibirán parches. 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 el nodo Adobe se seleccionarán todos los nodos situados debajo de él. • Si seleccionas un nodo y posteriormente Cytomic Patch 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 Cytomic Patch agrega dentro de Adobe un nodo nuevo (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 Patch 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 Patch agrega una entrada nueva en el árbol después de que el administrador haya configurado una tarea de parcheo, y esta entrada es

Valor	Descripción
	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.
Opciones de reinicio	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 inhabilitará. 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 aplicado 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 aplicado tanto a estaciones de trabajo como a servidores.

Tabla 7.31: Configurar una tarea de Cytomic Patch

Guardar la tarea (5)

Al guardar la tarea, CYTOMIC Nexus ejecuta las siguientes acciones:

- La tarea se añade a la lista de tareas de CYTOMIC Nexus con el estado **No publicada**.
- La tarea se envía a todos los clientes destinatarios de la tarea.
- En cada consola del cliente, la tarea se añade al grupo **Todos** para poder ejecutarse sobre todos los equipos de la red.
- En la consola del cliente, la tarea se marca con el tag *CYTOMIC Nexus*, que indica que es de solo lectura.

Versiones anteriores del software de protección

Si alguno de los equipos del parque informático tiene instalada una versión antigua del software de seguridad, es posible que no sea capaz de interpretar correctamente las configuraciones de frecuencia establecidas por CYTOMIC Nexus. En este caso, cada equipo establecerá las siguientes correspondencias para la configuración de la frecuencia en las tareas a ejecutar:

- **Tareas diarias**: sin cambios.
- **Tareas semanales**: se omiten los días elegidos por el administrador. La primera ejecución se realiza en la fecha indicada en **Empieza** y, a partir de este punto, se ejecutará nuevamente cada 7 días.
- **Tareas mensuales**: se omiten los días elegidos por el administrador. La primera ejecución se realiza en la fecha indicada en **Empieza** y, a partir de este punto, se ejecutará nuevamente cada 30 días.

Listado de tareas

Permisos requeridos

Todos los usuarios de CYTOMIC Nexus puede ver el listado de tareas, independientemente de los permisos y de la visibilidad asignada a su cuenta.

Acceso al listado de tareas

Selecciona el menú superior **Tareas** para listar tareas creadas, su tipo, estado y otra información relevante.

Campo	Comentario	Valores
Icono	Tipo de la tarea	• Tarea de tipo instalación de parches. • Tarea de tipo análisis programado.
Nombre	Nombre de la tarea creada	Cadena de caracteres
Programación	Cuándo se ejecuta la tarea.	Cadena de caracteres

Campo	Comentario	Valores
Estado	• **Sin destinatarios**: la tarea no se ejecutará porque no tiene destinatarios asignados. Asigna uno o más clientes a la tarea. • **Sin publicar**: la tarea no se ejecutará porque no ha entrado en la cola del programador de los clientes. Publica la tarea para que se envíe a los clientes y el programador de procesos planifique su ejecución. • **En curso**: la tarea se está ejecutando o ha finalizado en algunos o todos los equipos de los clientes. • **Cancelada**: la tarea fue cancelada de forma manual. No implica que todos los procesos en ejecución en los diferentes clientes se hayan detenido.	Cadena de caracteres

Tabla 7.32: Campos del listado Tareas creadas

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de tarea	Clase de la tarea	• Análisis • Instalación 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

Campo	Comentario	Valores
		• Descendente

Tabla 7.33: Campos de filtrado para el listado Tareas creadas

Gestionar tareas

Permisos requeridos

- Usuarios de la consola con alguno de los permisos siguientes:
  - Control total
  - Administrador de licencias y seguridad
  - Administrador de seguridad
- Visibilidad sobre todos los clientes que están asignados a la tarea para modificar los parámetros permitidos.
- Visibilidad sobre los destinatarios a añadir o eliminar de la tarea.

Acceso a la gestión de tareas

Seleccionael menú superior **Tareas** para publicar, borrar, copiar, cancelar o visualizar los resultados de las tareas creadas.

