Implantación de un sistema DLP en una Clínica Dental

Dámaso Rubén Fenoy Illacer

Máster Universitario en Ciberseguridad y Privacidad

Área de trabajo final: Privacidad

Tutor de TFM
Albert Jové Canela
Profesor responsable
Andreu Pere Isern Deyà

Fecha Entrega
10/01/2023

Universitat Oberta de Catalunya

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Implantación de un sistema DLP en una Clínica Dental*
Nombre del autor:	*Dámaso Rubén Fenoy Illacer*
Nombre del consultor/a:	*Albert Jové Canela*
Nombre del PRA:	*Andreu Pere Isern Deyà*
Fecha de entrega (mm/aaaa):	*01/2023*
Titulación o programa:	Máster Universitario en Ciberseguridad y Privacidad
Área del Trabajo Final:	*Privacidad*
Idioma del trabajo:	*Castellano*
Palabras clave	*DLP, Privacidad, Ciberseguridad*

Resumen del Trabajo

Actualmente todas las organizaciones que utilizan sistemas de información se enfrentan a riesgos de fuga de datos, que pueden suponer problemas competitivos, de imagen, y/o legales. Para mitigar este riesgo aparecen las soluciones DLP (*Data Loss Prevention*). Estas permiten monitorizar las actividades realizadas por parte de los usuarios en los sistemas, el tráfico que viaja por la red, y la información en reposo, con el fin de implantar controles de seguridad que monitoricen o impidan la fuga de datos de forma voluntaria o involuntaria.

En este trabajo se exploran las características de las herramientas DLP, se comparan varias de ellas, y se selecciona la más idónea para su posterior implementación en el marco de una clínica dental. Se elabora una guía de instalación, configuración y evaluación de un conjunto de controles definidos ad hoc, que representan diferentes casos de uso basados en la limitación de utilización de dispositivos extraíbles, de envío de información sensible a través de correo electrónico u otros programas, encriptación

de ficheros que contienen información personal, y escaneo y descubrimiento de información sensible en reposo. A continuación, se realiza un análisis de la contextualización legal a tener en cuenta durante la implantación de este tipo de soluciones para respetar la privacidad de los trabajadores.

El principal resultado obtenido es que estas herramientas permiten establecer de forma sencilla y efectiva un gran conjunto de controles de seguridad que cumplen el objetivo de detectar e impedir la fuga de datos antes de que se produzca.

Abstract

Currently, all organizations that use information systems face risks of data leakage, which can lead to competitive, image, and/or legal problems. To mitigate this risk, DLP (Data Loss Prevention) solutions appear. These allow monitoring the activities carried out by users in the systems, the traffic that travels through the network, and the information at rest, in order to implement security controls that monitor or prevent data leakage voluntarily or involuntarily. .

In this work the characteristics of the DLP tools are explored, several of them are compared, and the most suitable one is selected for its subsequent implementation in the framework of a dental clinic. An installation, configuration and evaluation guide is prepared for a set of ad hoc defined controls, which represent different use cases based on the limitation of the use of removable devices, sending sensitive information through email or other programs, encryption of files containing personal information, and scanning and discovery of sensitive information at rest. Next, an analysis of the legal contextualization to be taken into account during the implementation of this type of solutions to respect the privacy of workers is carried out.

The main result obtained is that these tools make it possible to easily and effectively establish a large set of security controls that meet the objective of detecting and preventing data leakage before it occurs.

Índice

Lista de imágenes

Lista de tablas

1. Introducción

La importancia de la información para las organizaciones se ha ido incrementando en los últimos años, hasta el punto de que esta es, junto a las personas, su activo más importante. Cada vez se almacena un volumen mayor de información relacionada con el negocio, los clientes, los procesos existentes o la propiedad intelectual, y su mal uso puede suponer graves problemas competitivos y legales. Por otro lado, las amenazas a las que está expuesta cualquier empresa u organismo también se han incrementado progresivamente, desarrollándose en paralelo diferentes medidas de protección para que el impacto de estas se vea minimizado, independientemente de si la seguridad se ve comprometida por un actor interno o externo. El objetivo de todas estas medidas es garantizar la confidencialidad, integridad, o disponibilidad de los sistemas de información, con el fin de evitar el daño reputacional, la pérdida de negocio y las posibles sanciones que un incidente de seguridad con fuga de información podría suponer.

Este trabajo explora el escenario de implantación de una herramienta *DLP* (*Data Loss Prevention*, prevención de pérdida de datos). Se define DLP como el conjunto de procesos, técnicas y herramientas que en su conjunto funcionan como una medida de seguridad activa, que permite impedir que se produzcan pérdidas y fugas de información, sean estas intencionadas o no, que se acceda a la información de forma no autorizada, o que esta sea usada con fines diferentes a los previstos.

1.1. Contexto y justificación del Trabajo

Los propios empleados de las organizaciones se pueden convertir en muchas ocasiones en *insiders* -responsables de la fuga de información- por diferentes motivos (Incibe, 2017).

- Económicos: su objetivo es obtener un beneficio a partir de la venta de la información de la compañía.
- Espionaje industrial: su objetivo es obtener información competitiva de los procesos o desarrollos realizados por terceros para beneficiarse de ella.
- Venganza: su objetivo es provocar acciones perjudiciales para la empresa porque existe algún motivo que provoca descontento.
- Desconocimiento: debido a la falta de conocimiento de la normativa de seguridad o las tecnologías utilizadas.

Es necesario contextualizar los tres términos que se usan para referirse con más frecuencia a las fugas de datos (Boolebox, 2022):

- Pérdida de datos: es una pérdida de datos real por parte de una organización, cuyo origen puede ser un accidente (fallo humano, mal funcionamiento del software o hardware y ausencia de copias de seguridad), o en el caso de un agente exterior que impida el acceso a los datos de forma temporal o permanente.
- Fuga de datos: es la exposición no intencionada de información sensible de cualquier índole. Puede ocurrir por publicación involuntaria de esta información en internet, o por pérdida de dispositivos/discos duros o información impresa por parte de los empleados.
- Brecha de datos: es un acceso no autorizado a información sensible por parte de uno o varios ciberdelincuentes, cuyo objetivo es explotar esta información con fines ilegítimos.

En Estados Unidos se produjeron más de dos millones de brechas de seguridad relacionadas con datos en los seis primeros meses del año 2022 (Boolebox, 2022). Para reducir este riesgo, se hace necesaria la puesta en marcha de medidas de seguridad que analicen las acciones de los usuarios, y prevengan las fugas de datos, siempre desde un prisma legal que legitimice los controles establecidos por la empresa.

Los tres casos de uso típicos en los que se despliegan tecnologías DLP son los siguientes (De Groot, 2022):

- Cumplimiento / Protección de información personal: las organizaciones que almacenan datos personales, datos sanitarios, o de medios de pago, requieren de herramientas que identifiquen, clasifiquen y etiqueten este tipo de información, con el objetivo de protegerla y monitorizar las actividades que se realizan en sus sistemas de información. Estas organizaciones están sujetas a normativas de seguridad que contemplan graves sanciones en caso de fugas de información.
- Propiedad intelectual: en el caso de organizaciones cuya misión es almacenar o procesar información competitiva, o altos secretos de estados o terceros, puede suponer un grave daño reputacional que ponga en riesgo su supervivencia.
- Visibilidad de los datos: las organizaciones que tienen como objetivo obtener una mayor visibilidad de los flujos de datos y el uso que le dan a estos los diferentes

trabajadores pueden recurrir a una herramienta DLP para clasificar y monitorizar el uso, obteniendo un mayor conocimiento de sus procesos internos.

El ámbito en el que se desarrolla el trabajo es el de una Clínica Dental ficticia, simulada mediante un laboratorio, que tiene entre cuarenta y cincuenta empleados, contando con los siguientes departamentos:

- Gerencia: formado por una única persona, es el máximo responsable de la clínica y realiza la gestión integral de esta.
- Equipo médico: compuesto por los diferentes profesionales médicos que asisten a los pacientes. A diferencia del resto de empleados, que se encuentran bajo un contrato laboral, algunos miembros del equipo médico se encuentran bajo un contrato mercantil, prestando sus servicios como autónomos.
- Administración: proporcionan apoyo al gerente y realizan las tareas diarias de gestión de la clínica.
- Servicios: personal encargado de mantener las instalaciones de la clínica y sus sistemas en las condiciones adecuadas.

En este escenario, se plantean diferentes situaciones que pueden requerir del uso de una herramienta de DLP:

- El gerente sospecha que ha habido una exfiltración de información, pero desconoce qué empleado puede haberla realizado.
- Existen sospechas de que uno de los médicos quiere irse a trabajar a una empresa de la competencia, llevándose información de los clientes de la clínica que incluyen datos de contacto e historial sanitario.
- La política de seguridad corporativa impide el uso de aplicaciones particulares de correo o almacenamiento en la nube y se quiere verificar que se cumple.
- Se quiere controlar la impresión de documentos que contengan información relacionada con las intervenciones médicas de los pacientes.
- Se quiere verificar que la documentación ubicada en las diferentes unidades compartidas de la Clínica respeta los principios mínimo privilegio y la necesidad de saber de los usuarios que acceden a esta.

1.2. Objetivos

El **objetivo general** es evaluar el uso de una solución de seguridad que prevenga la fuga y pérdida de datos en una clínica dental, a través de una herramienta DLP.

Este se puede dividir en los siguientes objetivos específicos:

- Exponer el funcionamiento de las herramientas de DLP y qué protección ofrecen a las organizaciones.
- Justificar la necesidad de instalar una herramienta DLP en una organización definiendo los casos de uso apropiados.
- Analizar y comparar las principales herramientas DLP en el mercado, seleccionando la más adecuada para el desarrollo del Trabajo.
- Implementar la solución seleccionada en un entorno de pruebas.
- Definir e implementar los diferentes controles de seguridad que se pueden establecer, relacionándolos con los diferentes casos de uso identificados previamente.
- Analizar los aspectos legales a considerar para que los controles de seguridad implementados sean lícitos.

1.3. Enfoque y método seguido

En primer lugar, se presenta el contexto en el que se hacen necesarias herramientas DLP para evitar la fuga de información en entornos empresariales.

Se cuenta con el apoyo del tutor del Trabajo para establecer un objetivo y alcances realistas, que permitan que se alcance un nivel de calidad adecuado en el plano académico, con rigor científico, y que permita obtener asimismo un aprendizaje significativo.

Se cuenta con una planificación detallada que desglosa diferentes tareas y las agrupa en hitos que permitan realizar un seguimiento adecuado, y que acota el trabajo en tiempo y forma.

En la primera fase del proyecto, se realiza la planificación inicial, se expone el estado del arte actual de las soluciones DLP, se justifica la necesidad de usarlas, y se identifican sus tipos y principales características.

En la segunda fase del proyecto, se analizan y comparan las principales características de las soluciones DLP empresariales, y se selecciona una de ellas para su implementación. Se definen los controles de seguridad a aplicar, y se valoran los aspectos legales a considerar para que estos sean conformes con la legislación vigente.

En la tercera fase del proyecto, se evalúa el trabajo realizado, se valora la consecución de los objetivos marcados inicialmente, y se establecen las posibles mejoras del proyecto y líneas de trabajo futuras que pueden derivarse de este.

Este enfoque se considera apropiado por su similitud al que sigue cualquier compañía cuando identifica una nueva necesidad tecnológica, que se traduce en una idea para mejorar alguna de sus dimensiones (de negocio, tecnológica, o de seguridad). Se analizan las posibles alternativas valorando sus pros y contras, y se selecciona e implementa una de ellas. Se configura la herramienta para desempeñar el propósito para el que ha sido adquirida, y se atiende a los aspectos técnicos y legales que son relevantes para su funcionamiento, para finalmente evaluar los resultados obtenidos.

Siguiendo esta estrategia se maximizan las posibilidades de conseguir los objetivos que se han marcado en el Trabajo: se establece en primer lugar un marco teórico que contextualiza el trabajo a realizar, se desarrolla posteriormente de forma aplicada, y por último, se obtienen las conclusiones.

1.4. Planificación del Trabajo

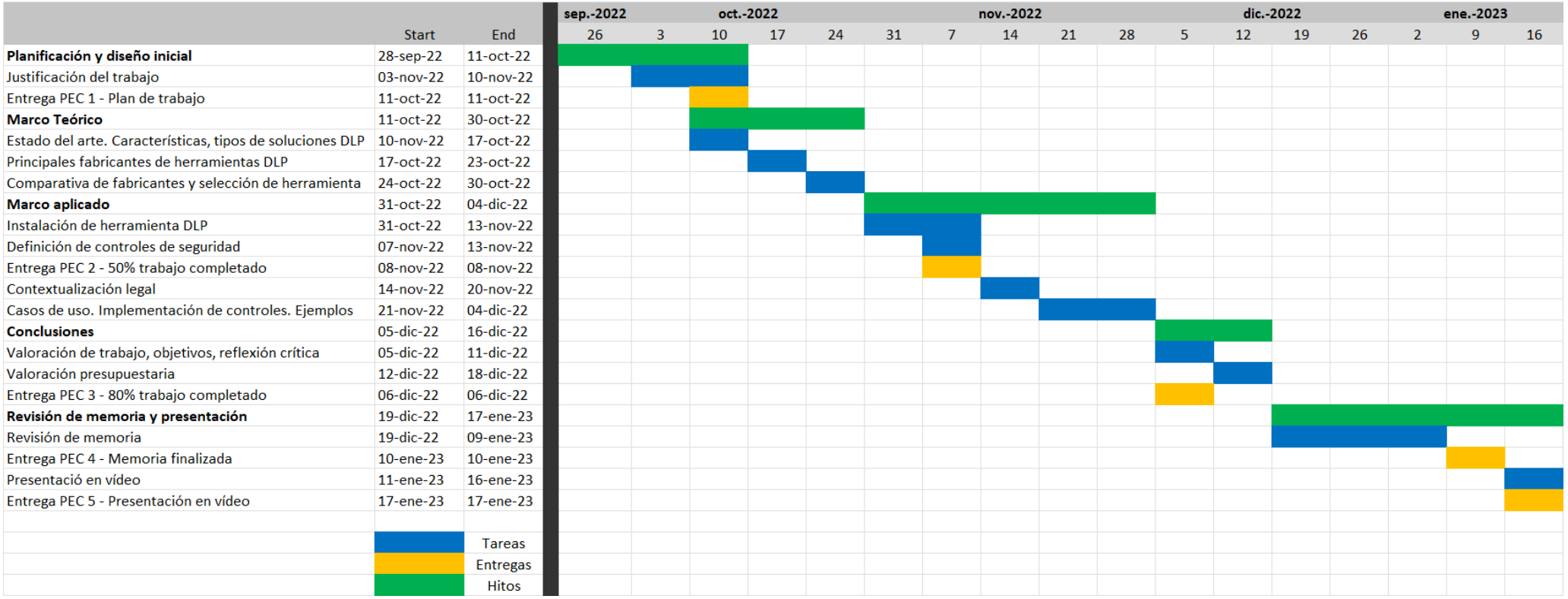
Para la realización del proyecto, serán necesarios los siguientes recursos:

- Infraestructura informática de laboratorio:
    - Servidor centralizado que permita autenticación y compartición de ficheros.
    - Puestos cliente que permitan el uso a los usuarios de gerencia, administración y mantenimiento.
- Licencia de uso de evaluación/académica de una herramienta DLP.

La infraestructura informática de la Clínica dental será simulada mediante el uso de máquinas virtuales o tecnologías en la nube que permitan definir un conjunto de sistemas de información similares a los que se encontrarían en un escenario real.

Se propone asimismo la siguiente planificación con el desglose de tareas más significativas.

Diagrama de Gantt



	Start	End
Planificación y diseño inicial	28-sep-22	11-oct-22
Justificación del trabajo	03-nov-22	10-nov-22
Entrega PEC 1 - Plan de trabajo	11-oct-22	11-oct-22
Marco Teórico	11-oct-22	30-oct-22
Estado del arte. Características, tipos de soluciones DLP	10-nov-22	17-oct-22
Principales fabricantes de herramientas DLP	17-oct-22	23-oct-22
Comparativa de fabricantes y selección de herramienta	24-oct-22	30-oct-22
Marco aplicado	31-oct-22	04-dic-22
Instalación de herramienta DLP	31-oct-22	13-nov-22
Definición de controles de seguridad	07-nov-22	13-nov-22
Entrega PEC 2 - 50% trabajo completado	08-nov-22	08-nov-22
Contextualización legal	14-nov-22	20-nov-22
Casos de uso. Implementación de controles. Ejemplos	21-nov-22	04-dic-22
Conclusiones	05-dic-22	16-dic-22
Valoración de trabajo, objetivos, reflexión crítica	05-dic-22	11-dic-22
Valoración presupuestaria	12-dic-22	18-dic-22
Entrega PEC 3 - 80% trabajo completado	06-dic-22	06-dic-22
Revisión de memoria y presentación	19-dic-22	17-ene-23
Revisión de memoria	19-dic-22	09-ene-23
Entrega PEC 4 - Memoria finalizada	10-ene-23	10-ene-23
Presentació en vídeo	11-ene-23	16-ene-23
Entrega PEC 5 - Presentación en vídeo	17-ene-23	17-ene-23

Imagen 1. Diagrama de Gantt (Elaboración propia)

1.5. Breve sumario de productos obtenidos

Al finalizar el trabajo, se obtendrán los siguientes productos:

1. Revisión del estado del arte: tipos y características principales de las soluciones DLP.
2. Análisis comparativo de varias soluciones DLP comerciales.
3. Guía de implementación de la solución seleccionada para desarrollar el trabajo.
4. Marco legal de interés para la implantación de soluciones DLP en entornos empresariales.

2. Marco teórico

2.1. Características de las soluciones DLP

Las herramientas DLP detectan potenciales fugas de datos y las previenen mediante técnicas de monitorización, detección y bloqueo de información mientras esta está en uso (acciones de endpoint), en tránsito (tráfico de red, cuando la información se envía de un punto a otro), o en reposo (cuando la información es almacenada en un repositorio final). (Lord, 2022).

Las principales características que podemos encontrar en las soluciones DLP empresariales según de Groot (2022) e Imperva (s.f.) son las siguientes:

- Clasificación de información sensible en base a políticas o autodescubrimiento.
- Monitorización continua de acciones realizadas en los clientes para identificar acciones que puedan suponer riesgos de fuga de datos.
- Monitorización y gestión del acceso de usuarios en diferentes programas y aplicaciones web, permitiendo bloquear acciones del usuario.
- Monitorización de dispositivos extraíbles y la información que se almacena en ellos.
- Encriptación de información sensible en tránsito y en reposo.
- Correlación de eventos en tiempo real para identificar posibles amenazas.

Riesgo concreto	**Cómo ayuda DLP**	**Datos en…**		
		Reposo	**Tránsito**	**Uso**
Pérdida de datos por error Pérdida de datos por acto criminal	Transferencias de datos no apropiadas (email, FTP, dispositivos extraíbles, servicios en nube) identificados y bloqueados.		X	X
Centro de Datos ubicados en una jurisdicción inapropiada	N/A			
Datos transferidos a/mantenidos en una jurisdicción inapropiada	Chequeos de entrada durante transferencia de ficheros/bases de datos	(X)	X	X
	Chequeos periódicos para sanear ficheros/bases de datos	X		
Propagación de información sensible	Chequeos periódicos para sanear ficheros	X		

Tabla 1. Cómo ayudan las herramientas DLP a reducir el riesgo (Haller, 2014)

Según Gartner (2021), DLP es un proceso de seguridad con una gran madurez, que se ve reforzado por una tecnología que proporciona garantías, y las organizaciones que buscan implementar más de un caso de uso están desplegando soluciones DLP de tipo

empresarial, cubriendo escenarios de pérdida/robo en equipos finales, correo electrónico, o nube.

2.2. Arquitecturas

Existen diferentes arquitecturas dentro de las soluciones DLP, según dónde se realice la inspección o análisis de los datos en uso (Crowdstrike, 2022).

- Endpoint DLP: se monitorizan los dispositivos finales (puestos cliente de sobremesa o portátiles, tabletas, móviles) donde la información se utiliza o almacena. Las herramientas de este tipo pueden realizar las siguientes acciones:
    - Bloquear de forma inmediata el envío de información confidencial de forma no autorizada, proporcionando al usuario retroalimentación inmediata.
    - Monitorizar y controlar los flujos de información entre grupos y tipos de usuarios.
    - Controlar las aplicaciones de mensajería y correo electrónico antes de que lleguen a la red corporativa, de manera que
    - Monitorizar y controlar el acceso a dispositivos físicos.
    - Clasificar la nueva información generada, ya que son conocedores de qué autor la está creando.
- Network DLP: se monitoriza y protege toda la información en uso, en tránsito o en reposo que viaja por la red de la organización, incluyendo los servicios en la nube. Las herramientas de este tipo pueden realizar las siguientes acciones:
    - Inspeccionar y controlar el tráfico en correo electrónico, aplicaciones web, HTTP/S, FTP/S, y TCP/IP.
    - Incrementar el control y la visibilidad sobre aplicaciones web de correo y FTP, incluyendo aquellas protegidas vía SSL.
    - Prevenir la pérdida de información sensible a través de la red, independientemente del puerto o protocolo.
    - Aplicar monitorización basada en políticas, incluyendo acciones de bloqueo para aplicaciones web.
    - Encriptar las transmisiones de correo electrónico para garantizar la seguridad de las comunicaciones.

- Notificar a los usuarios cuando el tráfico de red viole las políticas de protección de datos corporativas.

- Cloud DLP: es un subconjunto de Network DLP cuyo objetivo específico es proteger a las organizaciones que almacenan o procesan datos en la nube. Las herramientas de este tipo pueden realizar las siguientes acciones:
  - Escanear y auditar información con el objetivo de detectar y encriptar información sensible o de valor compartida con servicios en la nube (de forma independiente a su tipología: IaaS, PaaS o SaaS)
  - Mantener una lista de aplicaciones en la nube autorizadas y el listado de usuarios que pueden acceder a los datos sensibles.
  - Alertar en el caso de violación de la política o actividad anormal.
  - Establecer visibilidad extremo a extremo de todos los datos almacenados en servicios cloud.

2.3. Principales fabricantes y características

Gartner ha realizado en los últimos años varios análisis sobre soluciones de tipo Enterprise Data Loss Prevention (DLP), en los que detalla cuales son los principales fabricantes y los clasifica según su completitud de visión y su habilidad para ejecutar esta tecnología. A partir de esta clasificación, se obtiene un gráfico visual conocido como cuadrante de Gartner, y el último publicado sobre tecnologías DLP data de 2017:

Imagen 2. Cuadrante de Gartner para Data Loss Prevention (Gartner, 2017)

A pesar de haber transcurrido cinco años y de la natural evolución del mercado en cuanto a la aparición de nuevas capacidades, los principales fabricantes siguen siendo los mismos, pero debemos tener en cuenta que McAfee ya no es propiedad de Intel y opera nuevamente como una compañía independiente. Se detallan a continuación sus características principales:

Fabricante	Producto	Descripción alto nivel	Características DLP Endpoint
Symantec	Symantec Data Loss Prevention	Apropiado para entornos híbridos, altamente escalable. Ofrece tecnologías DLP de tipo Endpoint, Network, Cloud y Storage	Previene fugas de datos en correo, navegadores, apps cloud, dispositivos extraíbles y escritorios virtuales
Digital Guardian	Digital Guardian DLP	Solución multiplataforma, amplia protección para ficheros estructurados/no estructurados	Clasificación automatizada, control granular de todos los movimientos de datos.
Forcepoint	Forcepoint DLP	Protección en dispositivos finales multiplataforma.	Control y protección avanzada de datos activos (detección), en movimiento y en uso. Monitorización de aplicaciones de correo, web y cloud
McAfee	McAfee DLP	Prevención extremo a extremo en dispositivos multiplataforma.	Control y protección de dispositivos, correo electrónico, aplicaciones cloud. Administración centralizada.
CoSoSys	Endpoint Protector	Prevención en dispositivos basada en agente multiplataforma	Control de dispositivos, protección basada en contenido, cifrado forzado, descubrimiento electrónico

Tabla 2. Principales fabricantes DLP (Elaboración propia)

A continuación, se analizan en mayor profundidad las soluciones de tres de los principales fabricantes.

2.3.1. Symantec DLP

La solución de Symantec DLP es una suite de productos que ofrece cuatro bloques principales de protección ante fugas de información: Endpoints, Network, Cloud, y Storage.

La solución de Symantec se puede adquirir mediante dos tipos de licenciamiento:

- DLP Core: ofrece protección en dispositivos finales, almacenamiento, red, incluyendo reconocimiento de imágenes y analítica de información de forma centralizada.

- DLP Cloud: ofrece una solución de seguridad para entornos de nube (Cloud Access Security Broker, CASB), incorporando funcionalidades de DLP en aplicaciones SaaS como Office 365, Gmail, BOX y otras.

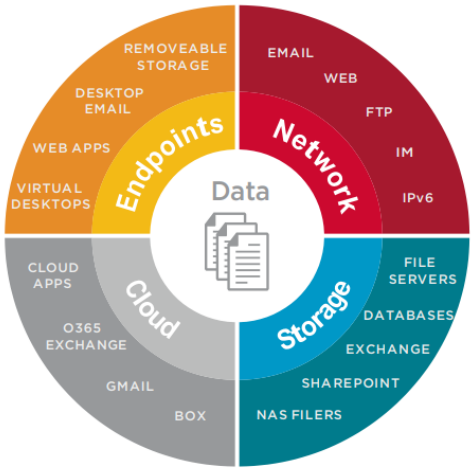


Imagen 3. Symantec DLP. Bloques de protección (Symantec, 2022)

Posee integración con los principales navegadores (Chrome, Firefox, Safari, Edge), y con los sistemas operativos de tipo cliente y servidor más utilizados en la industria (Windows, macOS, Linux).

Protege la información en tránsito y en reposo, y cumple con todos los requisitos técnicos relacionados con bloqueo de dispositivos e impresión, análisis de ficheros enviados por correo electrónico, clasificación de información, etc.

Finalmente, cabe destacar su gran potencia analizando la información para su clasificación y protección, utilizando técnicas como la detección de patrones, indexado, reconocimiento de imágenes o inteligencia artificial y la gestión centralizada desde una única consola.

Imagen 4. Mecanismos de detección de contenido (Symantec, 2022)

Ventajas:

- Protección en múltiples canales: dispositivos finales, web, correo, almacenamiento, cloud.
- Consola unificada para gestión de políticas, respuesta a incidentes, informes y administración.
- Amplio rango de integraciones:
    - Security Access Service Edge (SASE) del propio fabricante
    - Microsoft Information Protection para clasificación de datos, encriptación, y gestión de permisos.

Desventajas:

- Coste muy elevado para una PYME.
- Symantec se escindió de Veritas en 2015 y fue adquirida por Broadcom en 2019 Algunos clientes temen que la compañía disminuya la calidad de sus servicios de soporte y la innovación. (Computer World, 2022).

2.3.2. Digital Guardian DLP

Digital Guardian es una empresa estadounidense que fue fundada en 2003. Su solución DLP se despliega y gestiona en la nube bajo modalidad SaaS, se caracteriza por ser multiplataforma (Windows, macOS y Linux) y por la definición de controles flexibles que eviten el compromiso y la exfiltración de datos antes de que estos se produzcan. En sus inicios funcionaba únicamente como un Endpoint DLP, pero desde 2015 y gracias a la adquisición de Core Green Networks (CGN) ofrece también una línea de producto basada en Network DLP.

Digital Guardian propone cuatro requisitos para conseguir con éxito la protección de los datos:

- Visibilidad de todos los datos, todo el tiempo.
- Analítica de datos para entender y gestionar el riesgo.
- Controles para forzar las políticas de protección de datos.
- Vista consolidada de todas las amenazas a datos sensibles.

Esto lo logra mediante su agente y los sensores que envían información a la consola centralizada en la infraestructura interna de la organización, que a su vez se redirige a un sistema de gestión de seguridad en la nube, donde se analizan las amenazas y datos

existentes, se generan informes, o se pueden gestionar casos. Su arquitectura se muestra en la siguiente imagen:

Imagen 5. Arquitectura DLP de Digital Guardian (Digital Guardian, 2020)

Ventajas:

- Un único agente cubre las características de Endpoint DLP, pero también ofrece protección ante amenazas y características de Endpoint Detection and Response (EDR)
- Capacidades avanzadas de protección mediante el uso del appliance de Network DLP.
- Gestión centralizada en la consola SaaS alojada en la nube, que ofrece funcionalidades adicionales a las propias de DLP.

Desventajas:

- No ha sido posible conseguir una licencia de evaluación, a pesar de que inicialmente sí se obtuvo respuesta por parte de su departamento comercial.
- Algunos clientes indican que el agente tiene problemas de estabilidad y rendimiento.

2.3.3. McAfee DLP

McAfee es una empresa estadounidense que fue fundada 1987 por el excéntrico John McAfee, uno de los primeros desarrolladores de software antivirus de la industria.

McAfee DLP es una suite de múltiples herramientas (Discover, Prevent, Endpoint y Monitor) que ofrecen protección ante fugas y robo de información. La solución de McAfee pone un mayor foco que sus competidores en la realización de análisis forenses sobre los eventos ocurridos en la organización, y permite extender las políticas de seguridad definidas en la infraestructura de los clientes a la nube.

Su funcionamiento en los entornos privados se basa la utilización de un agente que recopilan datos acerca de ubicación de información sensible, envían información acerca de los eventos realizados por los usuarios al sistema centralizado, y fuerza las políticas de seguridad definidas. Destacan las siguientes características (McAfee, 2020):

- Utilización de etiquetas de Microsoft Azure Information Protection (AIP) para los datos en movimiento. Estas etiquetas permiten clasificar los datos según su grado de confidencialidad, de manera que se puedan establecer políticas de control y visibilidad sobre ellos.
- Integración con análisis de comportamiento de usuarios (UEBA) de terceros para detectar amenazas de seguridad internas.
- Permite al usuario realizar análisis e iniciar reparaciones, aprovechando esto para descubrir mayor información en los dispositivos cliente.
- Clasificación de información flexible mediante diccionarios, algoritmos de validación, documentos registrados.
- Tecnología de etiquetado para clasificación de documentos según su origen.

Ventajas:

- Protección extremo a extremo, desde el dispositivo, hasta el Cloud, gracias a la suite de productos diferentes que se integran para garantizar la protección.
- Capacidades avanzadas de protección mediante fingerprinting, clasificación, etiquetado de ficheros y técnicas de análisis para datos no estructurados.
- Gestión centralizada en la consola McAfee MVISION ePolicy Orchestrator.

Desventajas:

- No ha sido posible conseguir una licencia de evaluación, y los costes de la solución no son públicos.
- No dispone de agente para equipos Linux/Unix.
- Complejidad de instalación y administración superior a otras tecnologías DLP.

2.3.4. CoSoSys Endpoint Protector

CoSoSys es una empresa fundada en 2004 y cuyos servicios centrales se ubican en Rumanía. Su producto principal es Endpoint Protector, una solución DLP basada en agente que pretende poner fin a los problemas de fuga y robo de datos, asegurando el cumplimiento con las regulaciones de protección de datos existentes.

Es compatible con sistemas operativos Windows, Linux y macOS, e integra controles específicos para regulaciones como HIPAA, RGPD, CCPA, PCI DSS u otras.

Sus principales características son (CoSoSys, s.f.):

- Control de dispositivos. Permite bloquear, controlar y monitorizar los puertos USB y periféricos para impedir el robo de información.
- Protección basada en contenido. Permite monitorizar y controlar los datos en tránsito, pudiendo establecer políticas que definan qué archivos confidenciales pueden salir o no de la empresa, clasificándolos por tipo de archivo, aplicación, contenido predefinido o personalizado, o expresiones regulares.
- Cifrado forzado. Permite asegurar de forma automática los datos copiados a dispositivos extraíbles con encriptación AES 256 bits, protegidos por contraseña.
- Descubrimiento de datos. Permite escanear los datos en reposo en equipos dentro de la red corporativa para aplicar acciones de remediación como cifrar o borrar en caso de que se identifiquen datos confidenciales en equipos no autorizados.

Ventajas:

- Multiplataforma: disponible para sistemas operativos Windows, Linux, y MAC.
- Sencillez de despliegue y administración.
- Puede cubrir algunas funcionalidades en dispositivos móviles.

Desventajas:

- Solución no tan completa como otras tecnologías DLP.
- No cubre escenarios en nube (CASB).

2.4. Selección de tecnología DLP a implementar

Tras evaluar las características de los principales fabricantes, obtenemos la siguiente tabla comparativa de características técnicas:

Característica \ Producto	Symantec DLP	Digital Guardian DLP	McAfee DLP	Endpoint Protector
Servidor físico/virtual	Sí	No	Sí	Sí
Servidor en Cloud	Sí	Sí	Sí	Sí
Agentes para dispositivos Windows	Sí	Sí	Sí	Sí
Agentes para dispositivos MAC	Sí	Sí	Sí	Sí
Agentes para dispositivos Linux	Sí	Sí	No	Sí
Control de dispositivos	Sí	Sí	Sí	Sí
Reglas de protección (web, email, portapapeles, impresión)	Sí	Sí	Sí	Sí
Protección de ficheros y medios extraíbles	Sí	Sí	Sí	Sí
Etiquetado de ubicaciones y aplicaciones	Sí	Sí	Sí	Sí
Consola para usuario final	Sí	No	Sí	No
Acceso basado en roles (RBAC)	Sí	Sí	Sí	Sí
Soporte para diferentes navegadores	Sí	Sí	Sí	Sí
Reglas para proveedores Cloud	Sí	Sí	Sí	No
Múltiples formas de clasificación	Sí	Sí	Sí	Sí
File Shadowing[1]	Sí	Sí	Sí	Sí
Descubrimiento automático	Sí	Sí	Sí	Sí
Modo oculto al usuario	Sí	Sí	Sí	Sí
Ofrece Network DLP	Sí	Sí	Sí	No

Tabla 3. Características técnicas de las soluciones DLP (Elaboración propia)

Gartner (2017) publicó además la siguiente clasificación de herramientas DLP para PPI:

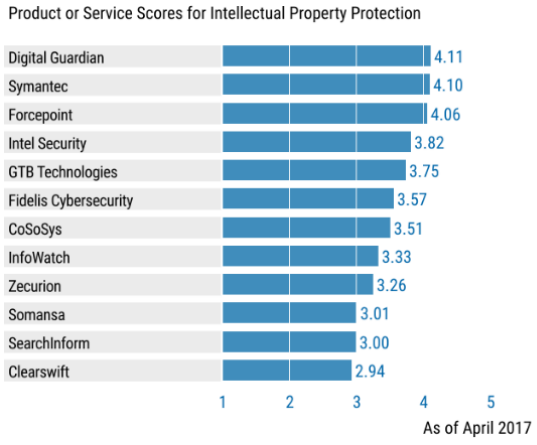


Imagen 6. Clasificación de herramientas DLP para Protección de Propiedad Intelectual (Gartner, 2017)

[1] File Shadowing es una característica que permite al servidor de DLP almacenar una copia de un fichero transferido al exterior por un usuario a través de un dispositivo extraíble, almacenamiento en nube o correo.

Se ha seleccionado Endpoint Protector de CoSoSys para la implementación del proyecto por los siguientes motivos:

- Cumple con todos los requisitos técnicos:
    - Bloqueo y autorización de dispositivos extraíbles.
    - Bloqueo y autorización de contenido a través de aplicaciones (web, cloud, correo electrónico…)
    - Bloqueo de impresión de ficheros.
    - Encriptación de unidades extraíbles.
    - Trazabilidad de las acciones realizadas por los trabajadores con la información corporativa.
- Su instalación es sencilla y no es necesario un gran conocimiento técnico para su despliegue y administración.
- Permite evaluar la solución durante un periodo de prueba de 30 días sin compromiso de adquisición de licencias.
- El coste de la solución es asumible por una empresa mediana.
- Su desventaja principal es que no ofrece características de Cloud/Network DLP, como sí lo hacen sus competidores, pero para este proyecto se puede prescindir de estas características.

3. Marco aplicado

Para desplegar la solución DLP de CoSoSys, el fabricante recomienda seguir los siguientes pasos (CoSoSys, s.f.).

1. Elegir el tipo de implementación. El servidor de Endpoint Protector se puede desplegar en formato máquina virtual, dentro de la infraestructura de servidores del propio cliente, o como servicio Cloud en los principales hiperescalares (Amazon AWS, Microsoft Azure, Google Cloud Platform).
2. Importar las licencias de uso. El fabricante proporciona una licencia de evaluación de 30 días para evaluar su software.
3. Comunicar a todos los empleados que utilicen algún dispositivo que vaya a formar parte del entorno protegido por la solución DLP la implantación de esta solución, detallando los controles definidos. Se debe alinear con las políticas de seguridad corporativa, donde se considere el uso de los dispositivos y la privacidad de los trabajadores.

4. Desplegar el software cliente en los equipos (servidores u ordenadores personales de usuario), que van a ser protegido contra la filtración y el robo de datos.
5. Configurar las políticas de control de dispositivos (Device Control Policies), que nos permiten definir quién tiene acceso a qué dispositivos. Inicialmente, se pueden establecer políticas globales que apliquen a todos los dispositivos, para posteriormente personalizar en base a grupos, equipos y usuarios.
6. Activar las características de File Tracing y File Shadowing, de manera que si se envían ficheros al exterior el servidor almacena una copia de estos y un registro de qué usuario realizó esa acción, de forma que se pueda saber quién lo hizo y qué copió exactamente.
7. Definir los datos sensibles. Esto se debe realizar de manera conjunta con la Gerencia, de manera que se tenga un listado de información a proteger y su tipo: información personal, números de seguridad social, números de tarjeta de crédito, y tipos de fichero y palabras clave a proteger.
8. Configurar las políticas de protección basadas en contenido (Content Aware Protection Policies)
9. Configurar las políticas de sombreado de ficheros basadas en contenido (Content Aware File Shadowing). Se define en qué aplicaciones y para qué tipos de contenido se activa esta característica que se activó previamente en el paso 6.
10. Dejar funcionar las políticas en modo solo reporte durante quince o veinte días, de manera que se puedan analizar los datos obtenidos y decidir qué dispositivos se quieren bloquear, para qué usuarios se quieren establecer políticas más restrictivas, qué grupos de usuarios presentan más amenazas, etc.
11. Realizar el ajuste granular de las políticas de protección basadas en contenido (Content Aware Protection Policies). Una vez definidas las políticas básicas, se pueden realizar ajustes más granulares para determinados grupos, usuarios o equipos: deshabilitar el portapapeles, la impresión de pantalla, el escaneo de dispositivos de red, crear listas blancas de URLs, o bloquear algunas impresoras que no nos interesen.

3.1. Instalación de herramienta DLP

La última versión disponible de Endpoint Protector (EPP) es la 5.6.0. Para el presente proyecto, la herramienta se ha instalado como máquina virtual con Oracle VM

VirtualBox. A continuación se realiza la configuración inicial del servidor, tal y como se detalla en el Anexo I.

La arquitectura de laboratorio desplegada es la siguiente:

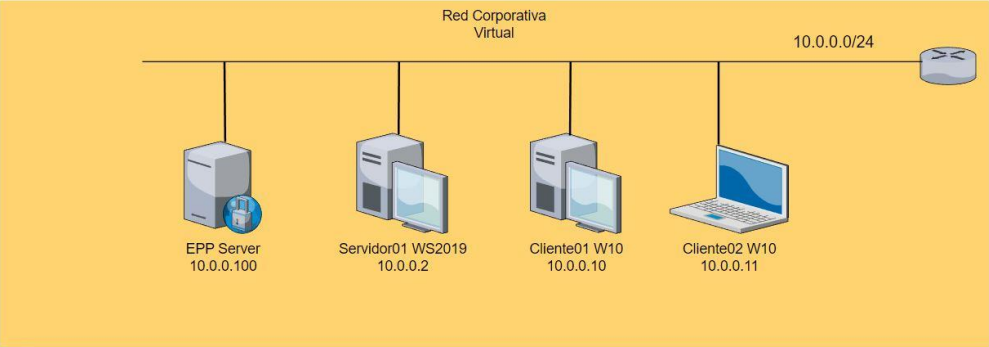


Imagen 7. Arquitectura de red del laboratorio DLP (Elaboración propia)

Una vez hemos desplegado el servidor de EPP, este está accesible vía web para su gestión a través de la dirección ip que le hemos configurado. En nuestro accedemos a https.//epp.aclog.int, ya que hemos creado el alias epp y utilizaremos el dominio aclog.int.

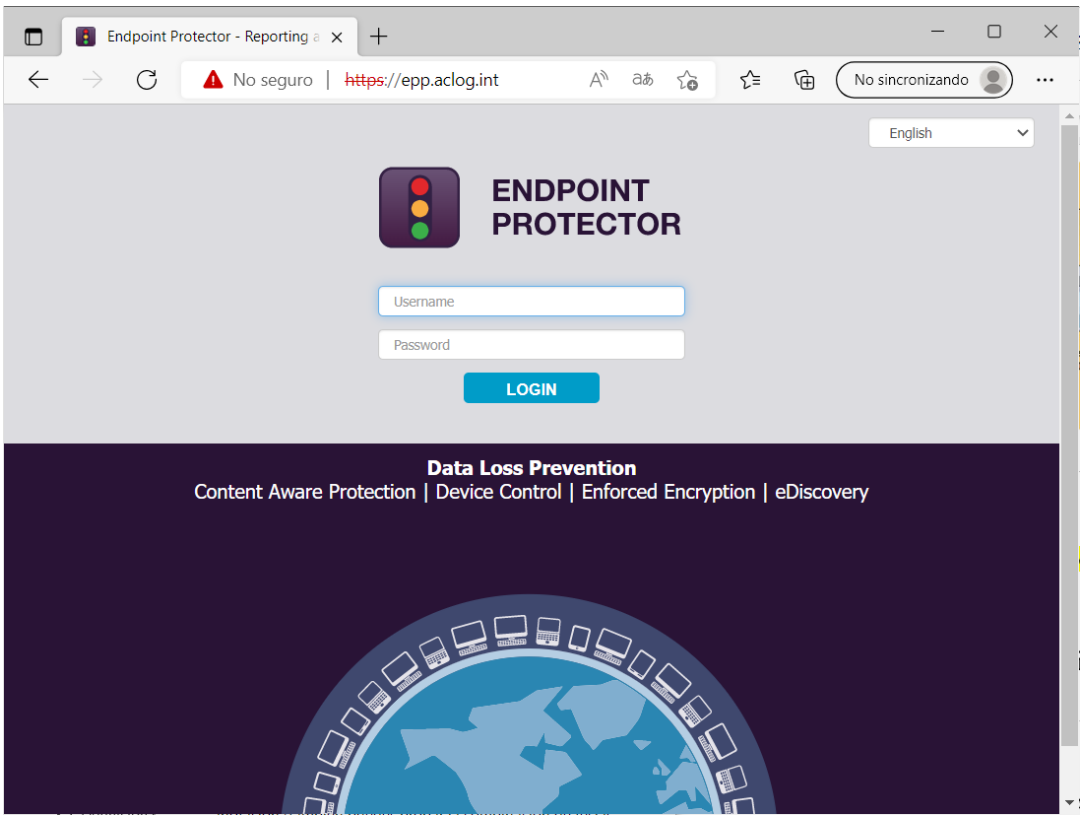


Imagen 8. Pantalla de login de Endpoint Protector (CoSoSys)

El agente de EPP se descarga del propio portal, en la sección System Configuration > Client Software, tal y como se detalla en el Anexo II. Se incluyen de forma opcional los

add-in de Outlook, Internet Explorer y Lotus Notes. La comunicación del agente y el servidor se realiza a través del puerto 443.

Una vez instalado el primer agente, este se muestra en la consola de EPP:

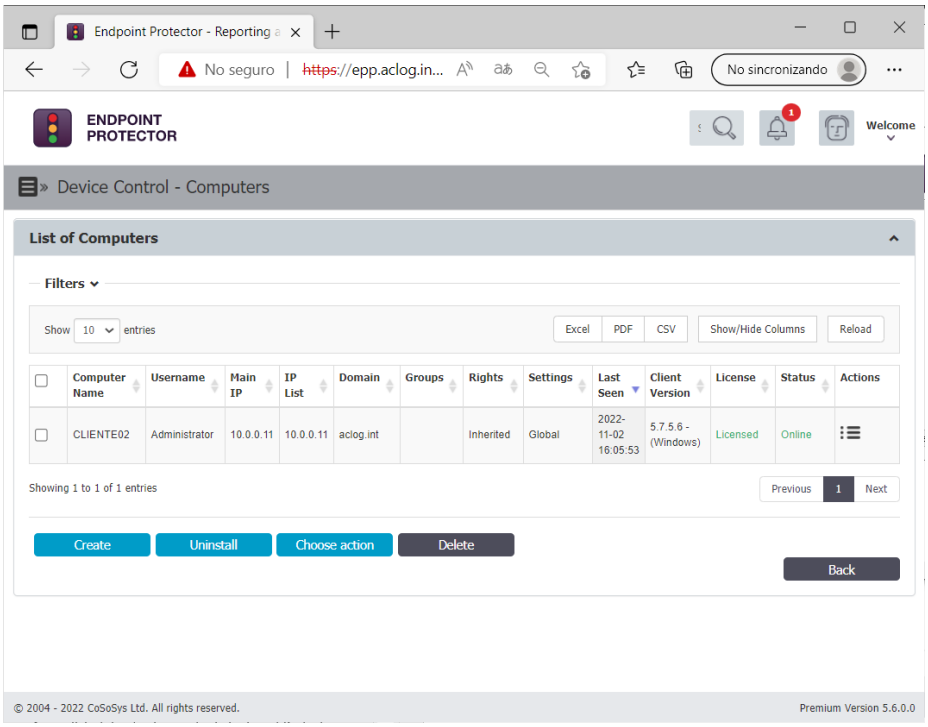


Imagen 9. Listado de equipos en EPP tras instalación del agente (CoSoSys)

Se realiza la instalación del agente en el resto de los equipos del laboratorio (WS2019 y Cliente01) siguiendo el mismo procedimiento.

3.2. Definición de controles de seguridad

Se han dividido los controles a implementar en cuatro bloques que coinciden con las principales funcionalidades de EPP:

1. Control de dispositivos (CD). Establecen políticas de control y limitaciones relacionadas con el uso de dispositivos USB.
2. Cifrado forzado (CF). Establecen controles de cifrado de dispositivos extraíbles.
3. Protección basada en contenido (PBC). Establecen controles y acciones a realizar basándose en los tipos de archivo, listas, y normativas aplicables a contenido.
4. eDiscovery (ED). Establecen las acciones de respuesta cuando se realicen escaneos de descubrimiento en los dispositivos bajo la supervisión de EPP.

A cada uno de los controles se le ha asignado un identificador único para poder referirnos a él a lo largo del proyecto.

3.2.1.Control de dispositivos

Las políticas de Control de dispositivos permiten al administrador permitir o denegar el acceso a USBs extraíbles, establecer alertas por uso, copiar los ficheros que se transfieren para su posterior revisión o limitar la transferencia en aplicaciones en línea. Por regla general, estas políticas de control se pueden asociar a grupos de usuarios o equipos.

Se definen los siguientes controles, de los cuales se evaluará un subconjunto en el apartado de casos de uso:

ID	Bloque	Control	Descripción
CD.1	Control de dispositivos	Permisos granulares	Configurar limitaciones de dispositivos USB de forma global
CD.2	Control de dispositivos	Permisos granulares	Configurar limitaciones de dispositivos USB por equipo
CD.3	Control de dispositivos	Permisos granulares	Configurar limitaciones de dispositivos USB por usuario
CD.4	Control de dispositivos	Permisos granulares	Configurar limitaciones de dispositivos USB por grupo
CD.5	Control de dispositivos	Permisos por dispositivo	Establecer permisos de denegación, permitir, o solo lectura a dispositivos específicos. (Basado en nº serie)
CD.6	Control de dispositivos	Clases personalizadas	Aplicar permisos a dispositivo basados en el ID del fabricante y/o ID de producto
CD.7	Control de dispositivos	Políticas fuera de horario laboral	Establecer reglas de horario y calendario para el uso de dispositivos
CD.8	Control de dispositivos	Políticas fuera de la red	Establecer políticas que se apliquen a equipos que acceden a los recursos desde fuera de la red de la empresa
CD.9	Control de dispositivos	File tracing	Registrar los intentos o transferencias de datos a dispositivos de almacenamiento USB
CD.10	Control de dispositivos	File shadowing	Crear instantáneas de archivos transferidos a dispositivos para auditorías detalladas
CD.11	Control de dispositivos	Contraseña temporal offline	Permitir el acceso temporal a los dispositivos de los equipos fuera de la red local mediante contraseña
CD.12	Control de dispositivos	Alertas por correo electrónico	Recibir alertas por correo en tiempo real para eventos relacionados con el uso de medios extraíbles
CD.13	Control de dispositivos	Panel de control y gráficos	Revisar los gráficos y tablas que ofrece la solución para obtener una visión general de los eventos más importantes
CD.14	Control de dispositivos	Informes y análisis	Monitorizar la actividad relacionada con la transferencia de archivos
CD.15	Control de dispositivos	Límite de transferencia	Establecer límites en el número de archivos o el tamaño que se puede transferir dentro de un intervalo de tiempo
CD.16	Control de dispositivos	Límite de transferencia	Incluir o excluir las transferencias por dispositivos
CD.17	Control de dispositivos	Límite de transferencia	Limitar la transferencia de ficheros en aplicaciones online

Tabla 4. Listado de controles de dispositivos (Elaboración propia)

3.2.2.Cifrado forzado

Las políticas de Cifrado forzado permiten el cifrado de dispositivos USB, de manera que sea seguro transportarlos sin miedo a una exfiltración de información en caso de robo o pérdida. EPP se apoya en la herramienta EasyLock para realizar el cifrado de los dispositivos, y tiene dos modos de funcionamiento:

- EasyLock: mediante una aplicación que no requiere instalación, protege los datos en el almacenamiento USB utilizando encriptación AES CBD de 256 bits.
- EasyLock Enforced Encryption: utiliza también una aplicación que requiere instalación en el equipo que utiliza el USB, pero se diferencia del anterior modo en que permite reconocer los dispositivos como confiables (Trusted Devices). Proporciona funcionalidades más avanzadas como la gestión remota (protección por contraseña, reinicio del dispositivo de almacenamiento USB). Esta característica solo puede ser usada en combinación con EPP.

Se pueden definir los siguientes controles, de los cuales se evaluará un subconjunto en el apartado de casos de uso:

ID	Bloque	Control	Descripción
CF.1	Cifrado forzado	Cifrado forzado de dispositivos USB	Autorizar únicamente el uso de dispositivos USB cifrados para asegurar que todos los datos copiados en estos dispositivos son cifrados
CF.2	Cifrado forzado	Políticas de cifrado	Permitir el acceso de solo lectura o forzar la encriptación del dispositivo si se quiere escribir en él
CF.3	Cifrado forzado	Contraseñas maestras	Establecer la complejidad de las contraseñas de cifrado
CF.4	Cifrado forzado	Gestión de contraseñas	Cambio de las contraseñas de cifrado de usuarios de forma remota
CF.5	Cifrado forzado	Borrado remoto	Borrar los datos de los dispositivos en el caso de que estos se hayan visto comprometidos

Tabla 5. Listado de controles de cifrado forzado (Elaboración propia)

3.2.3.Protección basada en contenido

Las políticas de Protección basada en contenido funcionan de forma similar a como lo hace un antivirus: el agente de EPP examina los ficheros activos para determinar sus propiedades, y realizar acciones en función de estas.