Publicar tareas

Las tareas creadas, configuradas y con destinatarios asignados se muestran en el listado de tareas con la etiqueta **Sin publicar**. Al hacer clic en el enlace **Publicar**, CYTOMIC Nexus introduce la tarea en el programador del producto del cliente, que se encarga de establecer el momento en que se lanzan las tareas según su configuración.

Es necesario que la tarea tenga destinatarios asignados para ser publicada. No se permite publicar una tarea si tiene grupos de clientes asignados pero están vacíos.

Modificar tareas

Haz clic en el nombre de la tarea para modificar su configuración. Dependiendo del estado y de la visibilidad del usuario, es posible modificar la información general de la tarea, sus destinatarios, la programación que tenga asociada o su configuración. Para conocer las distintas partes que componen una tarea consulta **Crear una tarea**.

- **Tareas no publicadas**:

Para modificar cualquier parámetro de la tarea (información general, destinatarios, programación o configuración) el usuario tiene que tener visibilidad sobre todos sus destinatarios.

- **Tareas publicadas sin programación recurrente**:
    - No se puede modificar ningún parámetro de la tarea (información general, destinatarios, programación ni configuración).
    - Para modificar los parámetros de la tarea, copiala y modifica la copia.
- **Tareas publicadas con programación recurrente**:
    - Se permite modificar la información general de la tarea si el usuario tiene visibilidad sobre todos sus destinatarios.
    - Se permite añadir o quitar destinatarios si el usuario tiene visibilidad sobre ellos.
    - No se permite modificar la programación ni la configuración.
- **Tareas canceladas o con error**: no se puede modificar ningún parámetro de la tarea ((información general, destinatarios, programación ni configuración).

Cancelar tareas publicadas

Solo se pueden cancelar las tareas en estado **En curso**. Solo se podrán cancelar aquellas tareas en las que el usuario de la consola tenga visibilidad sobre todos los clientes asignados.

- Selecciona las casillas de las tareas a cancelar y haz clic en el icono **Cancelar** de la barra de herramientas. Se abrirá una ventana de confirmación.
- Haz clic en el botón **Aceptar**. Las tareas se cancelarán, aunque no se borrarán de la ventana de tareas para poder acceder a sus resultados.

Borrar tareas

Las tareas ejecutadas no se eliminan automáticamente de la consola de CYTOMIC Nexus.

Para borrar una tarea:

- Comprueba que el usuario tiene visibilidad sobre todos los clientes que tienen asignada la tarea. Si no es así, el usuario tendrá inhabilitado el icono de borrar  .
- Comprueba que la tarea está en un estado válido para ser borrada:
    - **En curso**: es necesario cancelarla previamente.
    - **Sin publicar**.
    - **Cancelada**.
- Selecciona las casillas. Se mostrará la barra de herramientas en la parte superior de la ventana.
- Haz clic en el icono  . Se abrirá una ventana de confirmación indicando que se borrará la tarea de todos los clientes asignados.
- Si se confirma el borrado, la tarea se borrará de las consolas de los clientes.

- Se eliminará completamente la tarea de CYTOMIC Nexus junto a todos los resultados de los clientes.

Copiar tareas

Para crear una tarea nueva con la misma configuración, haz clic en su icono asociado. Los destinatarios no se copiarán.

Resultados de una tarea

Haz clic en el enlace **Ver resultados** de una tarea publicada, finalizada o cancelada para mostrar los resultados obtenidos hasta el momento.