Se pueden definir los siguientes controles, de los cuales se evaluará un subconjunto en el apartado de casos de uso:

ID	Bloque	Control	Descripción
PBC.1	Protección basada en contenido	Lista negra de tipo de archivo	Bloqueo de archivos basados en su extensión real
PBC.2	Protección basada en contenido	Listas negras de contenido predefinido	Crear filtros basados en contenido (Número de tarjetas de crédito y Números de seguridad social, por ejemplo)
PBC.3	Protección basada en contenido	Reconocimiento óptico de caracteres	Inspeccionar el contenido de fotos e imágenes, detectando información confidencial desde documentos escaneados y similares
PBC.4	Protección basada en contenido	Listas negras de nombre de archivo	Crear filtros basados en nombres de archivo para asociar acciones a ellas.
PBC.5	Protección basada en contenido	Listas negras y listas blancas de ubicación de archivo	Crear filtros basados en la ubicación de archivos para asociar acciones a ellas
PBC.6	Protección basada en contenido	Fuera de horario	Definir políticas de reserva que van a funcionar fuera de las horas laborales
PBC.7	Protección basada en contenido	Lista blanca de dominio y URL	Proporcionar flexibilidad a los empleados permitiéndoles el acceso a determinadas URLs que sean necesarias para su trabajo
PBC.8	Protección basada en contenido	Monitorización de la captura de pantalla y portapapeles	Desactivar la opción de realizar capturas de pantalla y limitar el uso de las opciones copiar/pegar.
PBC.9	Protección basada en contenido	Remediación del usuario	Ofrecer al usuario anular de forma segura una política DLP justificando transferencias de datos
PBC.10	Protección basada en contenido	Panel de control, informes y análisis	Monitorizar la actividad relacionada con las políticas de protección basadas en contenido. Generar informes.
PBC.11	Protección basada en contenido	Cumplimiento (RGPD, HIPAA, PCI DSS)	Cumplir con las normativas legales que apliquen
PBC.12	Protección basada en contenido	DLP para impresoras	Configurar políticas para limitar el uso de impresoras locales y en red

Tabla 6. Listado de controles de protección basada en contenido (Elaboración propia)

3.2.4.eDiscovery

Las políticas de eDiscovery permiten definir controles que inspeccionen datos almacenados en los equipos protegidos (Windows, macOS o Linux). Esto nos permite aplicar la política de protección de datos de una organización, y gestionar los riesgos que plantean los datos en reposo al descubrir información confidencial donde no debería estar almacenada: datos personales, información financiera o de tarjetas, o ficheros confidenciales.

Se pueden definir los siguientes controles, de los cuales se evaluará un subconjunto en el apartado de casos de uso:

ID	Bloque	Control	Descripción
ED.1	eDiscovery	Cifrar y descifrar datos	Cifrado de datos en reposo que contengan información confidencial
ED.2	eDiscovery	Eliminar datos	Eliminar datos que supongan una violación de la política de seguridad en dispositivos finales
ED.3	eDiscovery	Listas negras de ubicación de escaneo	Escanear rutas predefinidas como base, evitando el escaneo redundante de datos en reposo
ED.4	eDiscovery	Escaneos automáticos	Planificar escaneos automáticos periódicos
ED.5	eDiscovery	Resultados del escaneo	Ejecutar acciones tras escaneo. Remediar y exportar eventos a un SIEM
ED.6	eDiscovery	Límites para filtros	Limitar el número de violaciones que puede tener un archivo para que se aplique la política de seguridad y se notifique al servidor
ED.7	eDiscovery	Listas negras de tipo de archivo	Bloquear documentos basándose en el tipo real del archivo
ED.8	eDiscovery	Listas blancas de archivos permitidos	Excluir determinados archivos del escaneo para mejorar la productividad y rendimiento de la herramienta
ED.9	eDiscovery	Listas blancas por tipo MIME	Excluir determinados archivos según su tipo MIME del escaneo para mejorar la productividad y rendimiento de la herramienta

Tabla 7. Listado de controles eDiscovery (Elaboración propia)

3.3. Casos de uso implementados

Se han desplegado los siguientes usuarios en el entorno de laboratorio para la realización de las pruebas:

ID	Nombre	Grupo	Descripción
Gerente01	Gerente01 Garcia	Gerentes	Usuario de muestra para el perfil de Gerencia
Dentista01	Dentista01 Fernandez	Dentistas	Usuario de muestra para el perfil de Dentistas
Administrativo01	Administrativo01 Lopez	Administrativos	Usuario de muestra para el perfil de Administrativos
Servicio01	Servicio01 Rodríguez	Servicios	Usuario de muestra para el perfil de Servicios

Tabla 8. Listado de usuarios del laboratorio (Elaboración propia)

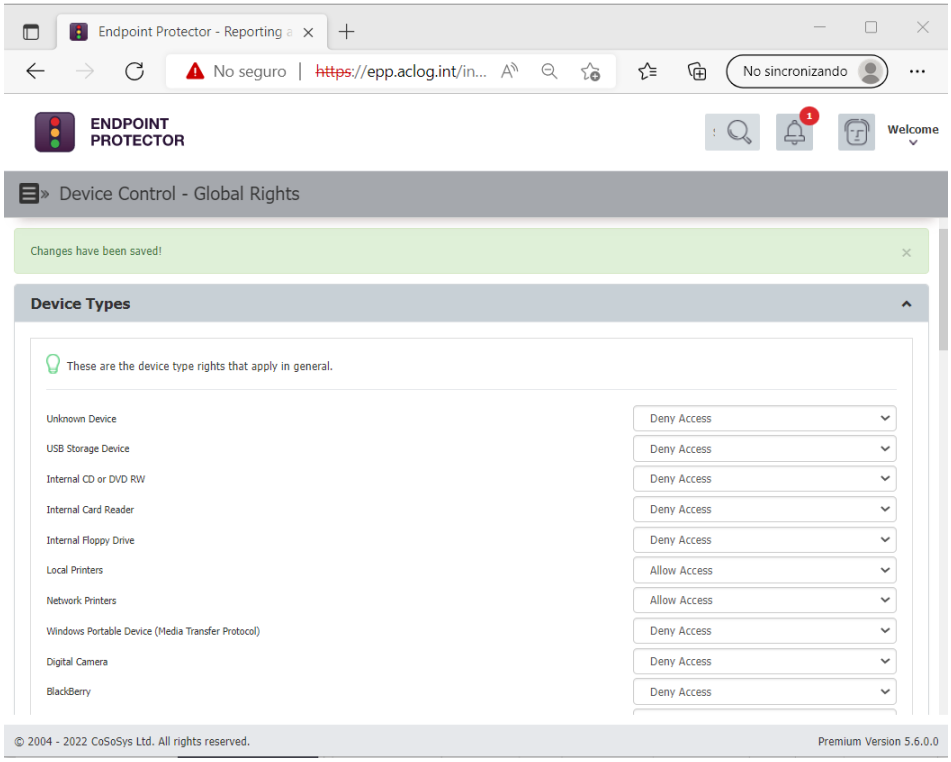
3.3.1.Control de dispositivos

La configuración de limitaciones de dispositivos se puede realizar de forma granular para Dispositivos, Equipos o Usuarios, Grupos, o de forma global. El orden de prioridad aplicado es el siguiente, siendo el primero de más alta prioridad:

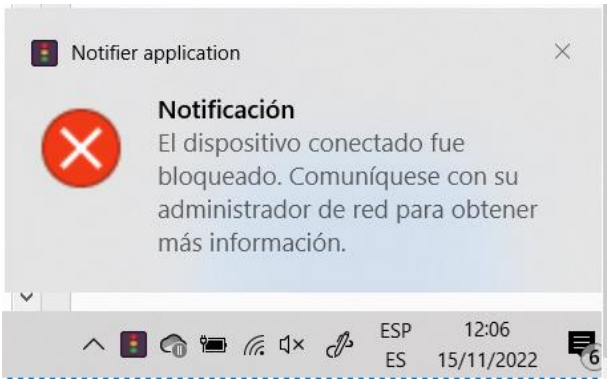
Dispositivos → Equipos → Usuarios → Grupos → Global.

CD.1: Configurar limitaciones de dispositivos USB de forma global

Las políticas globales de permisos de dispositivos se configuran en la sección Device Control > Global Rights. Se limitan a continuación el uso de dispositivos de almacenamiento USB de forma global:

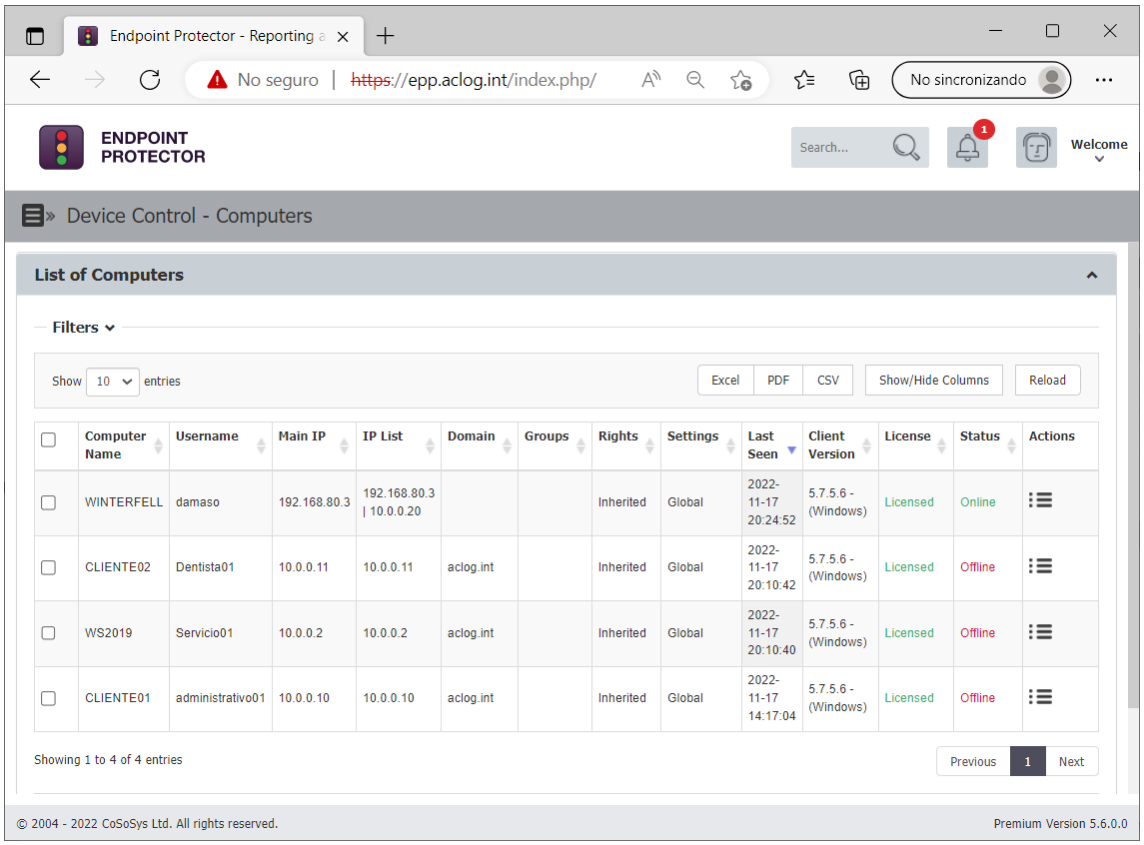


Cuando un dispositivo es bloqueado, aparece la siguiente notificación en la barra de tareas del equipo:

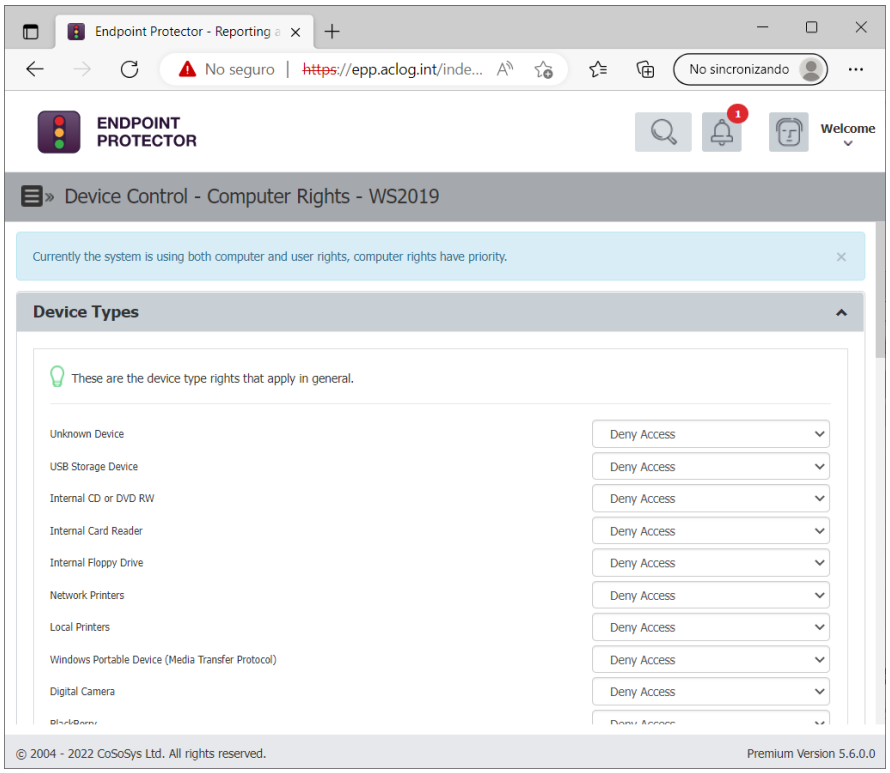


CD.2. Configurar limitaciones de dispositivos USB por equipo

Desde la sección Device Control, Computers, podemos ver el listado de equipos desplegados en EPP.

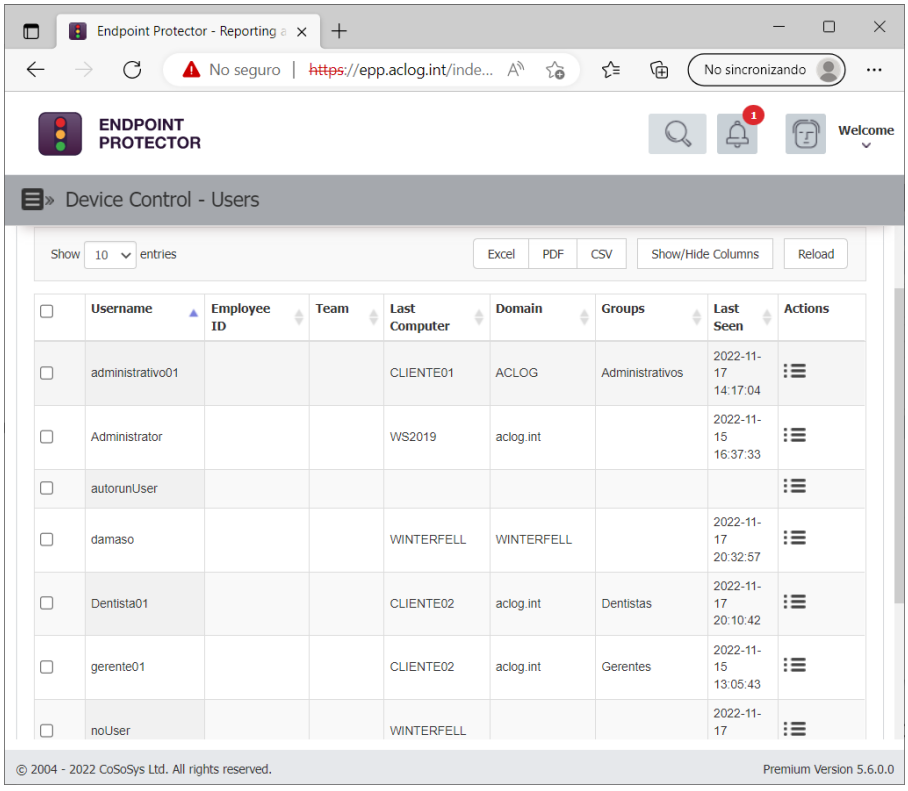


Desde la columna Actions > Manage Rights, podemos seleccionar los permisos que queremos configurar. En este caso de uso, se deniegan todos los dispositivos excepto teclado para el servidor WS2019:

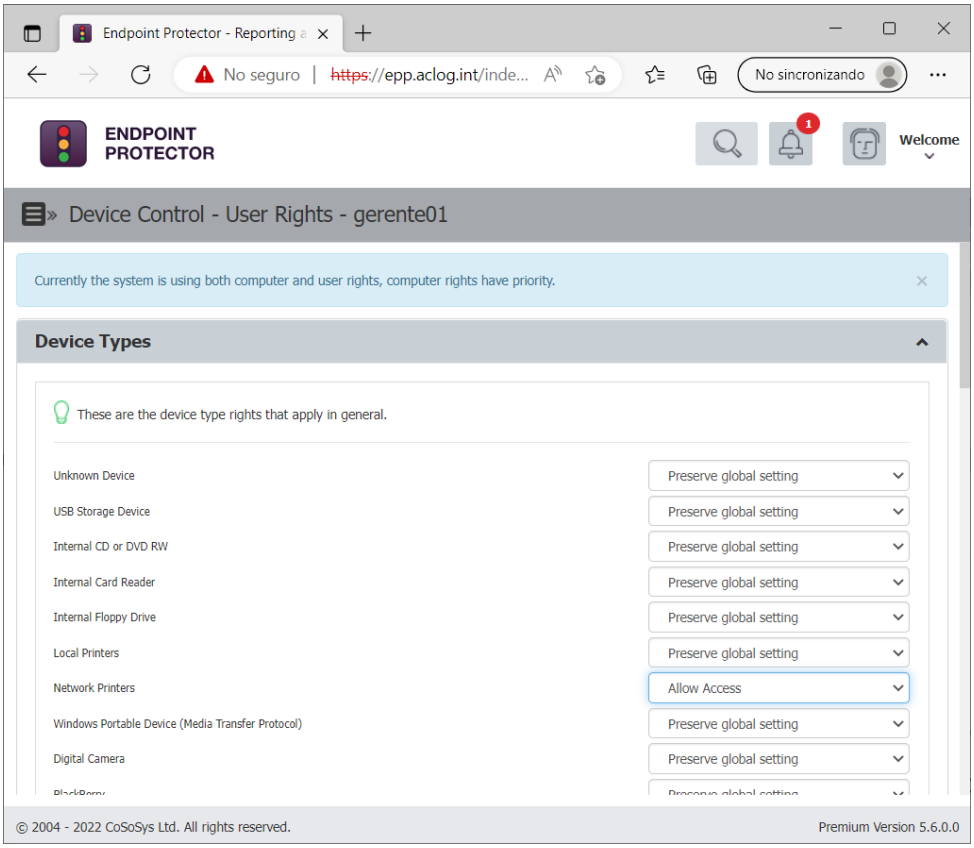


CD.3. Configurar limitaciones de dispositivos USB por usuario

Desde la sección Device Control > Users, podemos ver el listado de usuarios que han iniciado sesión en alguno de los equipos con agente de EPP configurado.

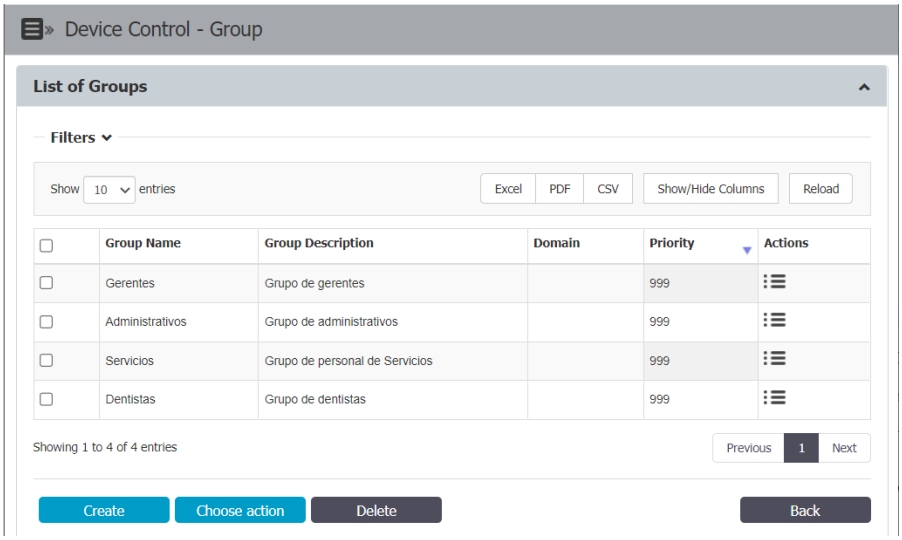


Desde el menú *manage rights* se les puede permitir/denegar de forma individual el uso de dispositivos extraíbles. En este caso, hemos configurado el usuario Gerente01 para que pueda usar impresoras de red:

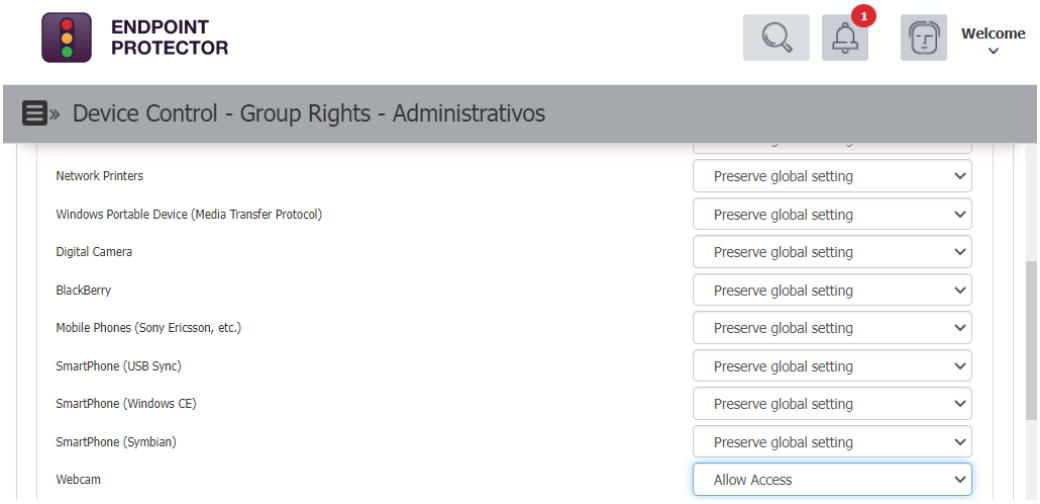


CD.4. Configurar limitaciones de dispositivos USB por grupo

En EPP se pueden crear grupos que contengan equipos, usuarios, o ambos. Para este caso de uso, se ha creado un grupo de EPP para cada uno de los departamentos identificados (Gerentes, Administrativos, Dentistas y Servicios)

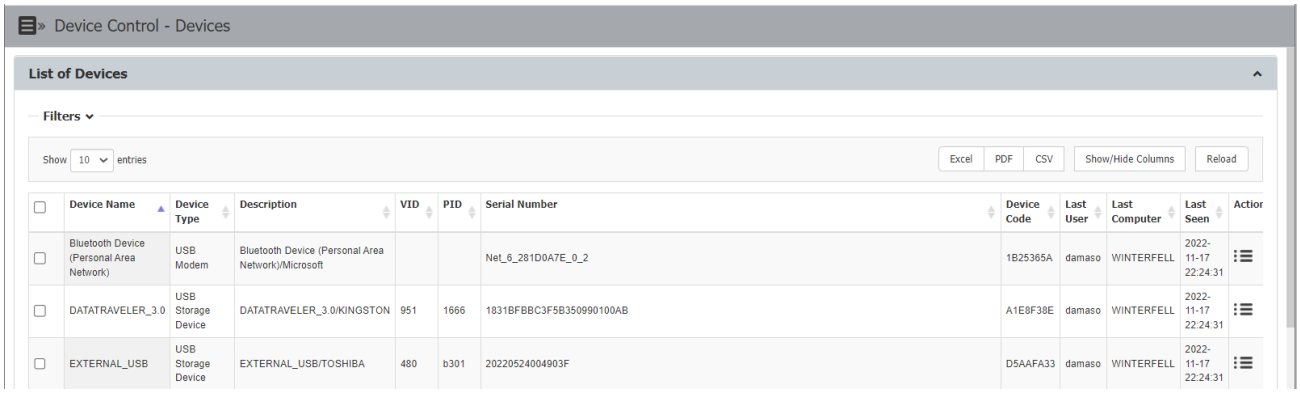


Se va a permitir al grupo de Administrativos el uso de webcam para poder capturar una foto de los pacientes cuando se les realiza la ficha de bienvenida.

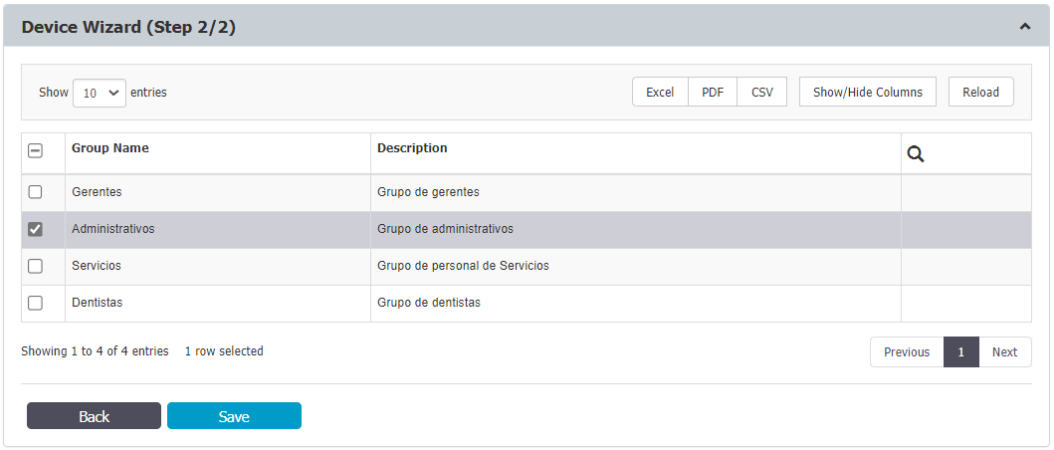


CD.5. Establecer permisos de denegación, permitir, o solo lectura a dispositivos específicos. (Basado en nº serie)

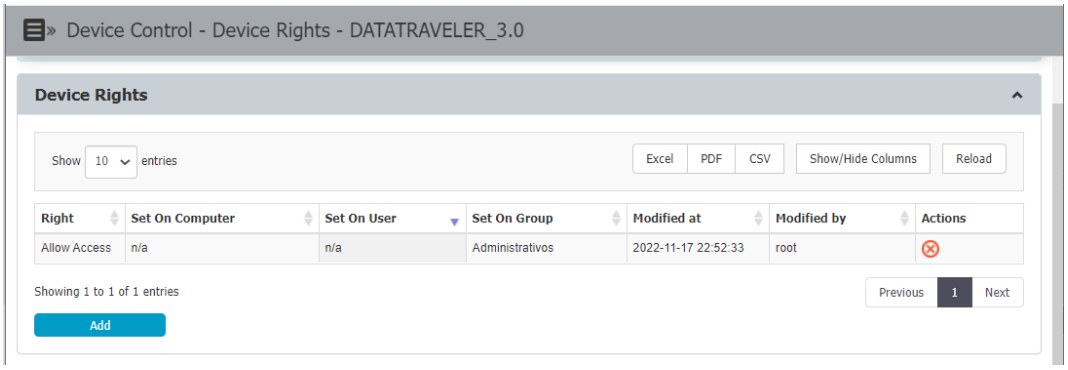
Desde la sección Device Control > Devices podemos listar los dispositivos extraíbles que se han conectado en alguno de los equipos cliente.



Desde el menú Actions podemos definir los permisos para estos dispositivos de forma granular. Como caso de uso, podemos permitir el uso de este dispositivo para el grupo de Administrativos.



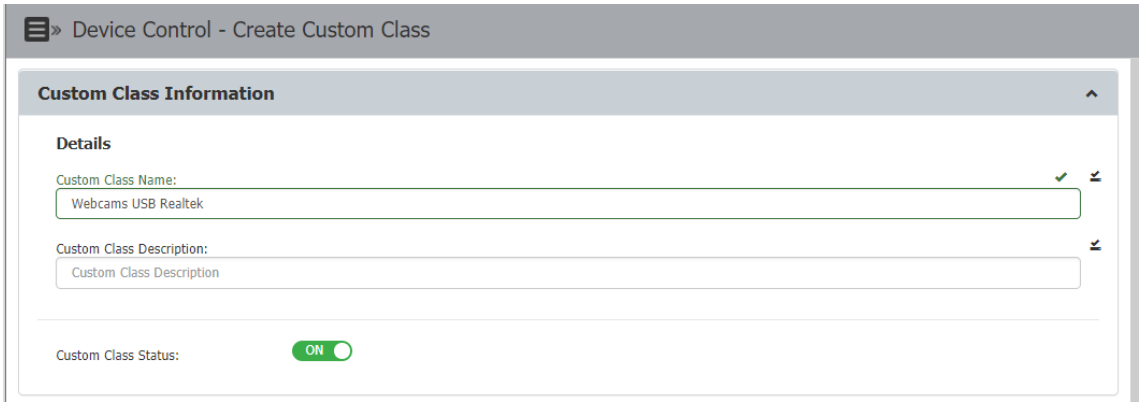
Estos permisos se muestran posteriormente en el resumen del dispositivo:



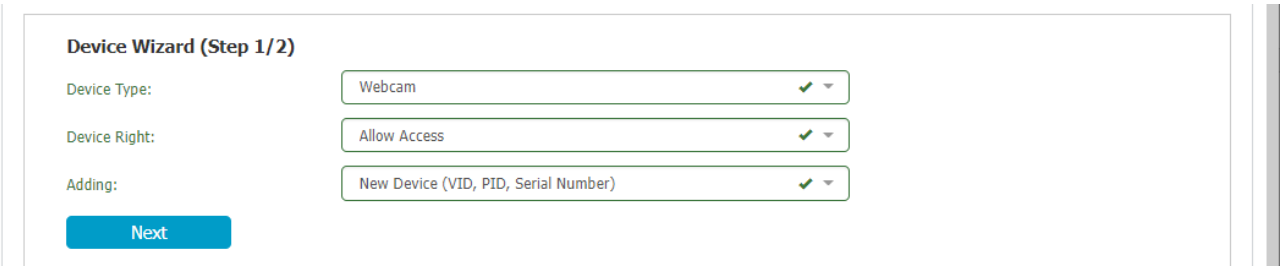
CD.6. Aplicar permisos a dispositivo basados en el ID del fabricante y/o ID de producto

Desde la sección Device Control > Custom Classes, podemos crear nuevas clases que identifiquen productos basándonos en el ID del fabricante (VID) y/o el ID de producto.

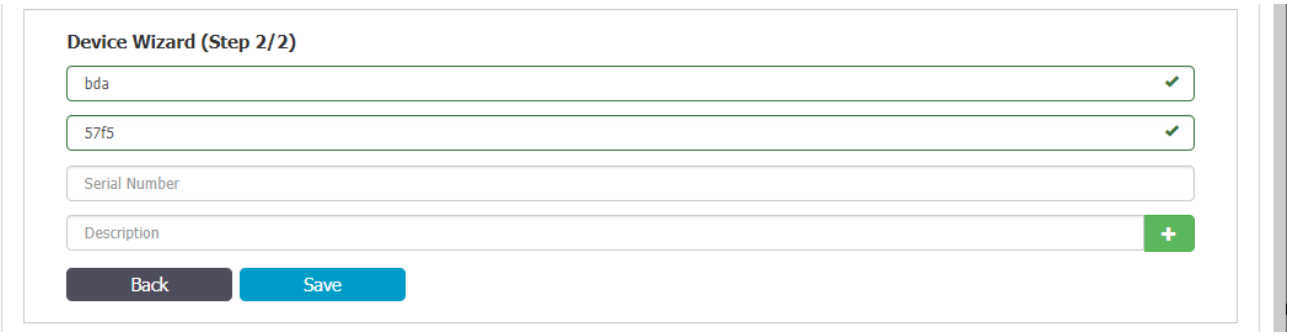
En este caso de uso, creamos una clase que identifique las webcam Realtek USB2.0 HD UVC, que hemos verificado previamente en EPP con VID “bda” y PID “57f5”, para permitir su acceso:



Añadimos ahora el tipo de dispositivo, la acción a realizar (permitir el acceso), y el filtro por el que se va a crear (VID, PID, Serial Number).



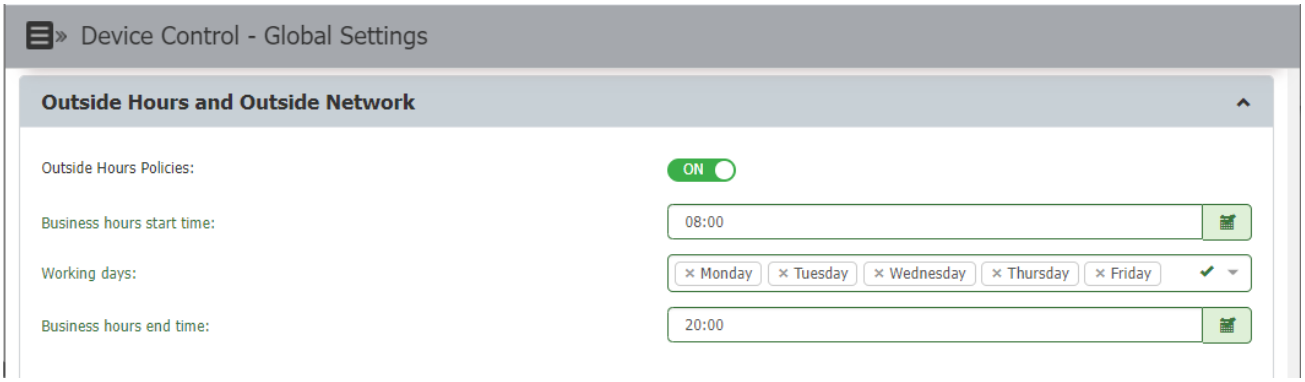
Y finalmente definimos los valores a los que se va a aplicar la clase creada:



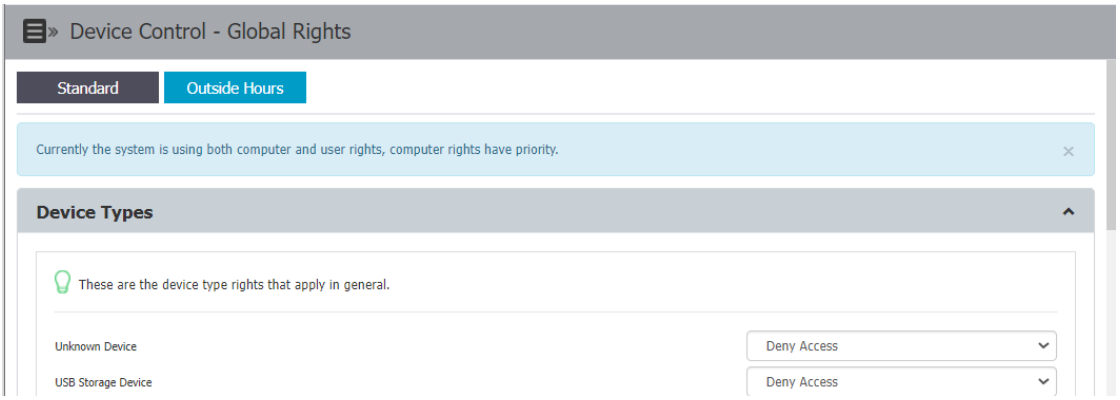
De este modo, cuando este dispositivo se conecte en cualquiera de los clientes, se permitirá su acceso.

CD.7. Establecer reglas de horario y calendario para el uso de dispositivos

En primer lugar habilitamos la política de configuración global que permite definir políticas que restrinjan el horario o el calendario en el uso de dispositivos. Esto se realiza en la sección Device Control > Global Settings, y tenemos que definir los días laborables y el horario de trabajo:



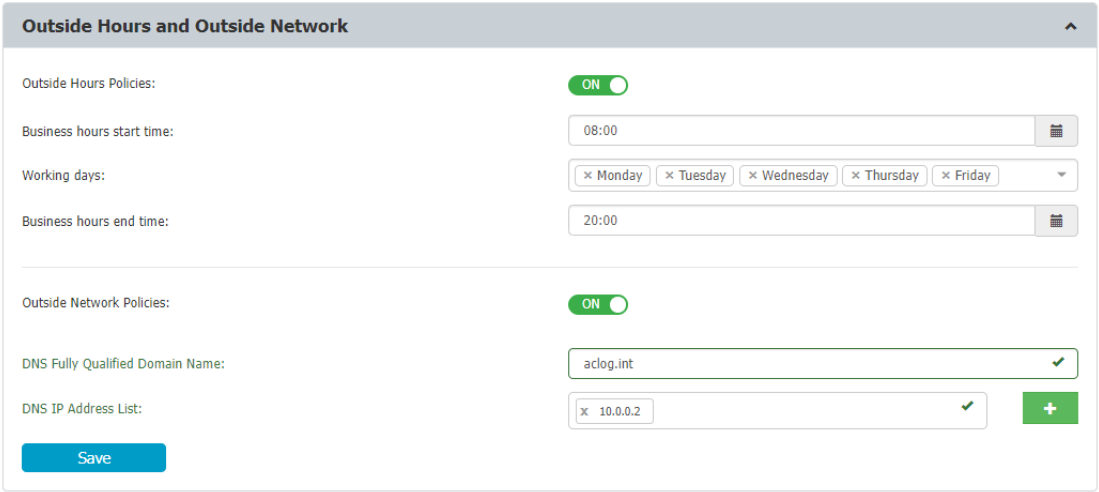
Tras esto, en la sección Device Control > Global Settings se habilita una página adicional para definir permisos globales que apliquen fuera de horario:



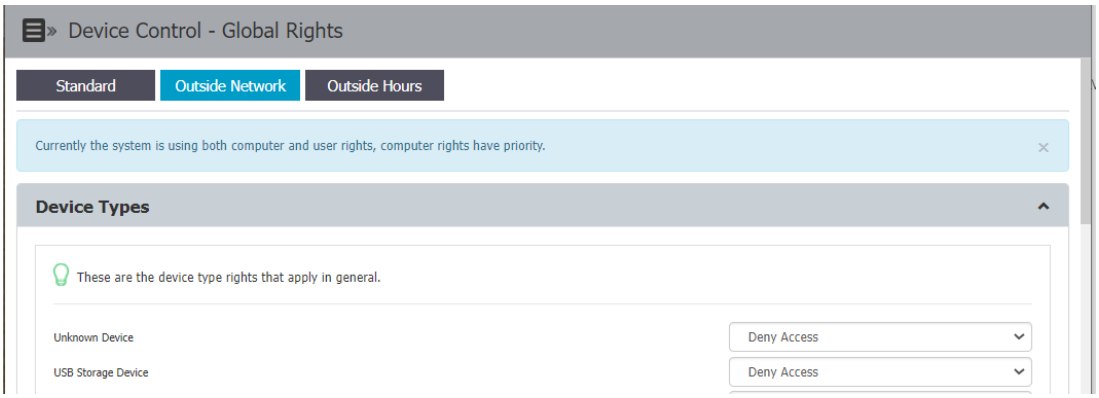
Se pueden aplicar políticas de control fuera de horario para dispositivos específicos. El caso de uso sería el de una intervención periódica programada por parte del departamento de Servicios que necesite la conexión de algún dispositivo concreto.

CD.8. Establecer políticas que se apliquen a equipos que acceden a los recursos desde fuera de la red de la empresa

De manera análoga a las reglas de horario, esta configuración se ha de habilitar en la sección Device Control > Global Settings:



Tras esto, se habilita en la sección Global Rights > Outside Network:

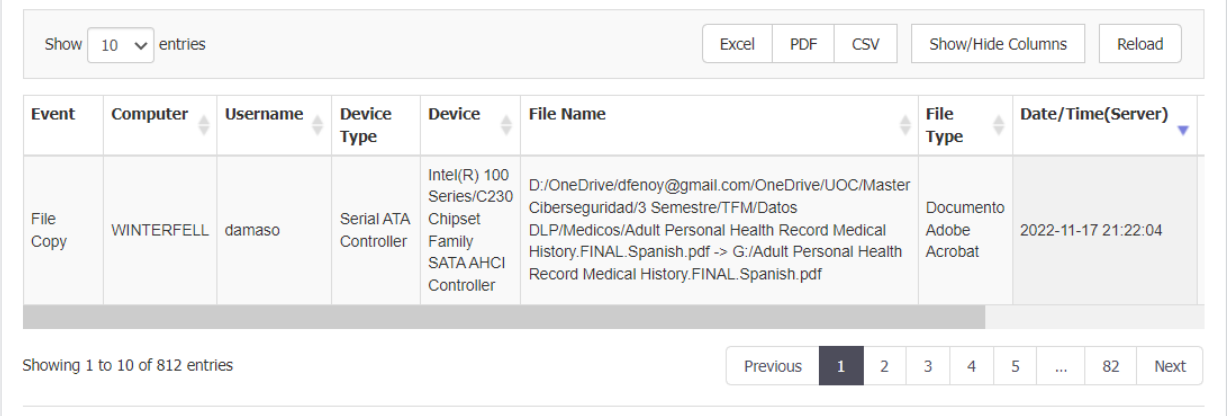


Se pueden dar dos casos de uso para usar este tipo de configuración:

- Denegar el acceso de todos los dispositivos cuando no se encuentren conectados a la red corporativa.
- Permitir el uso de un único dispositivo concreto cuando el agente de EPP no esté conectado al servidor. Por ejemplo, un dentista que realice un viaje con un portátil y necesite conectar un determinado dispositivo.

CD.9. Registrar los intentos o transferencias de datos a dispositivos de almacenamiento USB

Desde la sección Reports and Analysis > File Tracing podemos identificar las transferencias realizadas a dispositivos USB:



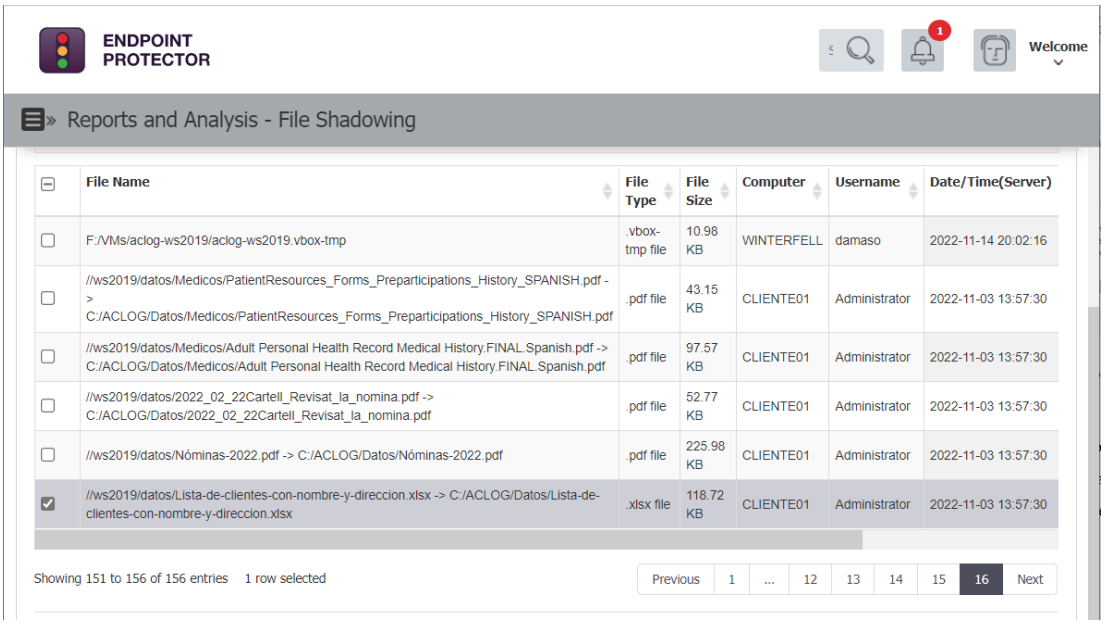
Por ejemplo, podemos ver como el usuario damaso ha realizado la copia de datos a una unidad extraíble en (G:).

CD.10. Crear instantáneas de archivos transferidos a dispositivos para auditorías detalladas

Desde la sección Reports and Analysis > File Shadowing podemos obtener una copia de los ficheros que han transferido los usuarios a dispositivos extraíbles, a unidades

compartidas de red, o a discos internos. Esta copia es almacenada en el servidor tras habilitar la característica de File Shadowing.

En el siguiente ejemplo vemos diversos archivos copiados por el Administrador a la máquina CLIENTE01:

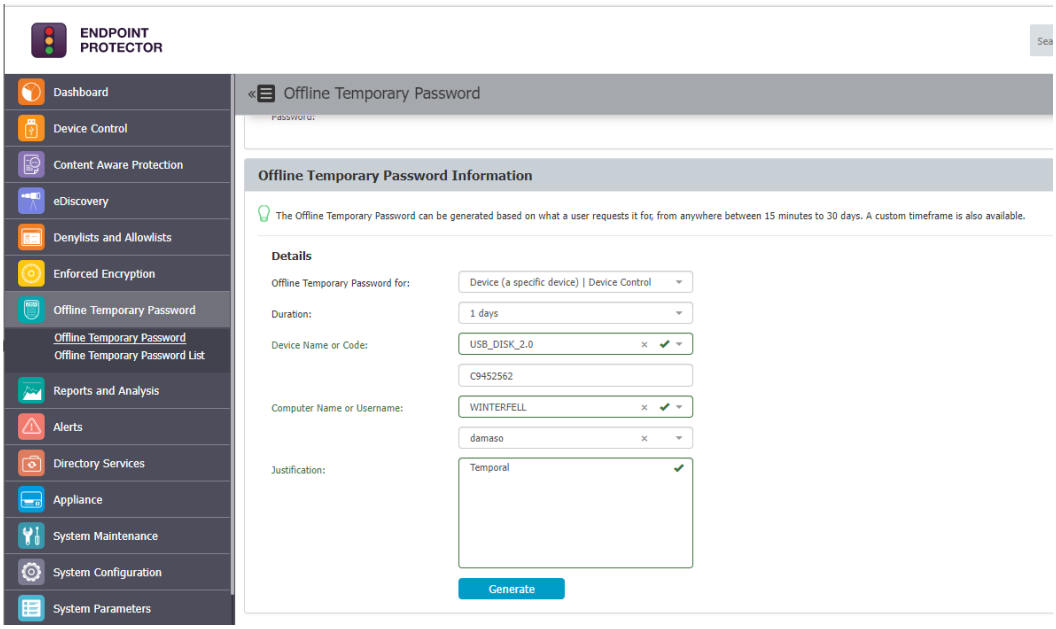


Estos ficheros pueden ser descargados por el Administrador o la persona designada para su revisión. Se pueden ajustar los permisos en EPP para limitar los usuarios que tienen acceso a los ficheros de File Shadowing.

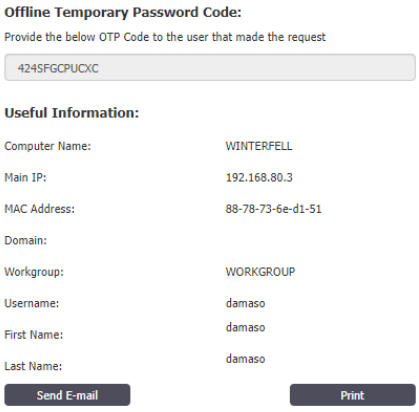
CD.11. Permitir el acceso temporal a los dispositivos de los equipos fuera de la red local mediante contraseña.

Este caso de uso es útil cuando se quiere proporcionar un permiso de acceso temporal a un dispositivo extraíble de un determinado usuario/grupo, o cuando no existe conexión entre el equipo protegido y el servidor de EPP y se quiere permitir el uso de un dispositivo extraíble en él de forma temporal. Para ello, se proporciona al usuario una contraseña temporal que introduce en el agente de EPP de su equipo cliente, permitiendo así el acceso para el que se haya configurado el acceso temporal.

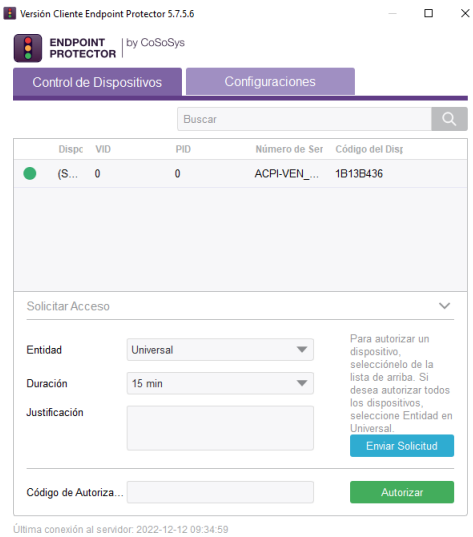
Esta característica se habilita en la sección Offline Temporary Password, seleccionando el dispositivo extraíble, la duración, y el equipo cliente para el que queremos configurar el acceso temporal:



Tras hacer clic en Generate, se obtiene la siguiente contraseña temporal:

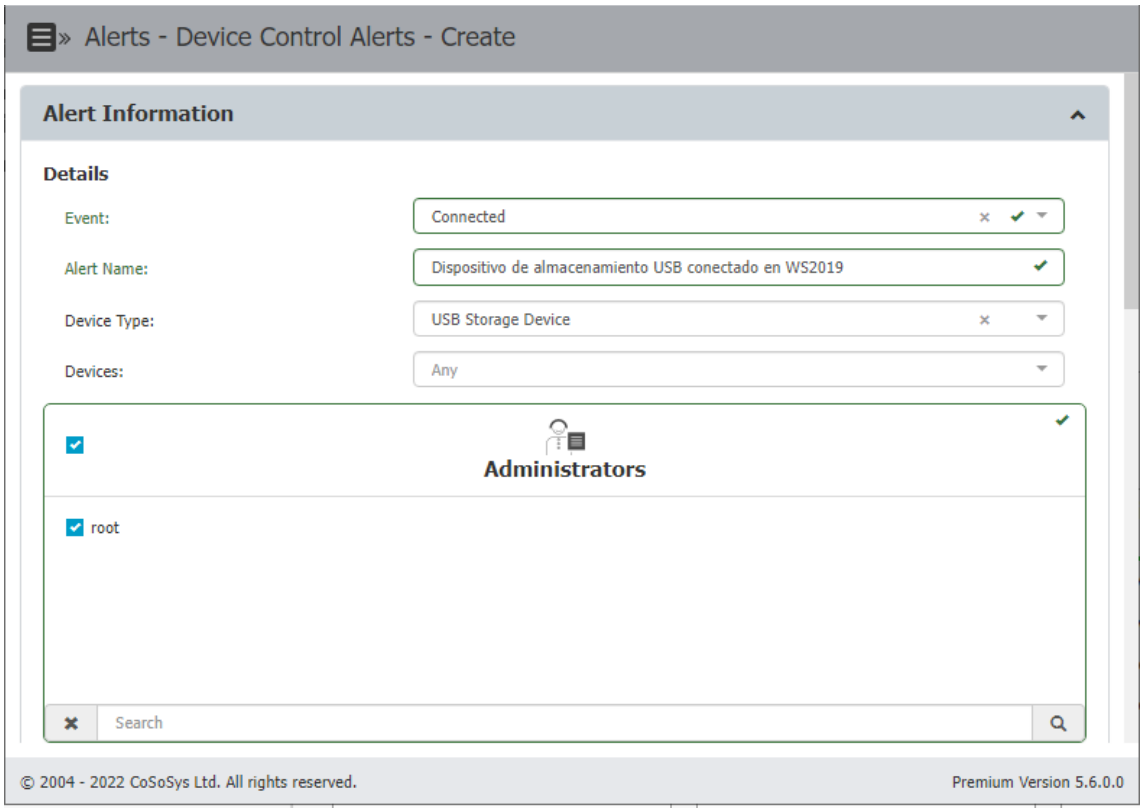


Esta contraseña se ha de proporcionar al usuario correspondiente, de manera que pueda introducirla en el campo Código de Autorización del agente de EPP.



CD.12. Recibir alertas por correo en tiempo real para eventos relacionados con el uso de medios extraíbles.