Campo	Descripción	Valores
Cliente	Nombre del cliente asociado al resultado de la ejecución de la tarea. Haz clic para acceder al dashboard que se corresponde con el tipo de tarea en la consola del cliente.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de CYTOMIC Nexus a la que pertenece el cliente.	Cadena de caracteres
Parches instalados	Este campo solo se muestra en las tareas de instalación de parches. Número de parches instalados en los equipos del cliente en la última repetición de la tarea. Haz clic para acceder al detalle de la tarea en la consola del cliente. Consulta la guía de administración del producto instalado en el cliente.	Cadena de caracteres
Detecciones	Este campo solo se muestra en las tareas de análisis. Número de detecciones en los equipos del cliente en la última repetición de la tarea. Haz clic para acceder al detalle de la tarea en la consola del cliente. Consulta la guía de administración del producto instalado en el cliente.	Cadena de caracteres

Tabla 7.34: Campos del resultado de una tarea

Para comprobar el resultado de la instalación de parches en los equipos de los clientes, consulta ***Resultado de la instalación de parches****.*

Ajuste automático de los destinatarios de una tarea

Si el usuario de la consola de CYTOMIC Nexus establece un grupo de clientes como destinatario de una tarea, el conjunto final de clientes sobre los que se ejecutará puede variar a lo largo del tiempo. Esto es debido a que los grupos son entidades dinámicas que el usuario de CYTOMIC Nexus puede alterar.

Por ejemplo: una tarea definida en el momento T1 y asignada a un grupo tendrá como destinatarios los clientes que forman el grupo seleccionado; pero en un momento de ejecución posterior T2, los miembros de ese grupo podrían haber cambiado. Por esta razón, es necesario establecer el comportamiento de CYTOMIC Nexus y del producto instalado en el cliente cuando el grupo destinatario de una tarea sufre cambios en su composición.

Tareas sin publicar

Cuando un cliente entra o sale de un grupo asignado a una tarea, se actualiza el listado de clientes asignados en la consola de CYTOMIC Nexus , se envía la tarea a la consola de los clientes que pertenecen al grupo y se elimina de aquellos que ya no pertenecen.

Tareas publicadas

Clientes que entran en un grupo asignado a tareas programadas de ejecución única:

Las tareas no se crean en los nuevos clientes.

Clientes que entran en un grupo asignado a tareas programadas de ejecución repetida:

El cambio en los miembros del grupo se tiene en cuenta en la siguiente repetición de la tarea, y los clientes que entraron al grupo recibirán la tarea en la consola de su producto.

Clientes que entran en un grupo asignado a tareas canceladas:

Las tareas no se crean en los clientes nuevos ya que no se volverán a ejecutar.

Clientes que entran en un grupo asignado a tareas no publicadas:

Se crea la tarea en el cliente para que se pueda ejecutar cuando se cumplan las condiciones de su programación.

Clientes que abandonan un grupo asignado a tareas en curso:

La tarea creada en la consola del cliente sigue su curso pero se rompe su relación con CYTOMIC Nexus: la tarea dejar de ser de solo lectura y se le retira la etiqueta “CYTOMIC Nexus”.

CYTOMIC Nexus borra de la tarea los resultados generados por los clientes que abandonan el grupo.

Clientes que abandonan un grupo asignado a tareas canceladas o publicadas:

Se borra de la consola del cliente la tarea y sus resultados si los hay.

CYTOMIC Nexus borra de la tarea los resultados generados por los clientes que abandonan el grupo.

Sincronización de tareas y relación de CYTOMIC Nexus con los clientes

Mientras exista una relación entre CYTOMIC Nexus y los clientes que gestiona, se sincronizarán entre ambas consolas la creación de tareas, los cambios de estado y los resultados generados. Cuando esta relación se modifica, se producen una serie de cambios tanto en la consola de CYTOMIC Nexus como en la del cliente.

Interrumpir la relación de CYTOMIC Nexus con los clientes

Para que CYTOMIC Nexus envíe a los clientes y sincronice el estado de las tareas creadas es necesario que:

- Exista una relación contractual con el cliente.
- El producto del cliente esté configurado como gestionado. Consulta **Modelos de gestión de servicios para productos de la familia endpoint**.
- El cliente tenga activada la configuración **Permitir a mi distribuidor acceder a mi consola** en la consola de su producto. Consulta **Requisitos para asignar configuraciones centralizadas** en la página **76**.

Si alguno de los puntos anteriores deja de cumplirse, las tareas configuradas en CYTOMIC Nexus no se enviarán ni sincronizarán.