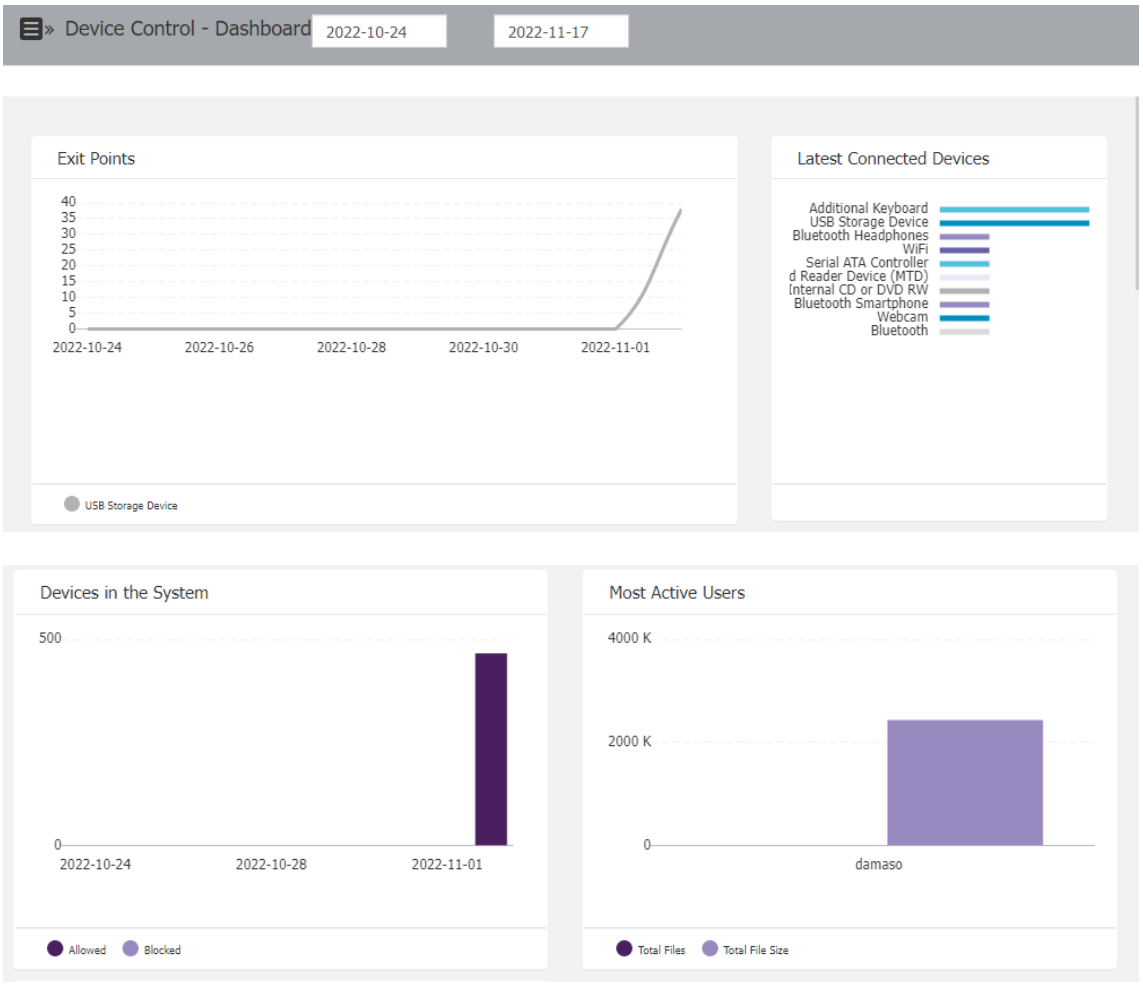
Las alertas de medios extraíbles se configuran en la sección Alerts > Device Control Alerts.



Adicionalmente, cada alerta definida se puede aplicar a los grupos, equipos o usuarios que seleccionemos. Se ha creado una alerta que avisa al correo cuando se conecte cualquier dispositivo de almacenamiento USB en el servidor WS2019, ya que en este equipo, por su naturaleza, no se deberían conectar este tipo de dispositivos.

CD.13. Revisar los gráficos y tablas que ofrece la solución para obtener una visión general de los eventos más importantes.

Desde Device Control > Dashboard podemos visualizar los diferentes gráficos y tablas que ofrece EPP:



En el presente proyecto, y debido a que los dispositivos extraíbles no funcionan en el entorno de laboratorio, únicamente aparecen amenazas para el usuario del equipo portátil Winterfell.

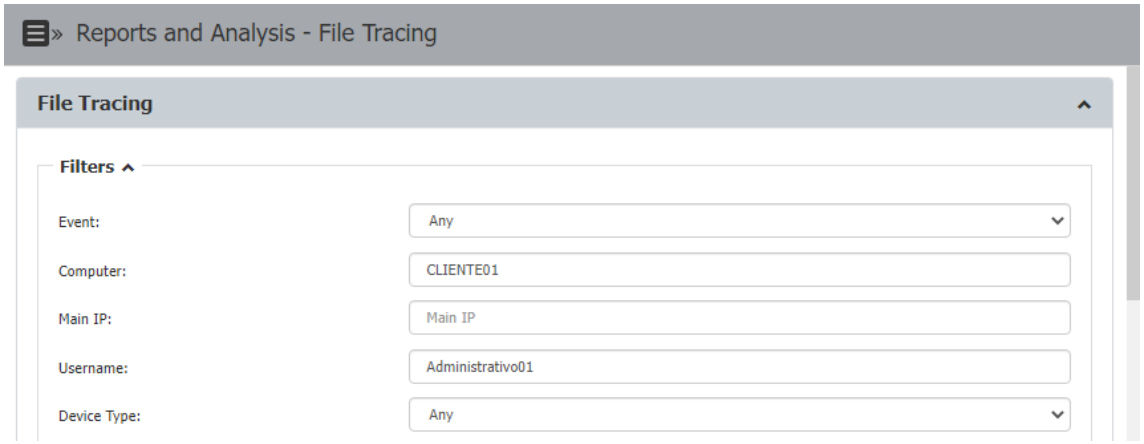
CD.14. Monitorizar la actividad relacionada con la transferencia de archivos.

Desde la sección Reports and Analysis > File tracing podemos realizar búsquedas de eventos aplicando diferentes filtros:

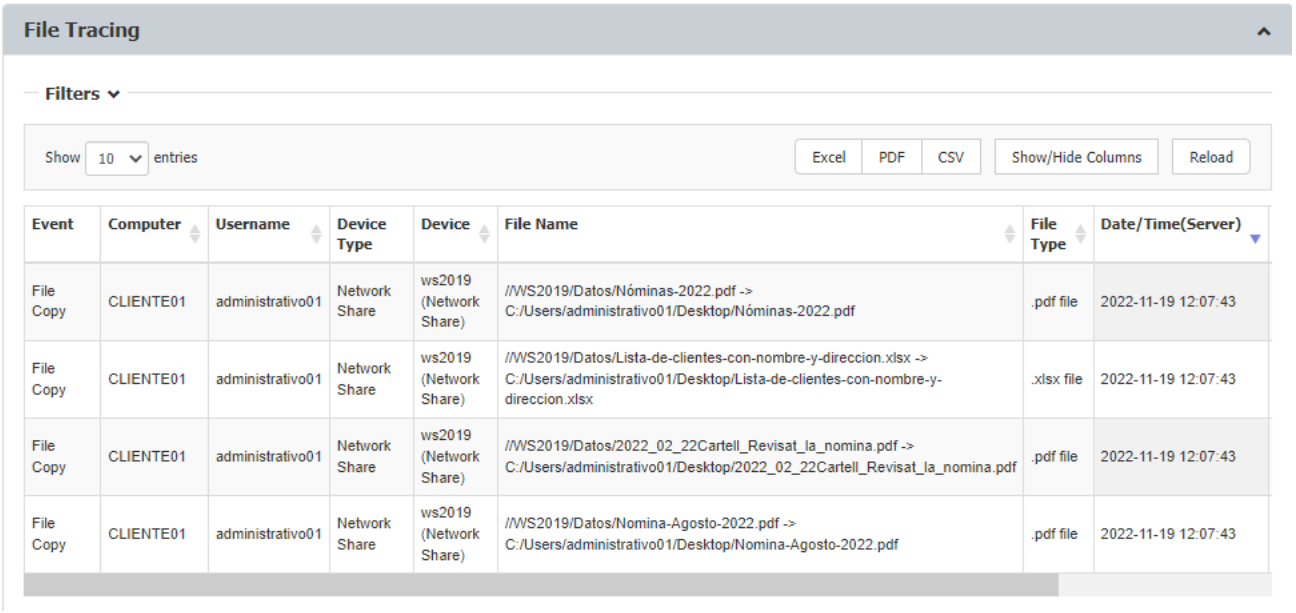
- Tipo de evento: (lectura, escritura, copia, borrado, renombrado, encriptado/desencriptado, etc.).
- Equipo en el que se ha realizado.
- Usuario que lo ha realizado.
- Tipo de dispositivo.
- Nombre del fichero.

El caso de uso aquí podría ser analizar las acciones realizadas por algún usuario en caso de sospechar que está exfiltrando información. Se muestra como ejemplo el filtro

realizado para revisar cualquier tipo de evento asociado al usuario Administrativo01 en el equipo Cliente01:



Y los resultados obtenidos:

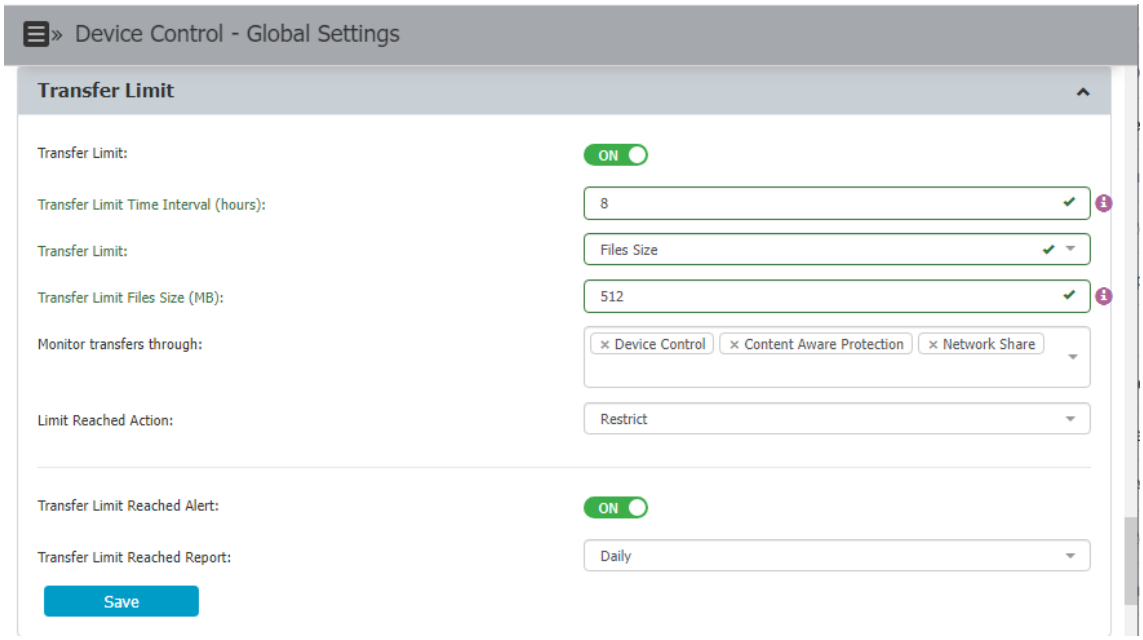


CD.15. Establecer límites en el número de archivos o el tamaño que se puede transferir dentro de un intervalo de tiempo.

Desde la sección Device Control > Global Settings se pueden establecer diferentes tipos de límites. Se pueden definir los siguientes parámetros:

- Intervalo de tiempo en horas en el que se calculará este límite.
- Si el límite se establece por tamaño o número de ficheros transferidos.
- Tamaño en MB o número de ficheros establecido como límite

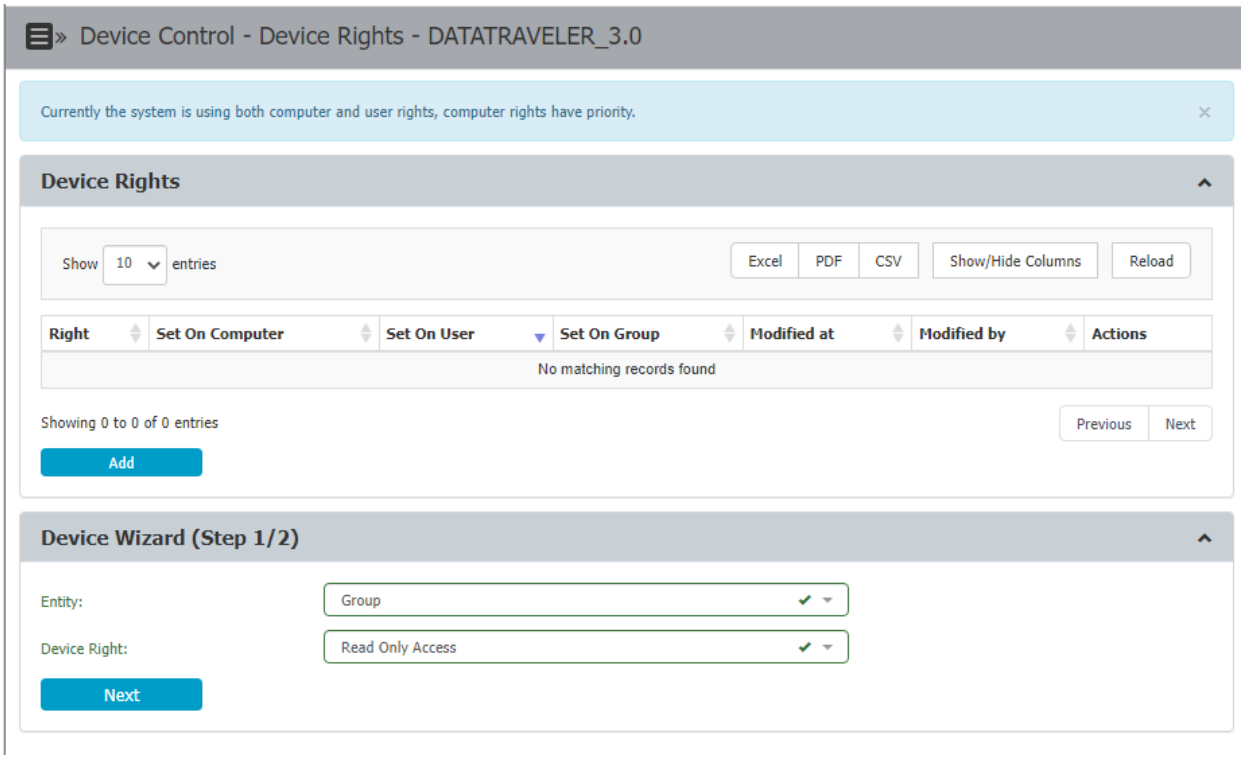
- Monitorizar a través de: Control de dispositivos, Protección basada en contenido, unidades de red compartidas, o una combinación de las anteriores.
- Acción que realizar en caso de alcanzar el límite: Monitor only (únicamente avisa cuando se alcanza el límite), Restrict (bloquea los dispositivos y aplicaciones definidos en las políticas de Control de dispositivos), o Lockdown (bloquea todos los dispositivos, independientemente de si se han definido o no en las políticas de Control de dispositivos).
- Se permite habilitar una alerta al usuario cuando se alcance el límite de transferencia.
- Se puede planificar un informe periódico diario, semanal o mensual sobre esta configuración.



La configuración de la imagen adjunta limita la transferencia de más de 512 MB en 8h por cualquier vía, y puede ser utilizada para impedir la exfiltración de una gran cantidad de información de la organización, aunque se debe ser cuidado con el umbral definido.

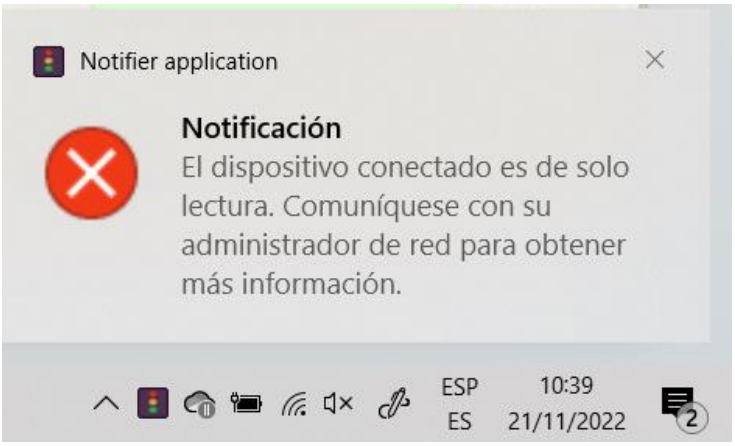
CD.16. Incluir o excluir las transferencias por dispositivos.

Desde la sección Device Control > Devices, podemos editar los permisos de los dispositivos extraíbles para que estos únicamente puedan ser accedidos en modo solo lectura.



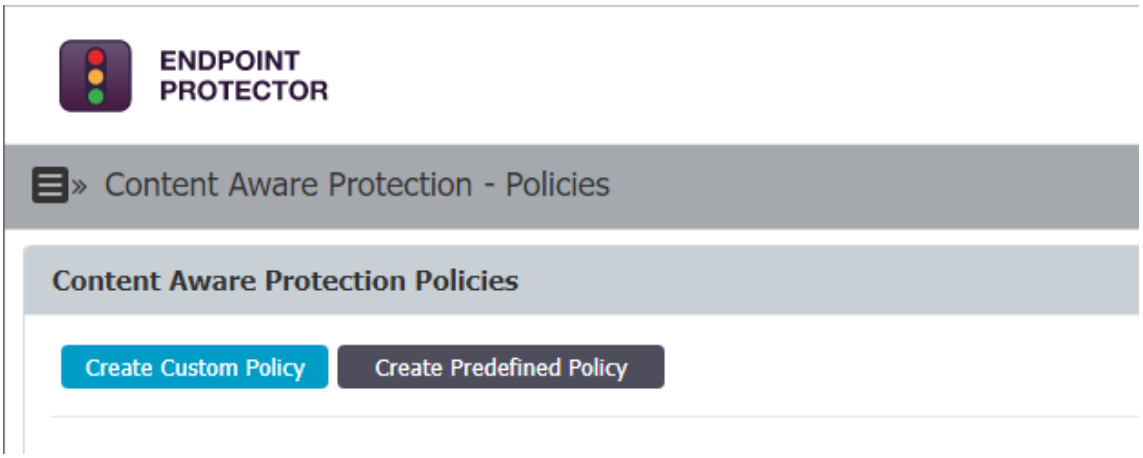
Este caso de uso puede ser útil si se quiere distribuir información a alguno de los departamentos de manera offline, pero se quiere impedir la copia de nuevos ficheros al dispositivo extraíble.

Cuando el usuario introduce el dispositivo en su equipo, se le advierte mediante una notificación de esta circunstancia:

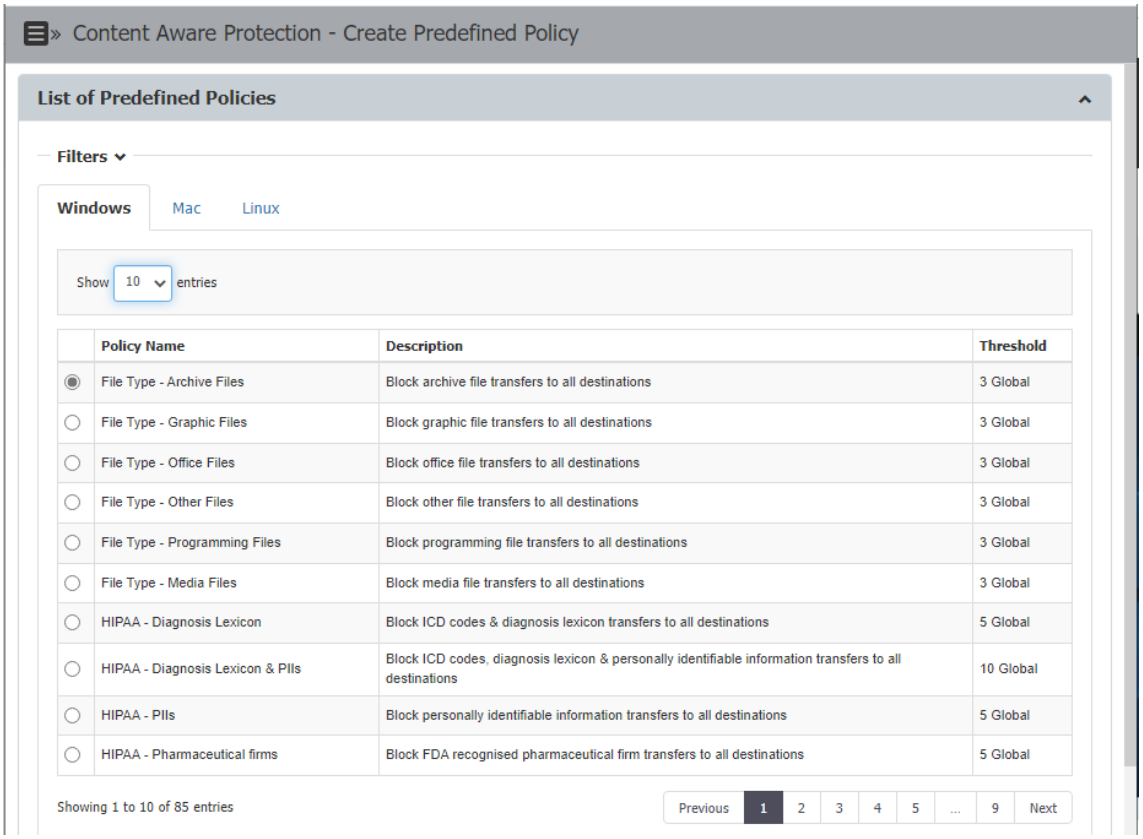


CD.17. Limitar la transferencia de ficheros en aplicaciones online.

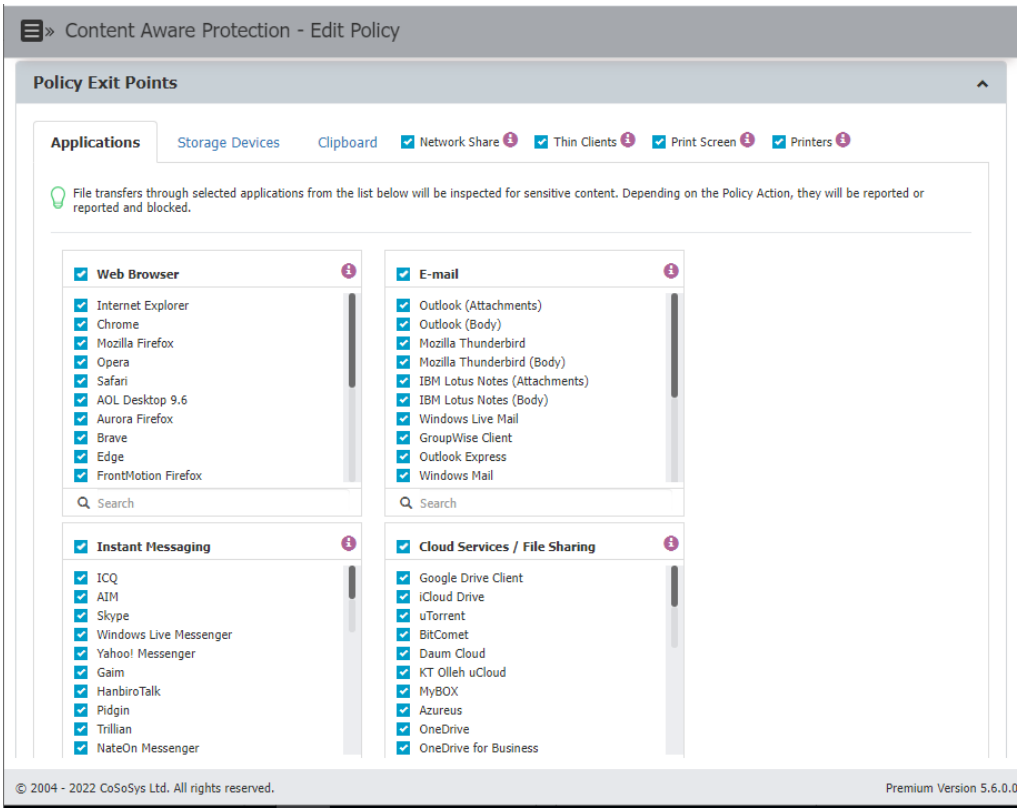
La limitación de transferencia de ficheros en aplicaciones online (Google Drive, Microsoft OneDrive, Dropbox, etc.) se habilita en la sección Content Aware Protection. EPP ofrece un conjunto de políticas predefinidas o nos permite crear nuestra propia política personalizada:



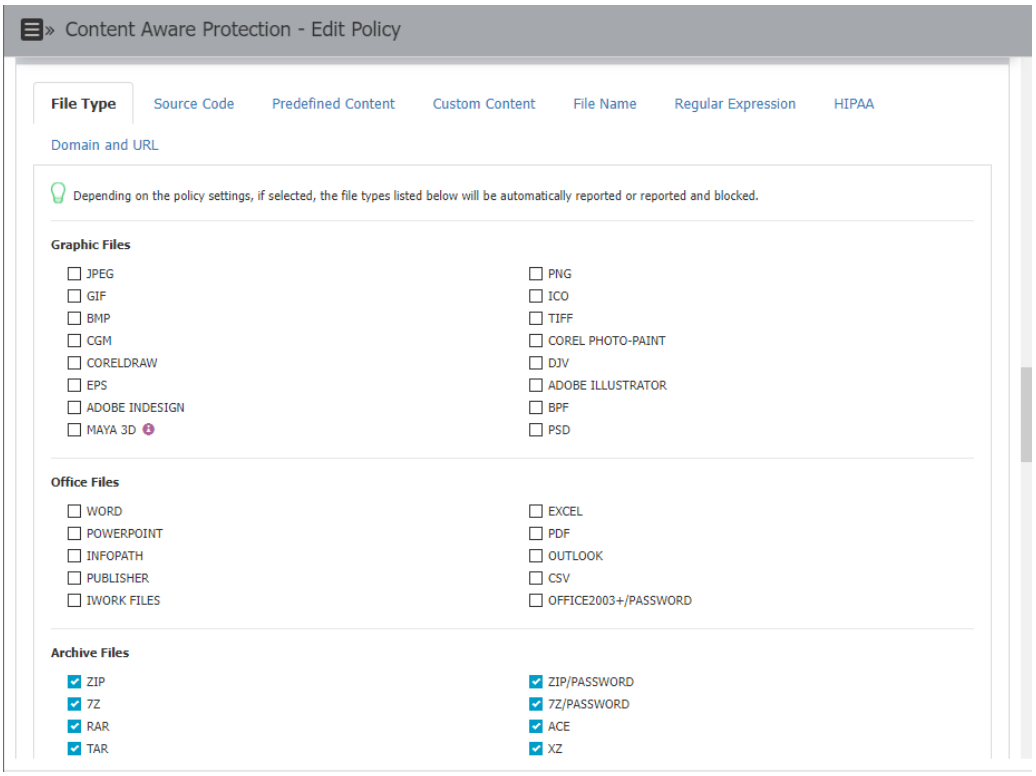
Creamos una política predefinida de tipo File type a todos los destinos para verificar su uso:



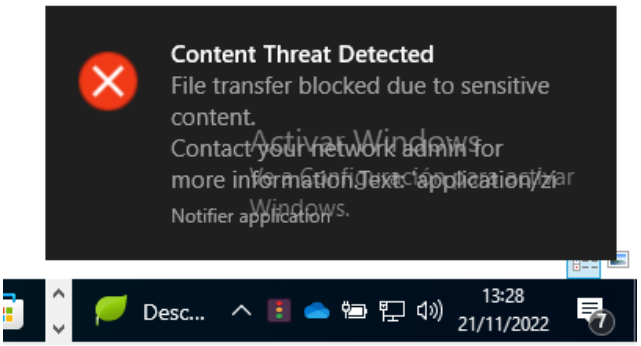
Esta política se puede personalizar posteriormente para concretar qué aplicaciones se inspeccionan, o qué tipos de fichero se bloquean, si aplican a dispositivos de almacenamiento, portapapeles, unidades de red compartidas, etc.