El comportamiento de CYTOMIC Nexus con respecto a la sincronización de tareas que ya fueron enviadas cambia según los casos mostrados a continuación:

- Las tareas no publicadas, finalizadas o canceladas se eliminan de la consola del cliente automáticamente. Los resultados generados por los clientes se eliminan de la tarea en CYTOMIC Nexus.
- Las tareas en curso se mantienen en la consola del cliente, se retira la etiqueta CYTOMIC Nexus y se pueden editar desde la consola del cliente, con lo que éste podrá cancelarlas si lo desea. Los resultados generados por los clientes se eliminan de la tarea en CYTOMIC Nexus.

Reanudar la relación de CYTOMIC Nexus con los clientes

Cuando un cliente reanuda una relación interrumpida con CYTOMIC Nexus, se ejecutan las siguientes acciones:

- El cliente recibe todas las tareas que tuviera anteriormente asignadas. Los resultados previamente generados se restauran en CYTOMIC Nexus.
- Aquellas tareas enviadas por CYTOMIC Nexus antes de la interrupción de la relación y que no han sido modificadas o borradas por el cliente, pasan a modo solo lectura con el tag CYTOMIC Nexus.
- En el caso de tareas enviadas por CYTOMIC Nexus antes de la interrupción de la relación a las que el cliente modificó sus destinatarios, se respetarán los destinatarios y se añade el grupo **Todos**.
- Las tareas enviadas por CYTOMIC Nexus antes de la interrupción de la relación y cuya configuración fue modificada por el cliente se volverán a enviar, creando una tarea nueva.

La cuenta Cytomic

La cuenta Cytomic ofrece al usuario de la consola web un mecanismo de autogestión 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 usuario de la consola web quien crea y activa el método de acceso a la consola web de CYTOMIC Nexus.

CONTENIDO DEL CAPÍTULO

Crear una cuenta Cytomic

Para crear una nueva cuenta Cytomic sigue el procedimiento descrito a continuación.

Recepción del mensaje de correo

- Al adquirir CYTOMIC Nexus recibirás un mensaje de correo electrónico procedente de Cytomic.
- Para acceder a la web desde donde crear la cuenta Cytomic, haz clic en el vínculo que contiene el mensaje.

Rellenar el formulario

- Rellena con tus datos el formulario mostrado.
- Para cambiar el idioma de la página, utiliza el desplegable situado en la esquina inferior derecha.
- Accede al acuerdo de licencia y la política de privacidad haciendo clic en el vínculo correspondiente.
- Para terminar y recibir un mensaje de correo electrónico en la dirección especificada en el formulario haz clic en **Crear**. 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 Central, desde donde podrás acceder a la consola web de CYTOMIC Nexus. Para ello, utiliza el icono de acceso directo que encontrarás en **Mis servicios**.

Modificar la cuenta Cytomic

Si tu proveedor de seguridad asociado es WatchGuard, accede a la web **https://watchguard.com/**

Haz clic en la opción **Edit account**

Figura 7.16: Editar cuenta de usuario

Glosario

A

Antivirus

Software 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).

Árbol de grupos

Estructura jerárquica formada por agrupaciones estáticas, utilizada para organizar el parque de clientes, facilitar la asignación de configuraciones y establecer la visibilidad de los usuarios de la consola web.

Archivo de identificadores / fichero de firmas

Fichero que contiene los patrones que el antivirus utiliza para detectar las amenazas.

Asignación automática / indirecta de configuraciones

Ver Herencia.

Asignación automática de licencias

En este modo de asignación el propio cliente toma automáticamente las licencias del pool del partner que necesite para proteger los equipos que va incorporando a su infraestructura.

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 usuario de la consola web.

Asignación manual de licencias

Procedimiento mediante el cual el usuario de la consola web asigna un número concreto de licencias a los equipos del cliente para que pueda activar el producto contratado. Si el cliente incorpora a su infraestructura un número superior de equipos al de licencias asignadas por el usuario de la consola web, estos equipos quedarán desprotegidos.

B

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.

C

Cliente

Empresa que contrata productos y servicios de seguridad con un partner de Cytomic.