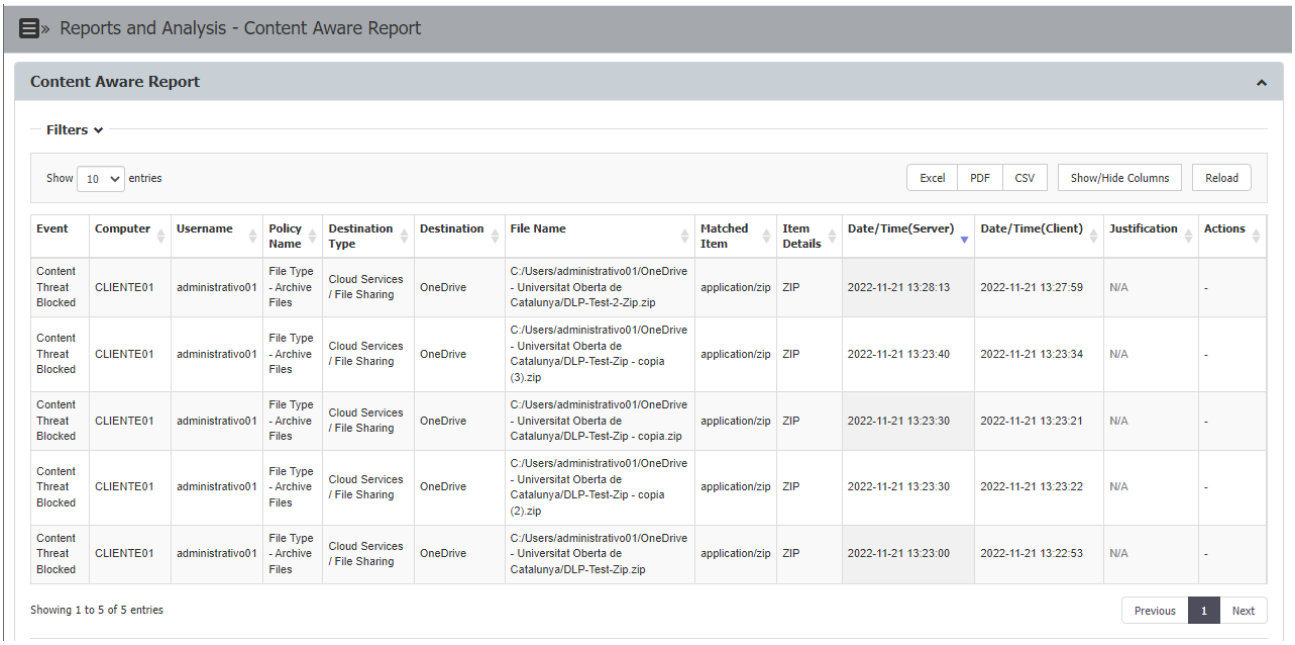
Esta política de ejemplo bloquea únicamente ficheros comprimidos:



Cuando intentamos copiar un fichero zip a Microsoft OneDrive para evaluar esta política, el agente de EPP nos impide realizar la copia:



Y se genera el evento correspondiente en los registros de Protección Basada en Contenido, que se pueden consultar en la sección Reports and Analysis > Content Aware Report.

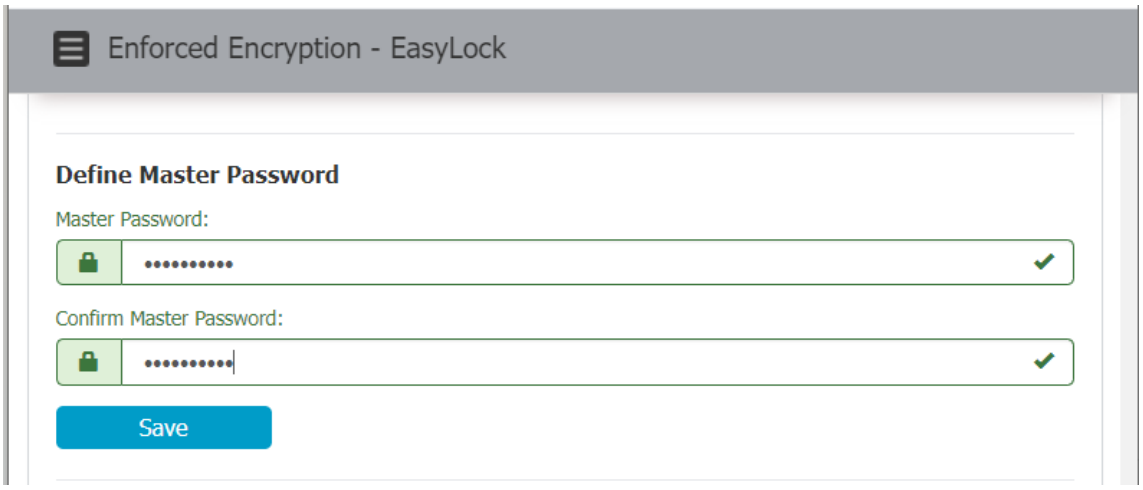


Event	Computer	Username	Policy Name	Destination Type	Destination	File Name	Matched Item	Item Details	Date/Time(Server)	Date/Time(Client)	Justification	Actions
Content Threat Blocked	CLIENTE01	administrativo01	File Type - Archive Files	Cloud Services / File Sharing	OneDrive	C:/Users/administrativo01/OneDrive - Universitat Oberta de Catalunya/DLP-Test-2-Zip.zip	application/zip	ZIP	2022-11-21 13:28:13	2022-11-21 13:27:59	N/A	-
Content Threat Blocked	CLIENTE01	administrativo01	File Type - Archive Files	Cloud Services / File Sharing	OneDrive	C:/Users/administrativo01/OneDrive - Universitat Oberta de Catalunya/DLP-Test-Zip - copia (3).zip	application/zip	ZIP	2022-11-21 13:23:40	2022-11-21 13:23:34	N/A	-
Content Threat Blocked	CLIENTE01	administrativo01	File Type - Archive Files	Cloud Services / File Sharing	OneDrive	C:/Users/administrativo01/OneDrive - Universitat Oberta de Catalunya/DLP-Test-Zip - copia.zip	application/zip	ZIP	2022-11-21 13:23:30	2022-11-21 13:23:21	N/A	-
Content Threat Blocked	CLIENTE01	administrativo01	File Type - Archive Files	Cloud Services / File Sharing	OneDrive	C:/Users/administrativo01/OneDrive - Universitat Oberta de Catalunya/DLP-Test-Zip - copia (2).zip	application/zip	ZIP	2022-11-21 13:23:30	2022-11-21 13:23:22	N/A	-
Content Threat Blocked	CLIENTE01	administrativo01	File Type - Archive Files	Cloud Services / File Sharing	OneDrive	C:/Users/administrativo01/OneDrive - Universitat Oberta de Catalunya/DLP-Test-Zip.zip	application/zip	ZIP	2022-11-21 13:23:00	2022-11-21 13:22:53	N/A	-

3.3.2.Cifrado forzado

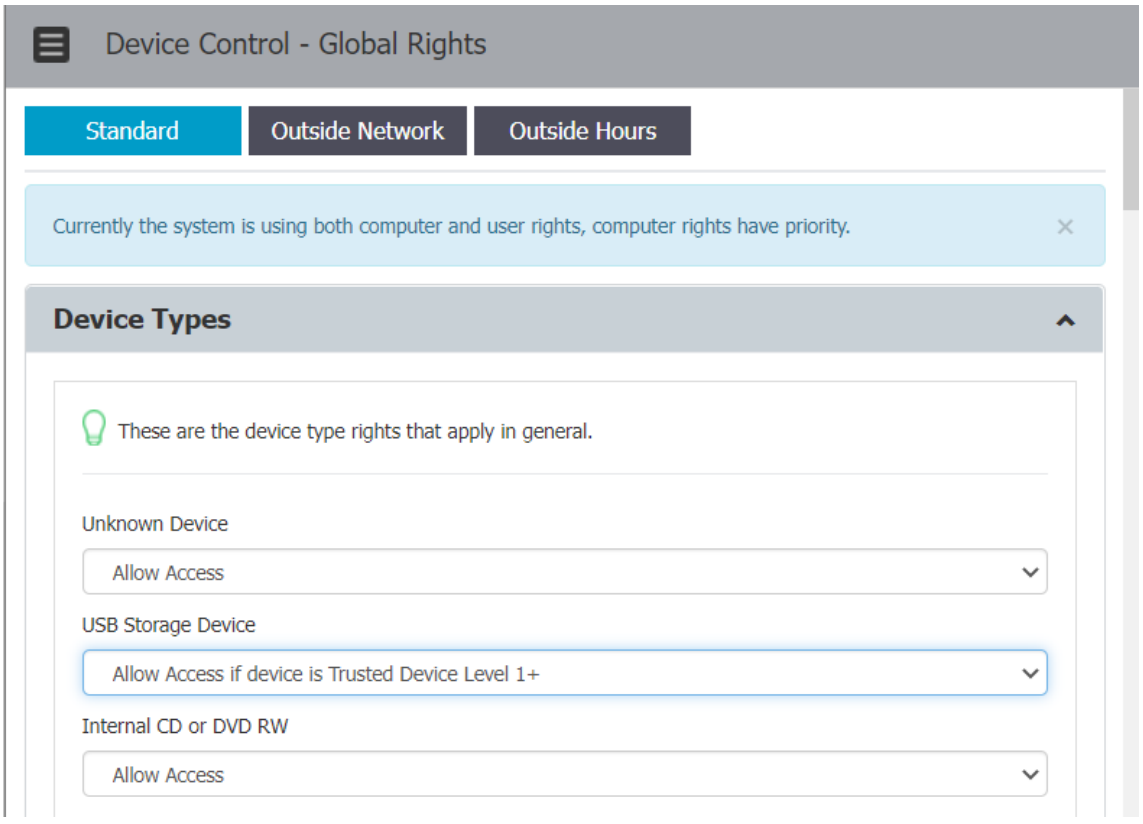
Las políticas de Cifrado forzado se habilitan en la sección Enforced Encyption > EasyLock. La instalación de la utilidad EasyLock que permite el uso de estas características se puede realizar de forma manual o automática.

Antes de habilitar estas políticas, debemos establecer una Master Password en la sección mencionada del servidor de EPP:

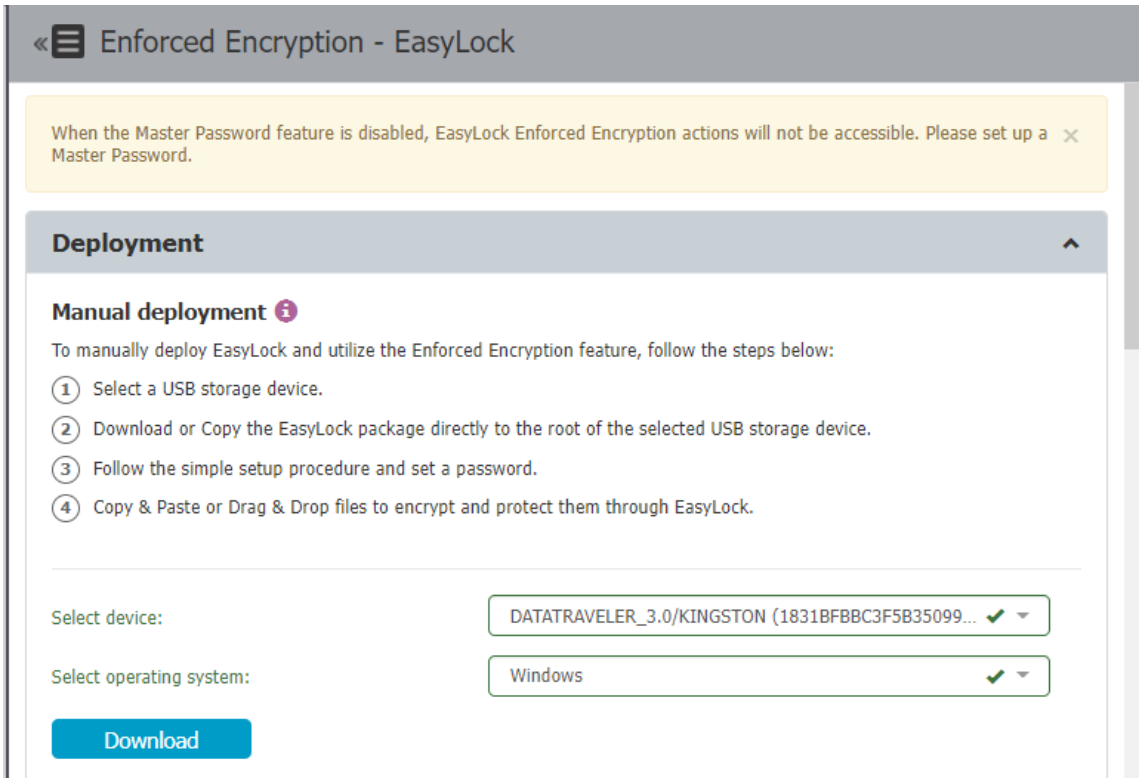


CF.1. Autorizar únicamente el uso de dispositivos USB cifrados para asegurar que todos los datos copiados en estos dispositivos son cifrados

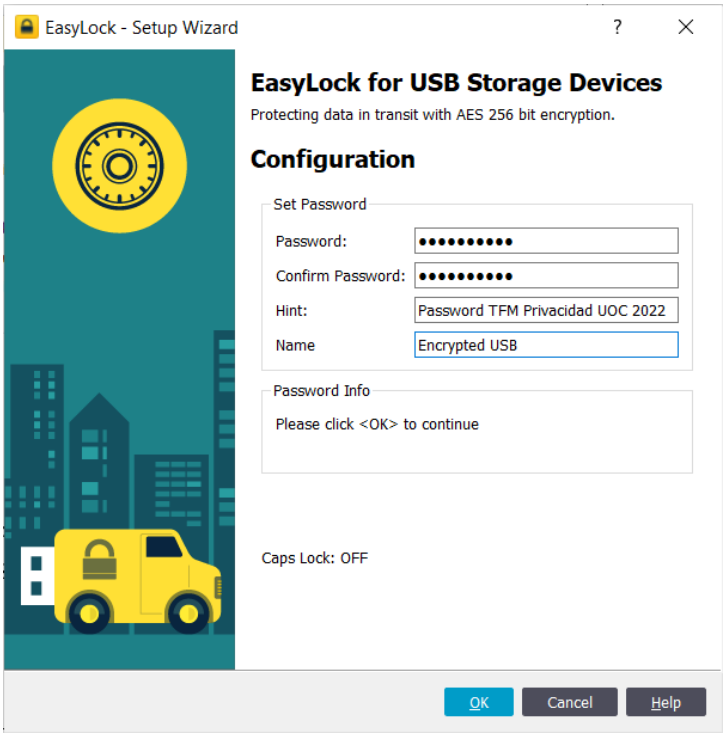
Desde la sección Device Control > Global Rights, podemos aplicar la configuración que permita el acceso únicamente a dispositivos USB cifrados, de manera que si no están cifrados, automáticamente no sean reconocidos por el sistema.



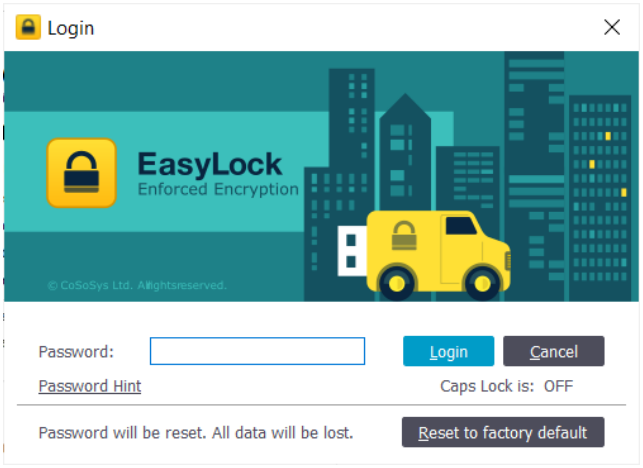
Para realizar el cifrado de un dispositivo extraíble, descargamos el software EasyLock de Enforced Encryption > EasyLock seleccionando el sistema operativo y el dispositivo concreto en el que vamos a realizar la instalación:



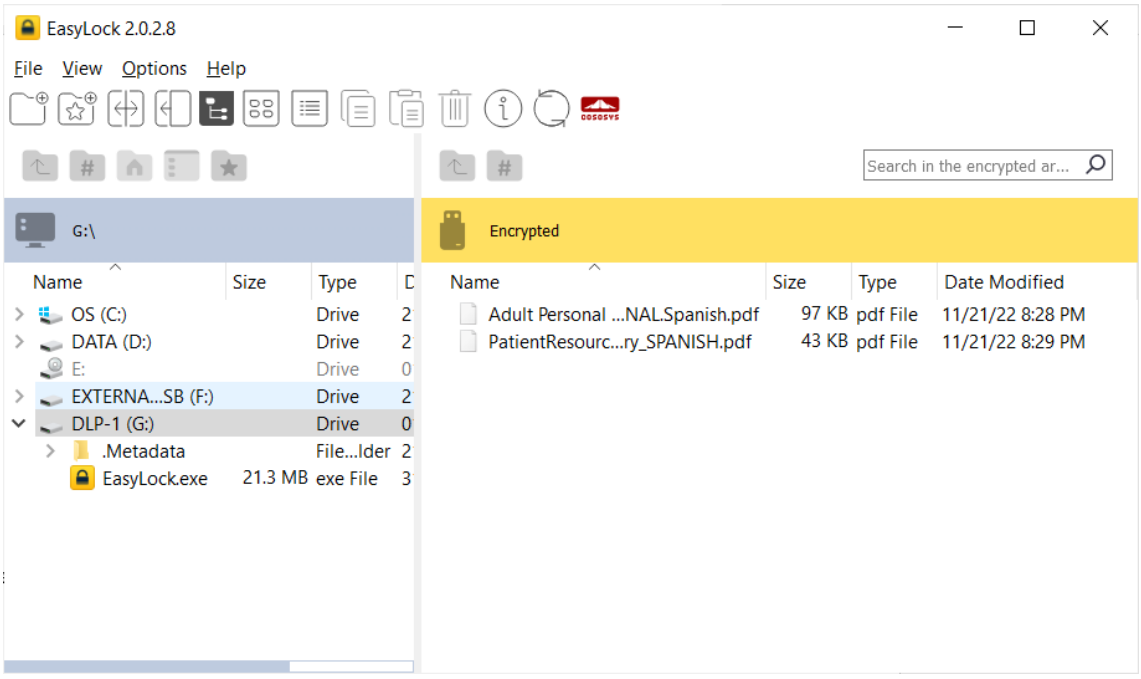
El software se presenta como un ejecutable portable, y lo copiamos junto a la carpeta .Metadata en la raíz del USB. Tras esto, lo ejecutamos y establecemos la contraseña:



Una vez hemos establecido la contraseña, cuando conectamos el dispositivo USB se nos presenta una ventana de login en la que tenemos que autenticarnos:



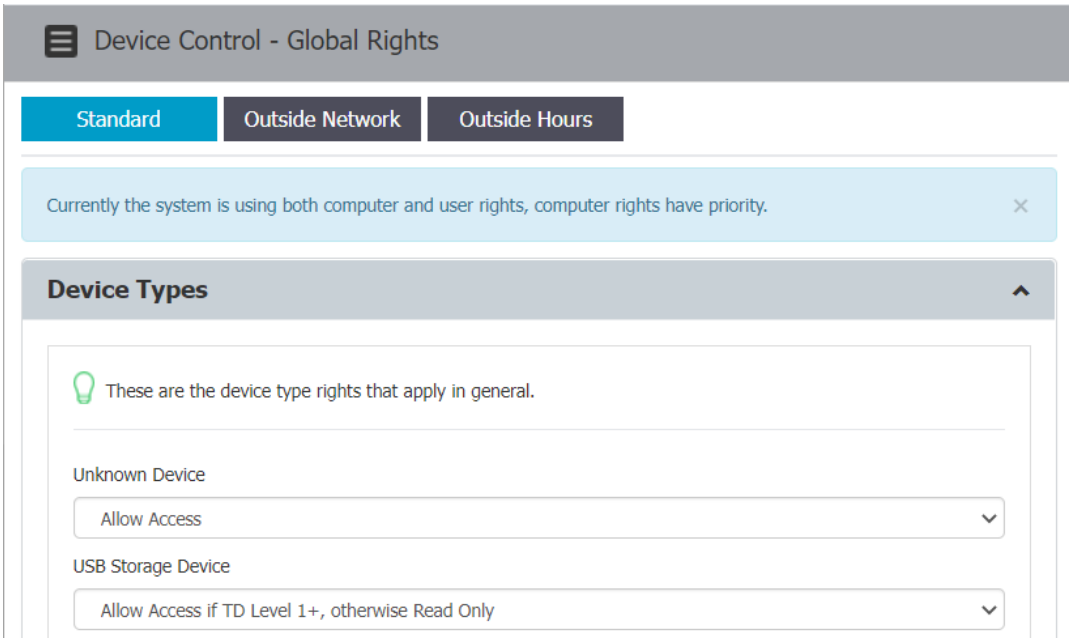
Tras introducir la contraseña, podemos utilizar EasyLocker para almacenar cualquier fichero de forma encriptada:



CF.2. Permitir el acceso de solo lectura o forzar la encriptación del dispositivo si se quiere escribir en él

De manera análoga a la configuración anterior, podemos configurar EPP para que permita el acceso de solo lectura a dispositivos extraíbles, pero solo permita escribir en ellos si se accede vía EasyLock. Esta configuración puede ser realizada por dispositivo en combinación con un filtro de equipo o usuario, grupos de dispositivos, o de forma genérica en la configuración global.