Co-branding

Configuración remota del aspecto de la consola web de gestión que utiliza el cliente para administrar los productos ofrecidos por el partner de Cytomic.

Comunicación en tiempo real

Los equipos del cliente protegidos con productos basados en Cytomic permiten la comunicación en tiempo real con los servidores de Cytomic, lo que se traduce en un despliegue sin retraso de las configuraciones creadas por el usuario de la consola web de CYTOMIC Nexus o por el administrador de la red del cliente.

Cuarentena

Ver Backup.

Cuenta de usuario

Ver Usuario de la consola web.

Cuenta Panda

Mecanismo de autogestión ofrecido por Cytomic mediante el cual el usuario de la consola web puede generar sus propias credenciales de acceso a los servicios contratados, frente al método estándar de recepción de credenciales por correo electrónico.

E

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.

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.

F

Familia de productos

Agrupación de productos de características similares que impiden la instalación en un mismo equipo de dos o más productos que pertenezcan a la misma familia.

Filtros

Conjunto de valores y criterios utilizados para excluir de los listados aquellas entradas que no resulten interesantes al usuario de la consola de administración

G

Grupo

Contenedor de tipo estático que agrupa a uno o más clientes. La pertenencia de un cliente 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 clientes.

I

ISP

Partners que integran su BackOffice con el BackOffice de Cytomic con el objetivo de dar de alta sus clientes y las licencias requeridas por ellos de forma automática. Los clientes y las licencias se visualizarán en la consola web de CYTOMIC Nexus.

L

Licencia

Mecanismo que controla el uso y acceso a los productos desarrollados por Cytomic. Una licencia permite el uso del producto para el que fue emitida durante un periodo de tiempo que varía de 1 a 3 años dependiendo el tipo de licencia.

Licencia virtual

Son las licencias que residen en el pool de licencias y que todavía no han sido asignadas a ningún cliente. Una licencia asignada a un cliente puede ser recuperada en algunos casos y devuelta al pool de licencias si por ejemplo el cliente no disfrutó del servicio por toda la duración contratada debido a un cambio de producto.

Licencias de prueba (trial)

Ofrecen al cliente toda la funcionalidad del producto durante un periodo de tiempo limitado; una vez terminado, el acceso al producto quedará deshabilitado automáticamente

M

Malware

Término general utilizado para referirse a programas que contienen código malicioso (MALicious softWARE), ya sean virus, troyanos, gusanos o cualquier otra amenaza que afecte 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.

Managed Service Provider (MSP)

Partners que venden productos de Cytomic a sus clientes y que además gestionan de forma proactiva su seguridad.

Mantenimiento

Es la asignación de un número concreto de licencias de duración determinada de un producto o módulo a un cliente.

Marca blanca

Versión especial de un producto de seguridad desarrollado por Cytomic que retira todos los elementos visuales que permiten identificar al proveedor de origen, y los sustituye por el logotipo y marca de una tercera empresa, generalmente el partner que distribuye el software y ofrece su mantenimiento.

Mayorista

Son partners que adquieren grandes volúmenes de licencias financiando la compra de las mismas. El mayorista distribuye posteriormente las licencias entre sus partners, y son éstos quienes tratan directamente con el cliente final. El mayorista mantiene licencias en stock, de manera que puede ofrecer una respuesta rápida a la demanda de licencias por parte de sus partners.

Modelo gestionado

Delegación por parte del cliente de la gestión del producto adquirido en el partner. De esta manera el cliente puede despreocuparse completamente de gestionar el servicio, que es mantenido por el propio partner, incrementando de esta forma el valor de los productos que ofrece a sus clientes

Modelo no gestionado

El propio cliente gestiona el producto que ha adquirido. CYTOMIC Nexus evitará el acceso del usuario de la consola web a la consola de administración del producto para no interferir con el cliente.

Módulo

Extensión de un producto que le añade funcionalidades adicionales. Dependiendo de la plataforma y del producto, estarán disponibles distintos módulos.