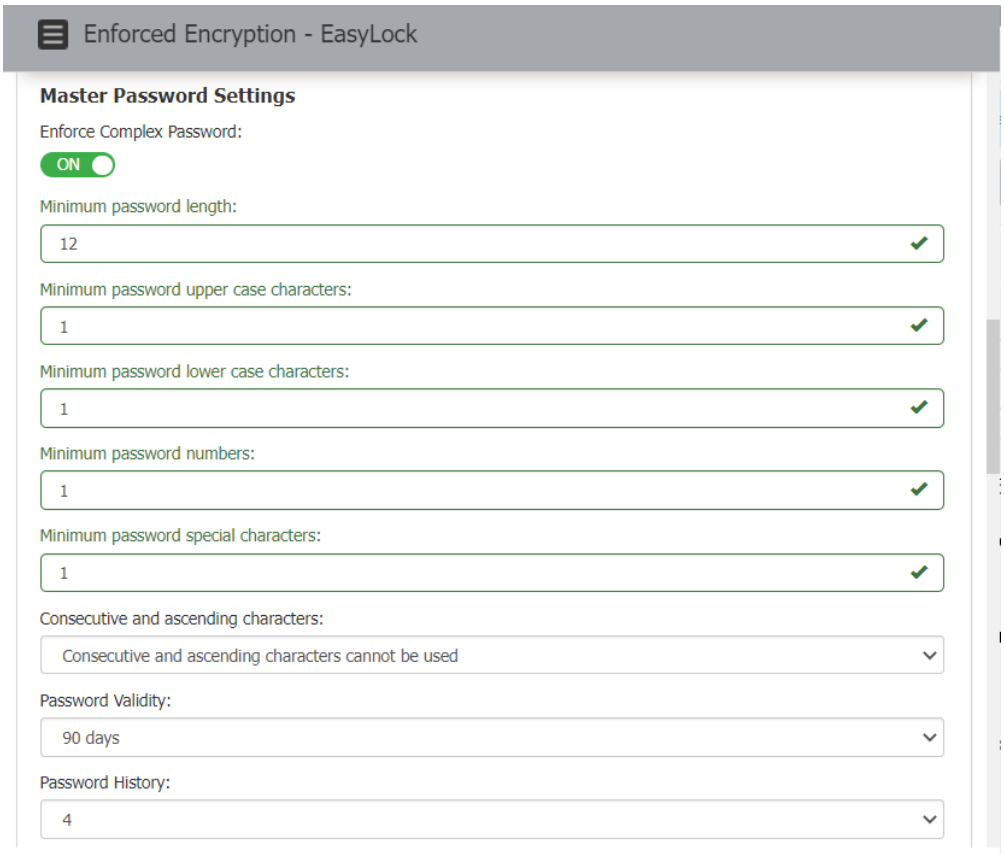
Para realizar esta configuración de forma global se accede a la sección Device Control > Global Rights:



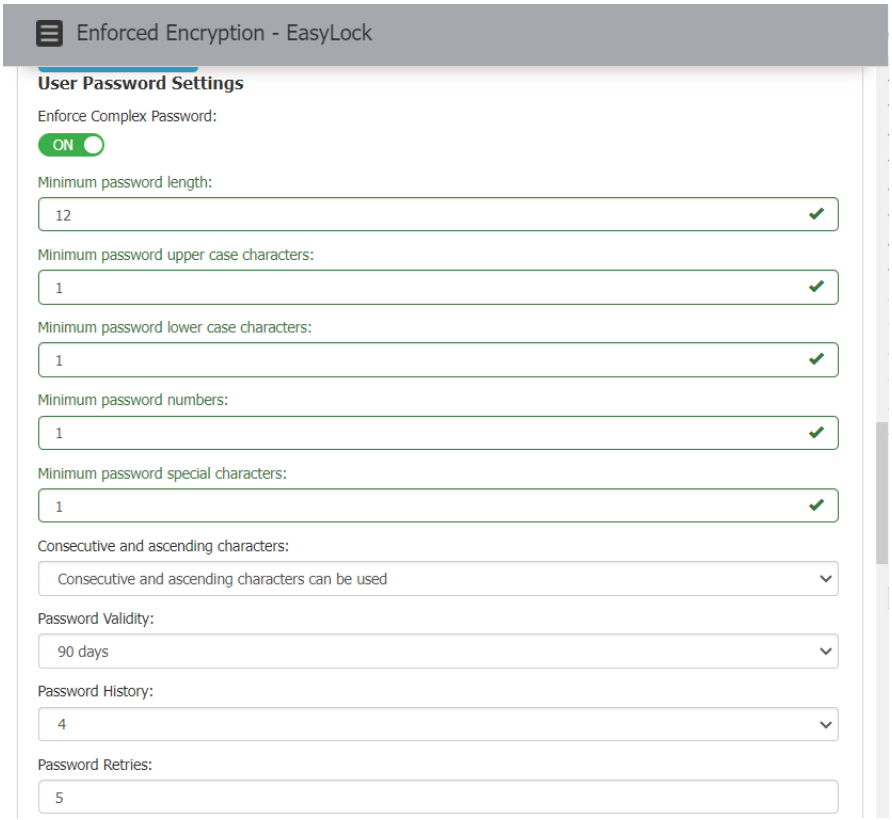
CF.3. Establecer la complejidad de las contraseñas de cifrado

Desde la sección Enforced Encryption > EasyLock, podemos establecer la complejidad de las contraseñas de cifrado maestra y de usuario. Se muestra la configuración realizada en el servidor de EPP:

Contraseña maestra:

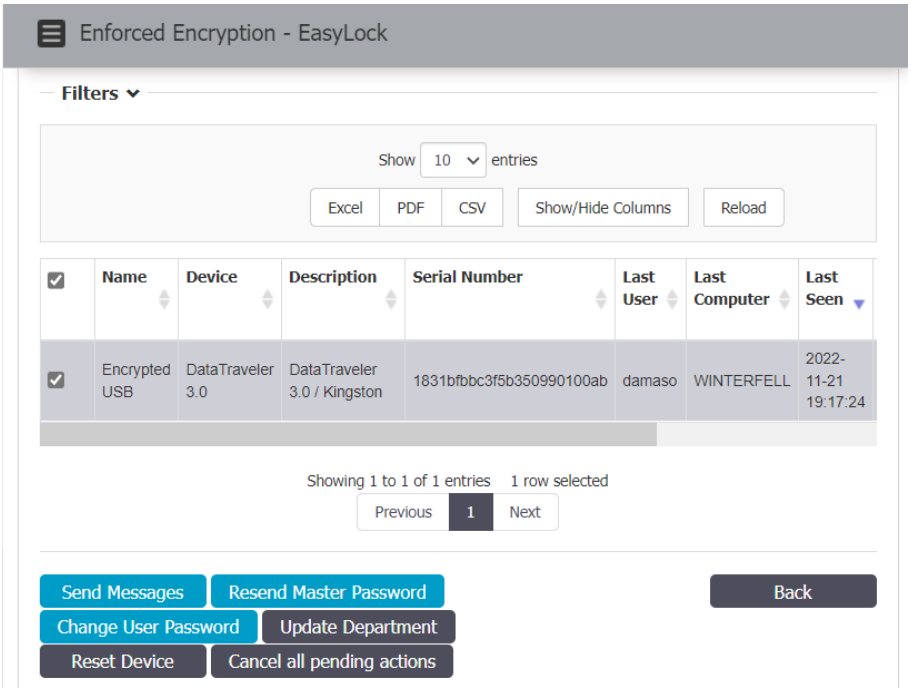


Contraseña de usuarios:

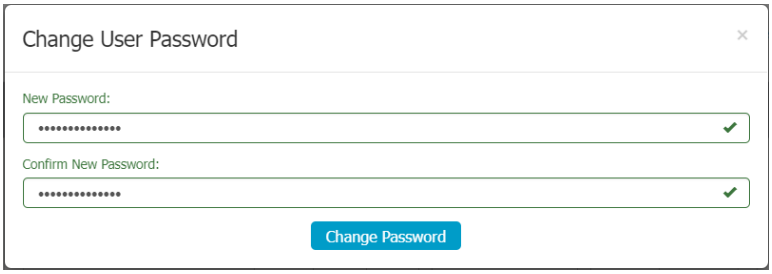


CF.4. Cambio de las contraseñas de cifrado de usuarios de forma remota

Desde la sección Enforced Encryption > EasyLock, podemos restablecer la contraseña de cualquier dispositivo almacenado en la base de datos de EPP de forma individual. Este cambio de contraseña es realizado a través del agente cuando el dispositivo se conecta.



Tras hacer clic en Change User Password, la establecemos:

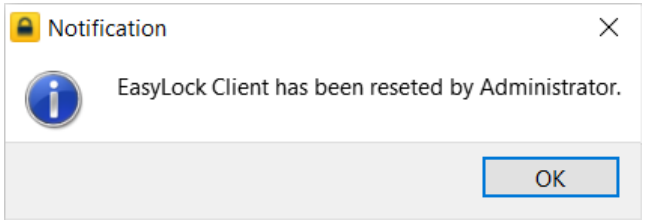


CF.5. Borrar los datos de los dispositivos en el caso de que estos se hayan visto comprometidos

En el caso de que un dispositivo se haya visto comprometido, podemos forzar el borrado la próxima vez que se conecte a un equipo con el agente de EPP. Esto es realizado en la misma sección que el cambio de contraseña de usuario, haciendo clic en Reset Device.

Nos pide confirmación:

Cuando volvemos a acceder al dispositivo a través de EasyLock, se nos notifica de que este ha sido restablecido, y los datos encriptados almacenados en él son borrados:



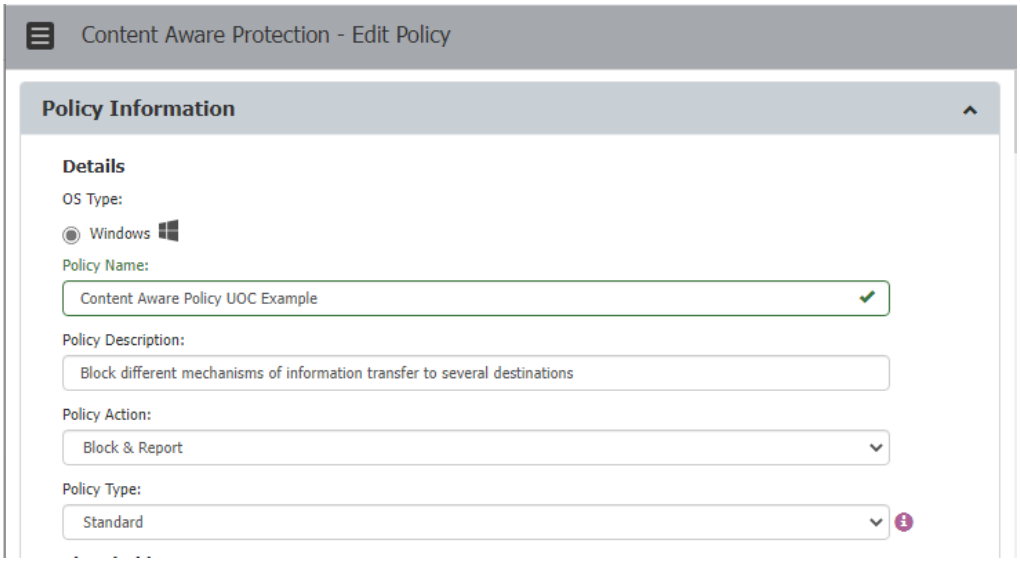
3.3.3.Protección basada en contenido

Las políticas de protección basada en contenido son un conjunto de reglas para la detección contenido confidencial, pudiendo impedirlo antes de que se produzca en las entidades seleccionadas (usuarios, equipos grupos o departamentos).

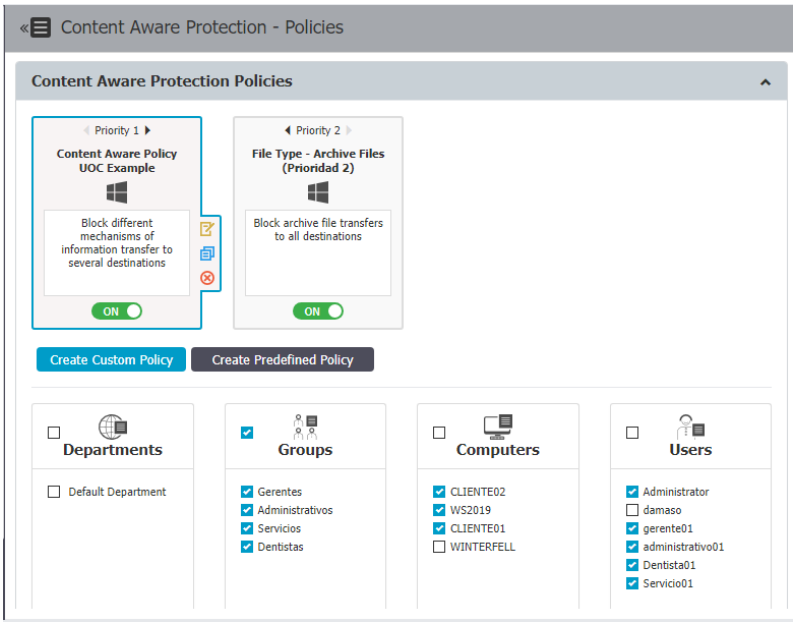
Para demostrar los diferentes casos de uso, se ha creado una política de este tipo en la sección Content Aware Protection > Content Aware Policies de EPP. Cada compañía puede personalizar sus listas de datos de contenido confidencial haciendo uso de los

Custom Content Dictionaries que proporciona EPP, no obstante, este módulo ya ofrece un conjunto de reglas predefinidas.

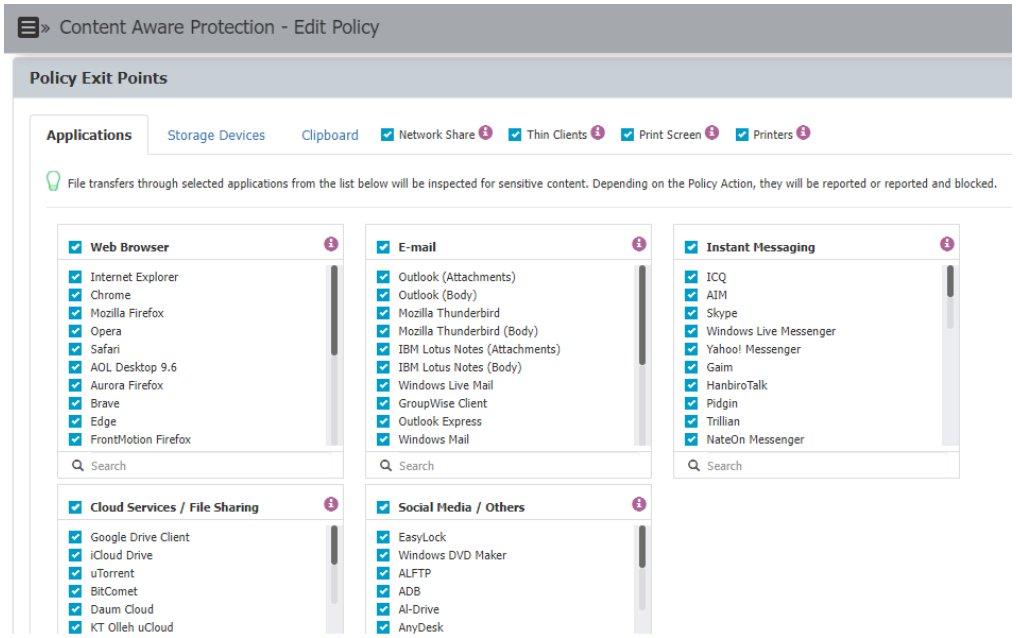
Diferentes políticas pueden aplicarse al mismo equipo/usuario, por lo que la prioridad de estas se realiza de izquierda a derecha según se presentan en la interfaz web, siendo la izquierda la más prioritaria. Esta sería una política de ejemplo que desarrollaremos a lo largo de este punto:



En la siguiente imagen se aprecia como la política *Content Aware Policy UOC Example* tiene la mayor prioridad, y está asignada a diferentes grupos, equipos y usuarios:



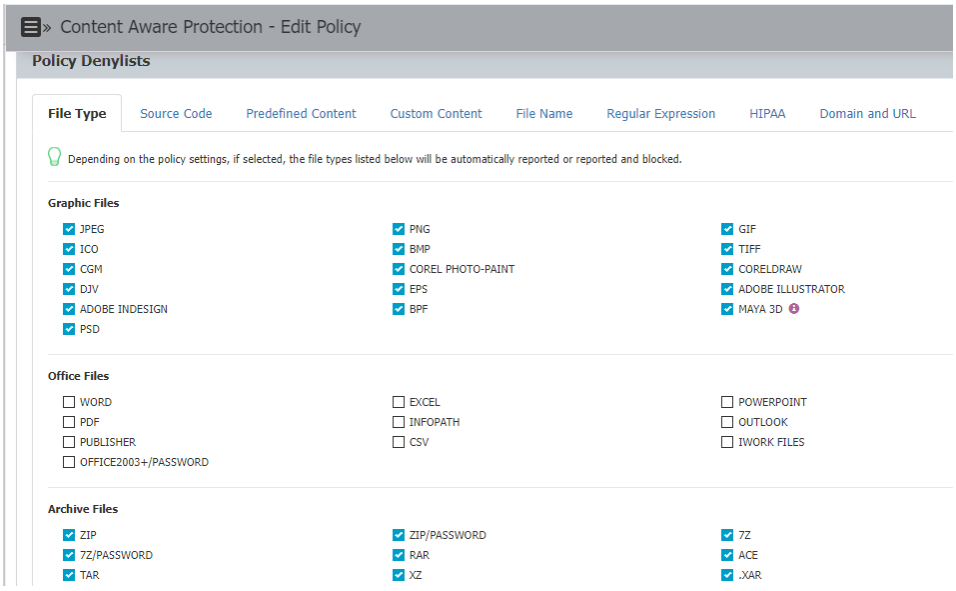
Las políticas pueden configurarse para inspeccionar un conjunto de aplicaciones, dispositivos extraíbles, unidades compartidas, puestos cliente o aplicaciones, tal y como se aprecia en la siguiente imagen:



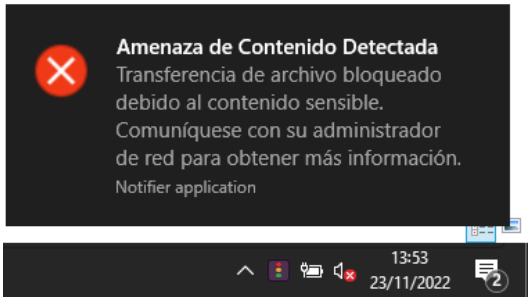
PBC.1. Bloqueo de archivos basados en su extensión real

Las políticas de protección basadas en contenido permiten el bloqueo de archivo basándose en la extensión real. El caso de uso puede ser la existencia de algún rol en la organización que no deba utilizar un determinado tipo de fichero.

Se configura en la política de protección basada en contenido, en la sección Policy Denylist > File Type. En la política de ejemplo hemos bloqueado los archivos de tipo gráfico, y los archivos comprimidos:



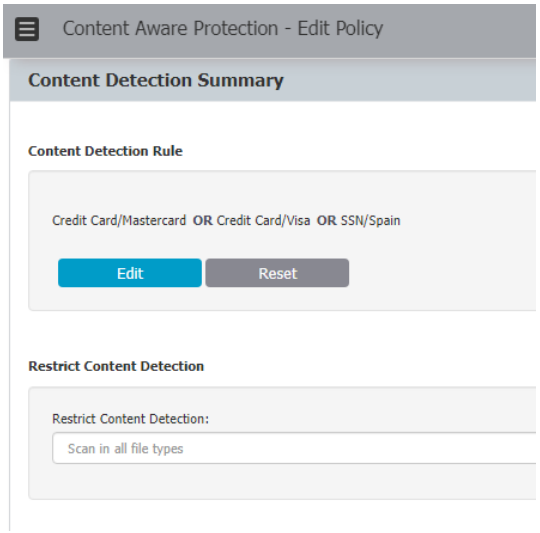
Verificamos el funcionamiento de esta política intentando adjuntar un fichero comprimido .zip a un correo electrónico de Gmail y a través de OneDrive, y efectivamente, el agente de EPP lo bloquea y muestra las alertas correspondientes:



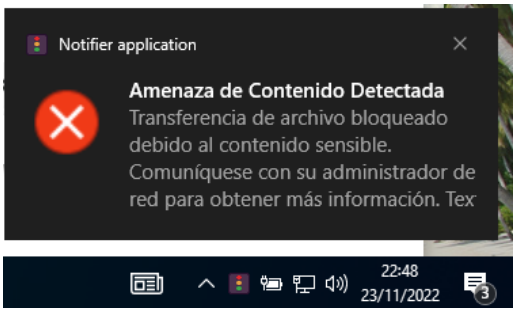
Content Threat Blocked	WS2019	servicio01	Content Aware Policy UOC Example	Web Browser	Edge	C:/Users/servicio01/Downloads/Cloud.zip	application/zip	ZIP	2022-11-23 14:54:23
Content Threat Blocked	CLIENTE01	administrativo01	Content Aware Policy UOC Example	Cloud Services / File Sharing	OneDrive	C:/Users/administrativo01/OneDrive - Universitat Oberta de Catalunya/DLP-Test-2-Zip.zip	application/zip	ZIP	2022-11-23 08:32:12
Content Threat Blocked	CLIENTE01	administrativo01	File Type - Archive Files	Cloud Services / File Sharing	OneDrive	C:/Users/administrativo01/OneDrive - Universitat Oberta de Catalunya/DLP-Test-2-Zip.zip	application/zip	ZIP	2022-11-22 13:06:52
Content Threat Blocked	CLIENTE01	administrativo01	File Type - Archive Files	Cloud Services / File Sharing	OneDrive	C:/Users/administrativo01/OneDrive - Universitat Oberta de Catalunya/DLP-Test-2-Zip.zip	application/zip	ZIP	2022-11-22 13:06:52

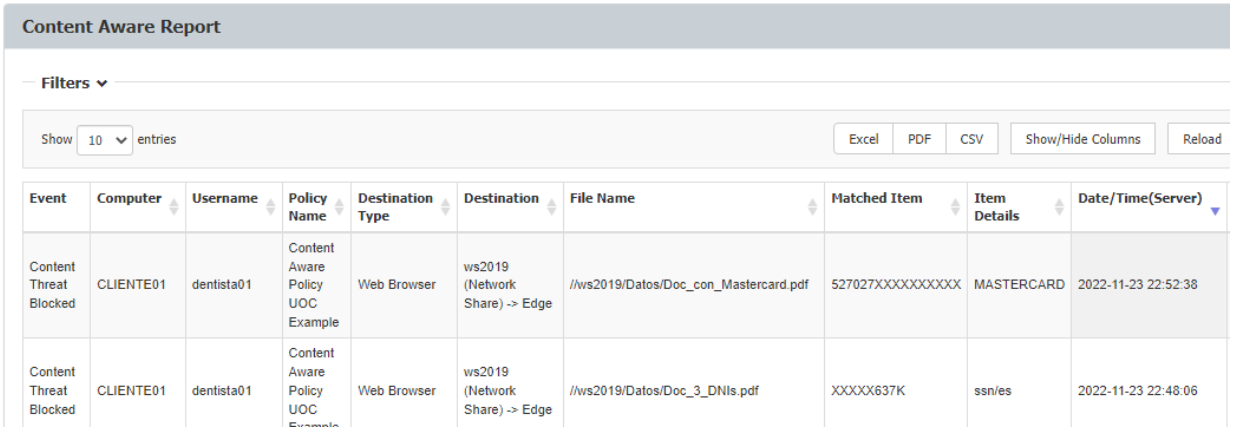
PBC.2. Crear filtros basados en contenido (Número de tarjetas de crédito y Números de seguridad social, por ejemplo)

En la sección Content Detection de la política de protección basada en contenido podemos definir qué contenido es sensible entre un conjunto de reglas predefinidas, o podemos crear reglas personalizadas. Para la verificación de este control se ha marcado como contenido sensible el *Spanish SSN* (predefinido por EPP, incluye el patrón de número de seguridad social, DNI y pasaporte), las tarjetas VISA y MasterCard.



Se han realizado pruebas con varios documentos PDF que contenían diferentes números de DNI y tarjetas de crédito, obteniendo un resultado satisfactorio en el bloqueo:





PBC.3. Inspeccionar el contenido de fotos e imágenes, detectando información confidencial desde documentos escaneados y similares

EPP inspecciona todos los documentos accedidos desde un cliente, incluyendo aquellos escaneados, en busca de contenido que pueda haberse definido como confidencial.

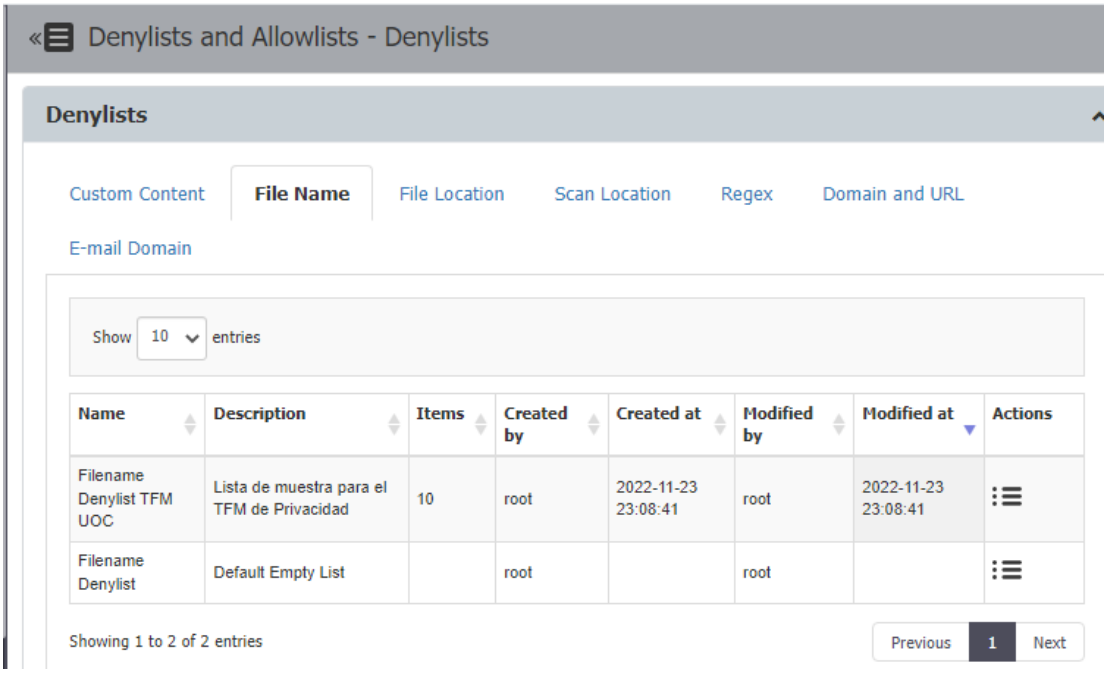
Para verificar el funcionamiento de esta característica, hemos utilizado un documento PDF que contenía una imagen de un DNI escaneado por ambas caras, y las imágenes de forma independiente en formato JPG.

Sin embargo, tras realizar varias pruebas, el agente de EPP no ha detectado cuando hemos enviado estos archivos por correo (Gmail), los hemos movido a una unidad de red compartida, o los hemos subido a OneDrive.

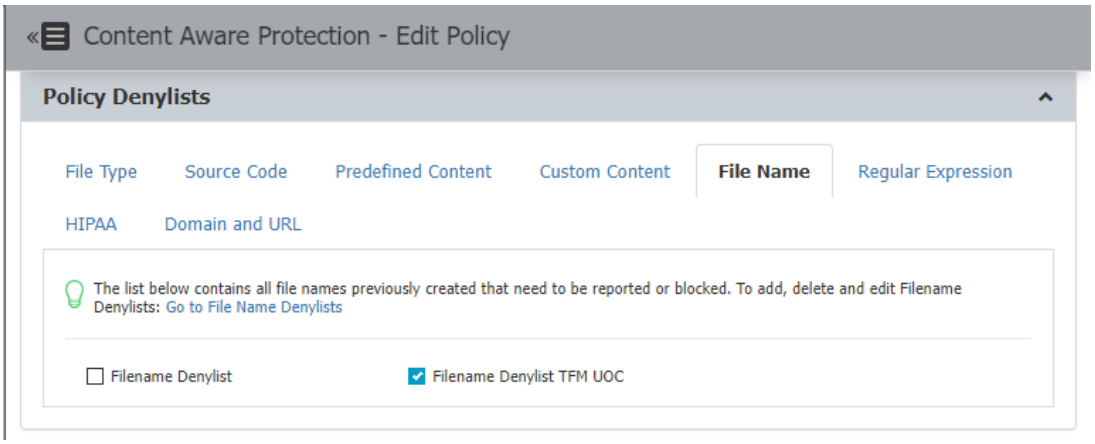
PBC.4. Crear filtros basados en nombres de archivo para asociar acciones a ellas.