N

Notificaciones

Sistema de avisos implementado enCYTOMIC Nexus que envía información al usuario de la consola web mediante la consola web

y correo electrónico, avisando de situaciones que pueden requerir de su intervención.

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.

O

On premise

Tipo de software que se ejecuta estrictamente en el ámbito de la oficina del cliente, requiriendo por lo general recursos adicionales (servidores, licencias etc) y su mantenimiento asociado. Por esta razón las soluciones On premise tienen un mayor TCO y una menor flexibilidad a la hora de acceder a sus funcionalidades desde localizaciones remotas.

P

Perfil de configuración

Configuración específica de la protección o de otro aspecto del software administrado. Una vez configurados los perfiles son asignados a un grupo o grupos de clientes y aplicado a todos sus equipos.

Permiso

Configuración específica de acceso que se aplica a una o más cuentas de usuario y autoriza a ver o modificar determinados recursos de la consola.

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.

Plataforma

Entorno donde los productos de la familia Endpoint se alojan en la nube.

Pool de licencias

También llamado "Stock de licencias", es un repositorio donde se almacenan de forma temporal las licencias de los distintos productos adquiridos a Cytomic para asignarlas posteriormente a los clientes.

Producto

Solución de seguridad que pertenece al porfolio deCytomic compatible con CYTOMIC Nexus, y por tanto gestionable por el partner o por grandes compañías.

R

Ransomware

Tipo de malware que bloquea el dispositivo o el acceso a los datos del usuario y exige un rescate a cambio de recuperar su acceso.

Recuperación de licencias

Proceso que devuelve al pool de licencias virtuales aquellas licencias asignadas a los clientes que no han sido disfrutadas completamente. El proceso se desencadena de forma automática al eliminar un producto asignado a un cliente o al cambiar un producto asignado a un cliente por otro.

Renovación

Proceso mediante el cual se extiende por una cantidad de tiempo determinada (1, 2 o 3 años) las licencias de los productos asignados al cliente.

Renovación anticipada (manual) de licencias

Tipo de renovación de licencias donde el usuario de la consola web hace un seguimiento manual para tener conocimiento de la finalización próxima de las licencias de un cliente y poder iniciar el proceso de renovación anticipada de licencias para evitar que los equipos queden desprotegidos

Renovación automática de licencias

Proceso automático implementado por CYTOMIC Nexus que permite renovar las licencias de los productos y módulos asignados a los clientes cuando se aproxima su finalización. De esta manera la gestión se simplifica al no tener que controlar diariamente qué clientes tienen productos con licencias a punto de caducar para iniciar una renovación manual / anticipada.

Resellers

Son partners que compran licencias de productos de CYTOMIC Nexus y las revenden a sus clientes sin ofrecer un valor añadido.

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.

RMM (Remote monitoring and management)

Tipo de software diseñado para ayudar a los proveedores de servicios de TI administrados (MSP) a monitorizar el funcionamiento de los equipos y las redes de sus clientes, así como ejecutar acciones correctivas para resolver los problemas.

Rollback

Desinstalación de los parches instalados por Cytomic Patch que presentan complicaciones o incompatibilidades.

S

Servicio

Agrupación de uno o más mantenimientos asociados a un mismo producto.

Standalone

Software que requiere el acceso local al equipo para su configuración.

T

TCO (Total Cost of Ownership)

El coste total de propiedad refleja los costes directos e indirectos, así como los beneficios, relacionados con un producto o sistema.

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.

U

Usuario de la consola web

Recurso formado por un conjunto de información que CYTOMIC Nexus utiliza para regular el acceso de los técnicos a la consola web y establecer las acciones que éstos podrán realizar sobre los equipos de la red.

Usuario principal

Es el primer usuario que se crea al contratar el servicio CYTOMIC Nexus. Este usuario tiene acceso a todos los recursos y clientes.

V

VDI

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.

Visibilidad

Concepto empleado para acotar el acceso de los técnicos del usuario de la consola web a los activos de determinados grupos de clientes.

VPN (Virtual Private Network)

Tecnología de red que permite interconectar redes privadas (LAN) utilizando un medio público, como puede ser Internet.