EPP permite realizar filtros basándonos en ubicación, dominio, URL, o nombre de los archivos. Este último filtro es utilizado para permitir o denegar el uso de un listado de palabras, filtrándose por los diferentes puntos de salida definidos en las políticas de protección basada en contenido. Para ello, establecemos en primer lugar este listado desde

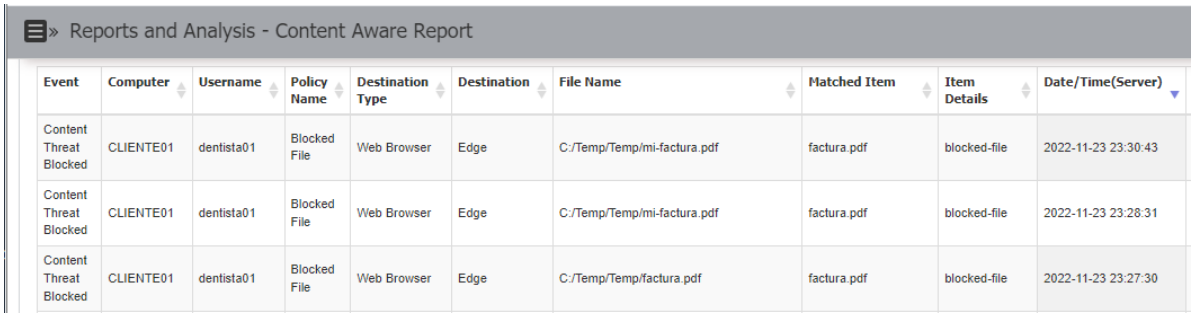
la sección Denylists and Allowlists > Denylists. La lista creada contiene las palabras: cliente, clientes, factura, facturas, historia, historial, historial_clinico, historial-clinico, presupuesto, presupuestos.



Posteriormente, podemos definir una política que se asigne a los grupos Servicios y Dentistas, de manera que no puedan enviar información al exterior con esos nombres:



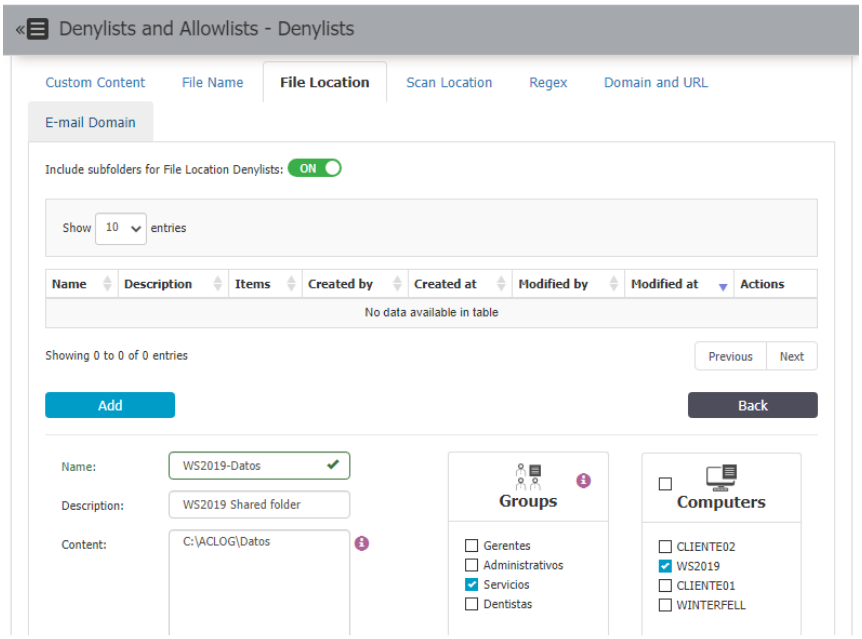
Se verifica el correcto funcionamiento de la política copiando un fichero llamado factura.pdf a OneDrive, sin embargo, se debe señalar que este tipo de filtros basados en nombre de fichero difícilmente conseguirán frenar una exfiltración de información: no ha funcionado cuando el nombre era “damaso-fenoy-factura” o “damaso-fenoy-factura-20221101”, y sí con la cadena “mi-factura”:



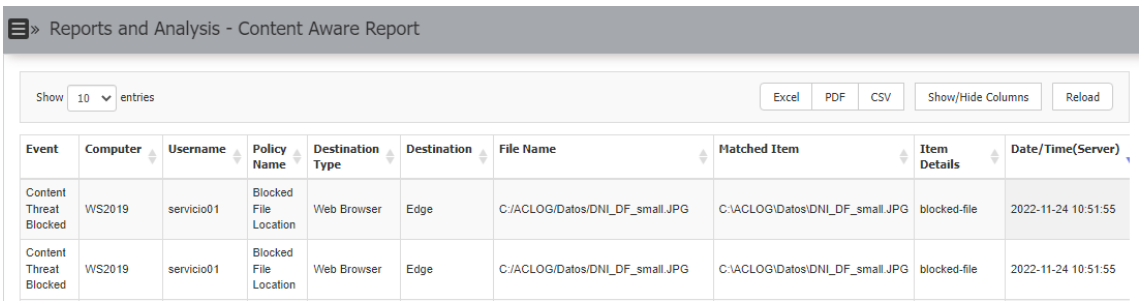
Event	Computer	Username	Policy Name	Destination Type	Destination	File Name	Matched Item	Item Details	Date/Time(Server)
Content Threat Blocked	CLIENTE01	dentista01	Blocked File	Web Browser	Edge	C:/Temp/Temp/mi-factura.pdf	factura.pdf	blocked-file	2022-11-23 23:30:43
Content Threat Blocked	CLIENTE01	dentista01	Blocked File	Web Browser	Edge	C:/Temp/Temp/mi-factura.pdf	factura.pdf	blocked-file	2022-11-23 23:28:31
Content Threat Blocked	CLIENTE01	dentista01	Blocked File	Web Browser	Edge	C:/Temp/Temp/factura.pdf	factura.pdf	blocked-file	2022-11-23 23:27:30

PBC.5. Crear filtros basados en la ubicación de archivos para asociar acciones a ellas.

Como hemos visto previamente, EPP permite la creación de listados de denegación y aprobación basados en diferentes características como nombre de fichero, ubicación, etc. Para utilizar este último, en la sección Denylists and Allowlists > Denylists creamos un filtro de ubicación de ficheros, con el objetivo de impedir al personal de Servicios transferir cualquier documento ubicado en el repositorio compartido C:\ACLOG\Datos del servidor WS2019:



Verificamos que EPP bloquea el envío de un fichero guardado en esta ubicación:

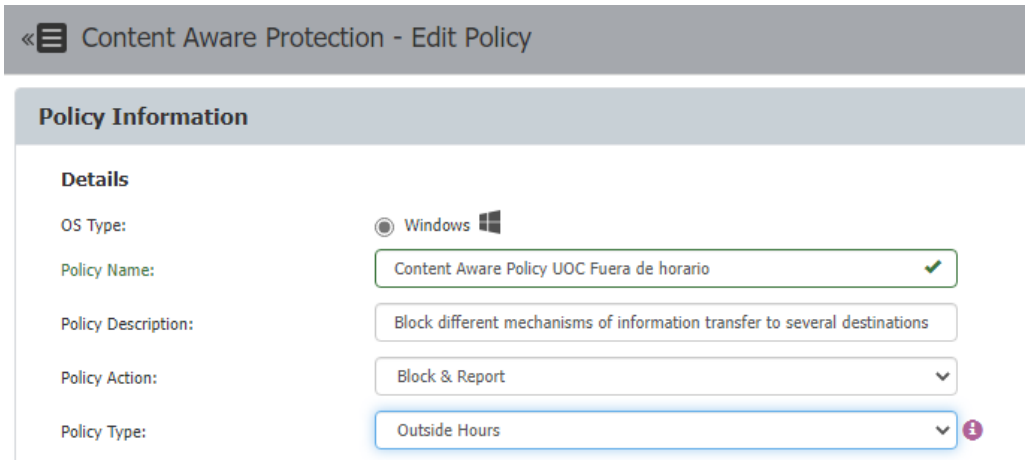


Event	Computer	Username	Policy Name	Destination Type	Destination	File Name	Matched Item	Item Details	Date/Time(Server)
Content Threat Blocked	WS2019	servicio01	Blocked File Location	Web Browser	Edge	C:/ACLOG/Datos/DNI_DF_small.JPG	C:\ACLOG\Datos\DNI_DF_small.JPG	blocked-file	2022-11-24 10:51:55
Content Threat Blocked	WS2019	servicio01	Blocked File Location	Web Browser	Edge	C:/ACLOG/Datos/DNI_DF_small.JPG	C:\ACLOG\Datos\DNI_DF_small.JPG	blocked-file	2022-11-24 10:51:55

Del mismo modo, se podría crear una Allowlist que permita en los clientes 01 y 02 las transferencias de una determinada carpeta que se considere lícita. El inconveniente de esta última configuración es que un usuario podría mover ficheros a dicha carpeta para después poder exfiltrarlos.

PBC.6. Definir políticas de reserva que van a funcionar fuera de las horas laborales.

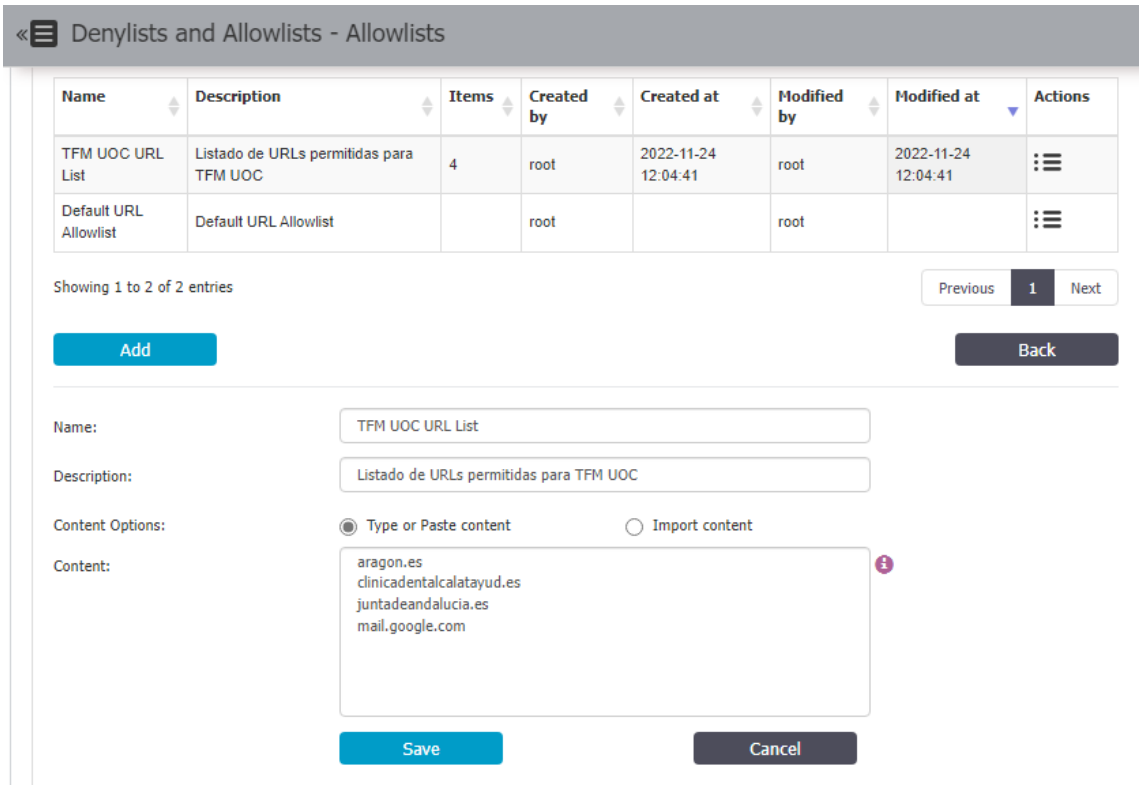
Las políticas de protección basadas en contenido permiten configurarse para ser aplicadas fuera del horario que se ha marcado en la herramienta como laboral. Para ello, en la definición de la política establecemos el Policy Type como Outside Hours:



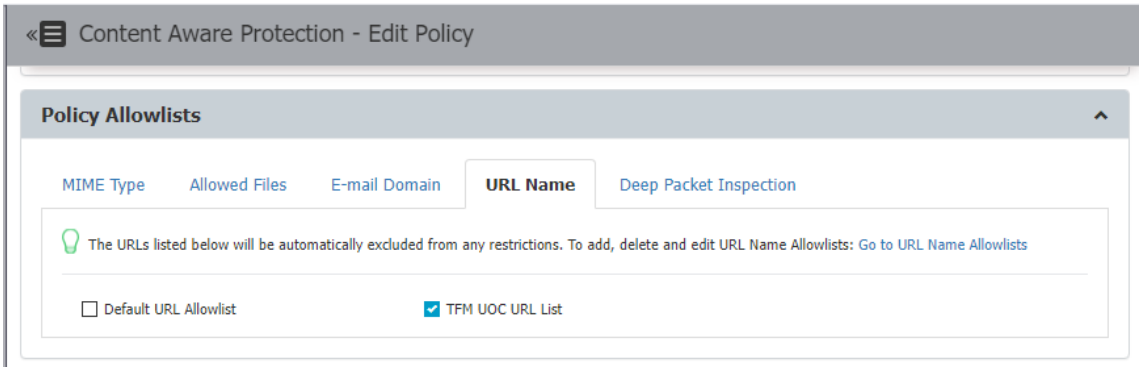
Esto permite definir una política que impida la impresión de cualquier tipo de fichero fuera del horario laboral.

PBC.7. Proporcionar flexibilidad a los empleados permitiendoles el acceso a determinadas URLs que sean necesarias para su trabajo.

EPP permite definir listas de URLs para posteriormente utilizarlas en políticas de protección basadas en contenido que denegándolas o permitiéndolas. En la sección Denylists and Allowlists > Allowlists, se ha definido un listado de URLs permitidas llamado TFM UOC URL List, que contiene las direcciones aragon.es, clinicadentalcalatayud.es, juntadeandalucia.es, etc.



A continuación, la configuramos en la política de protección basada en contenido:



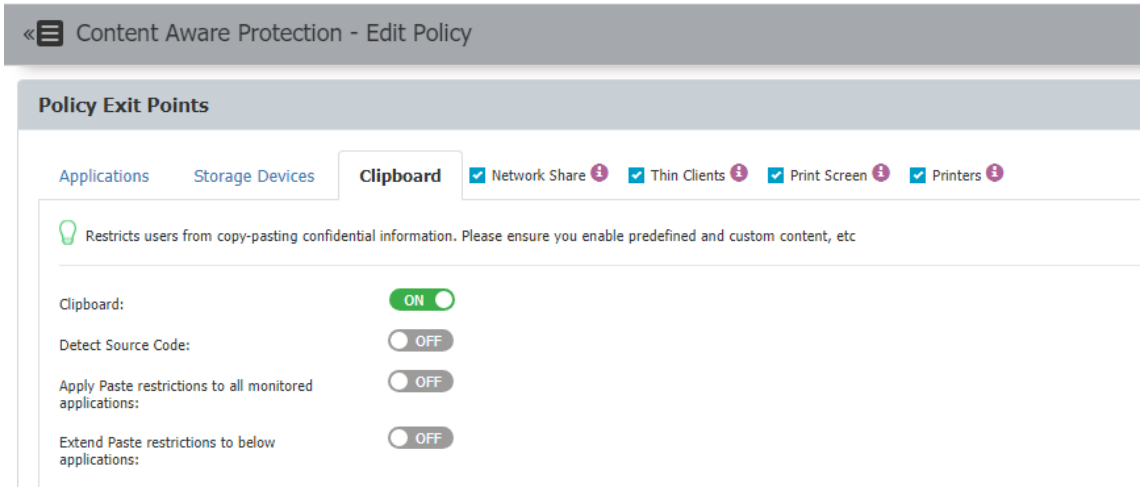
De esta forma, aunque tengamos una política de protección que impide el acceso a determinados tipos de contenido, se pueden establecer listas de URLs permitidas.

El caso de uso podría ser restringir el acceso a páginas de contenido deportivo, pero permitir a determinados grupos de empleados acceder a alguna página concreta.

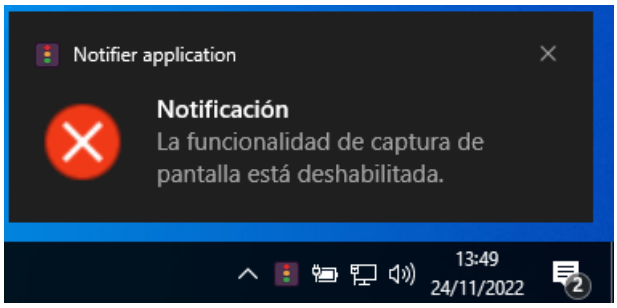
PBC.8. Desactivar la opción de realizar capturas de pantalla y limitar el uso de las opciones copiar/pegar.

Las políticas de protección basadas en contenido permiten definir como punto de salida las herramientas que realizan capturas de pantalla, o el propio portapapeles, para impedir que se pueda copiar información de un documento considerado confidencial al portapapeles.

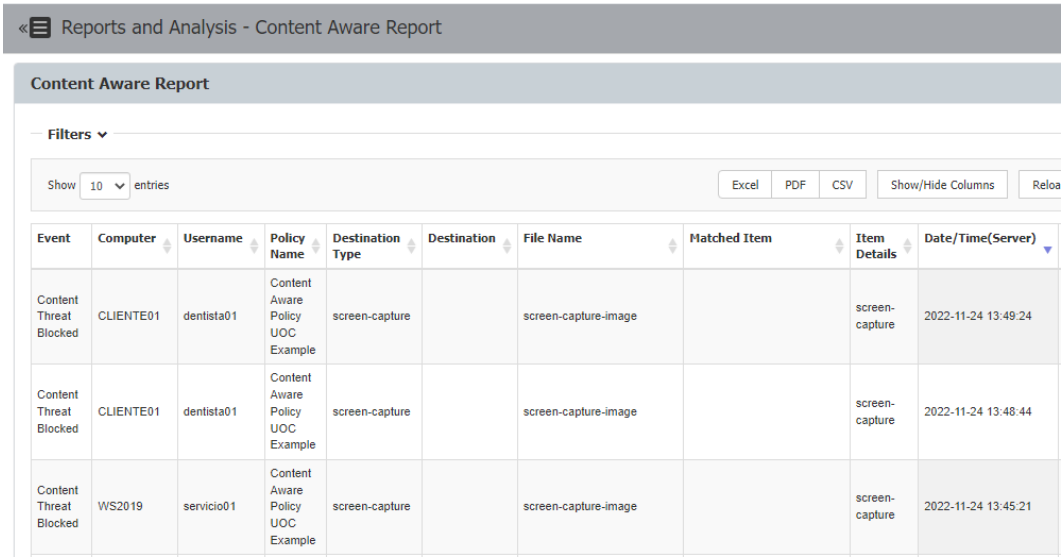
Esto se realiza desde la sección Policy Exit Points de las políticas, en el apartado de Clipboard y Print Screen.



Cuando intentamos realizar una captura de pantalla o utilizar la herramienta Recortes, aparece un aviso indicando que esta funcionalidad está deshabilitada y se genera la alerta correspondiente:

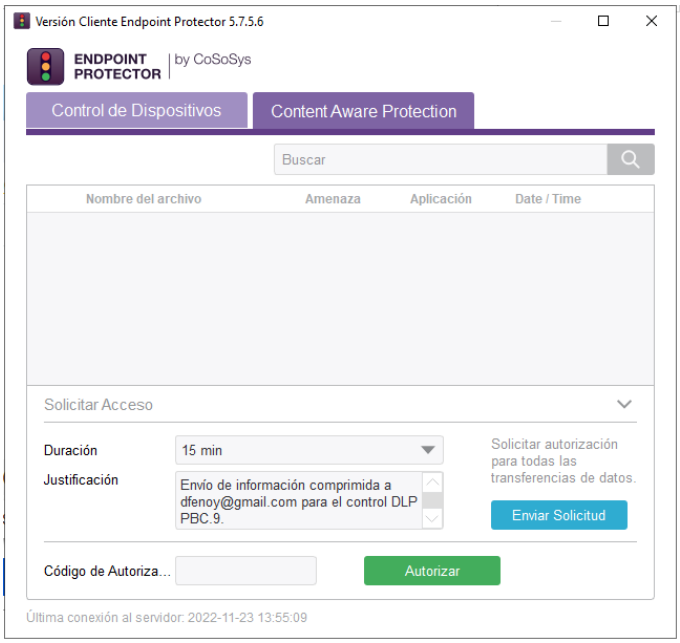


Podemos ver los eventos generados asociados a este comportamiento en la sección Reports and Analysis > Content Aware Report:

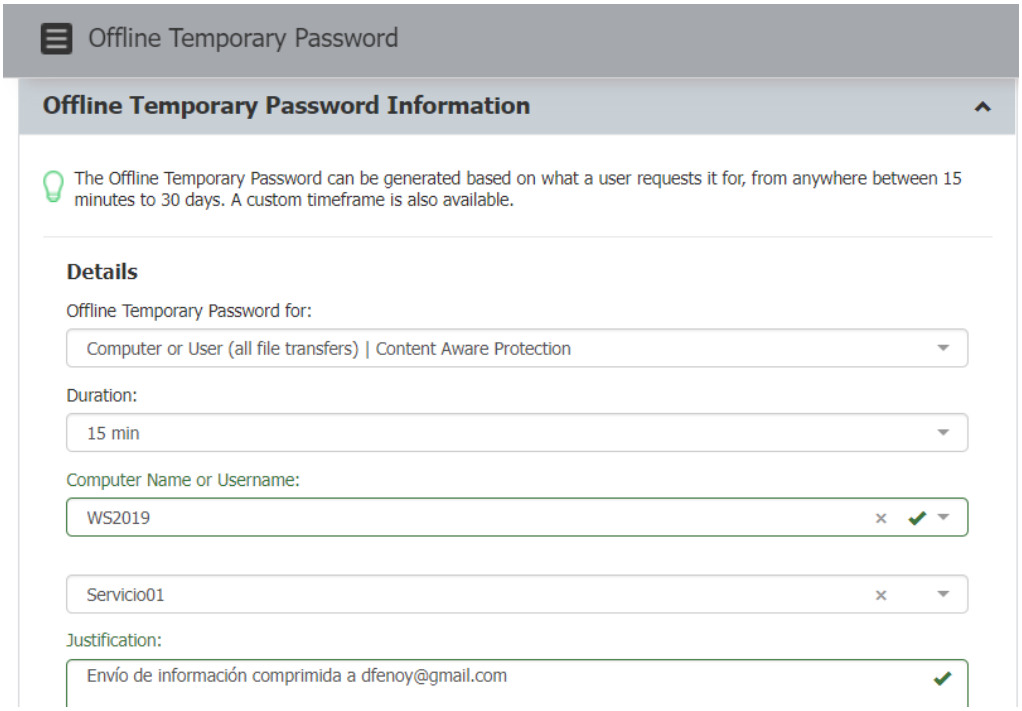


PBC.9. Ofrecer al usuario anular de forma segura una política DLP justificando transferencias de datos.

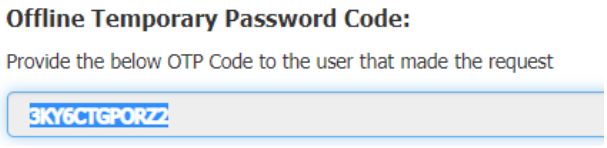
El agente de EPP permite al usuario solicitar una excepción de la política de protección basada en contenido durante un tiempo de terminado (desde 15 minutos hasta 30 días).



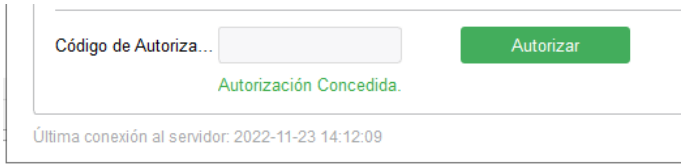
Esto simplemente genera un correo electrónico dirigido al administrador de EPP, indicando la justificación del acceso y el tiempo necesario. El administrador lo recibiría, y crearía una contraseña de un solo uso (OTP) en la sección Offline Temporary Password > Offline Temporary Password que remitiría al usuario:



Obtenemos el OTP en la interfaz de administración de EPP:



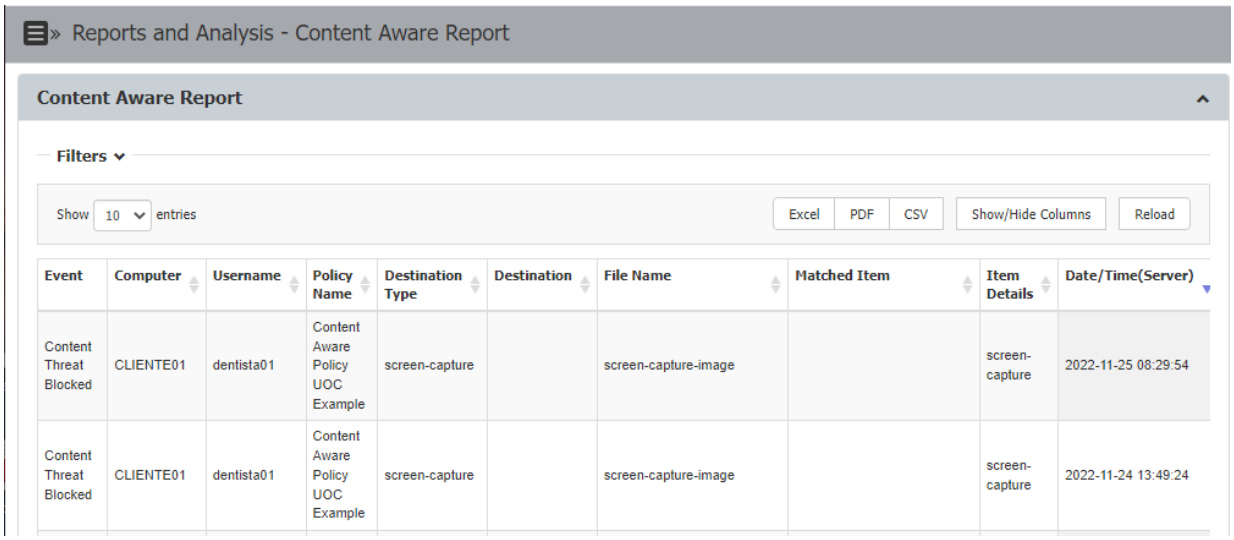
Tras introducirlo en el agente:



Una vez introducido, verificamos que sí podemos adjuntar un archivo a un correo de Gmail que anteriormente se había visto bloqueado. El inconveniente de esta configuración es que EPP no permite filtrar qué políticas o protecciones se deshabilitan, cuando autorizamos a un usuario a deshabilitar la protección, puede realizar cualquier tipo de acción.

PBC.10. Monitorizar la actividad relacionada con las políticas de protección basadas en contenido. Generar informes.

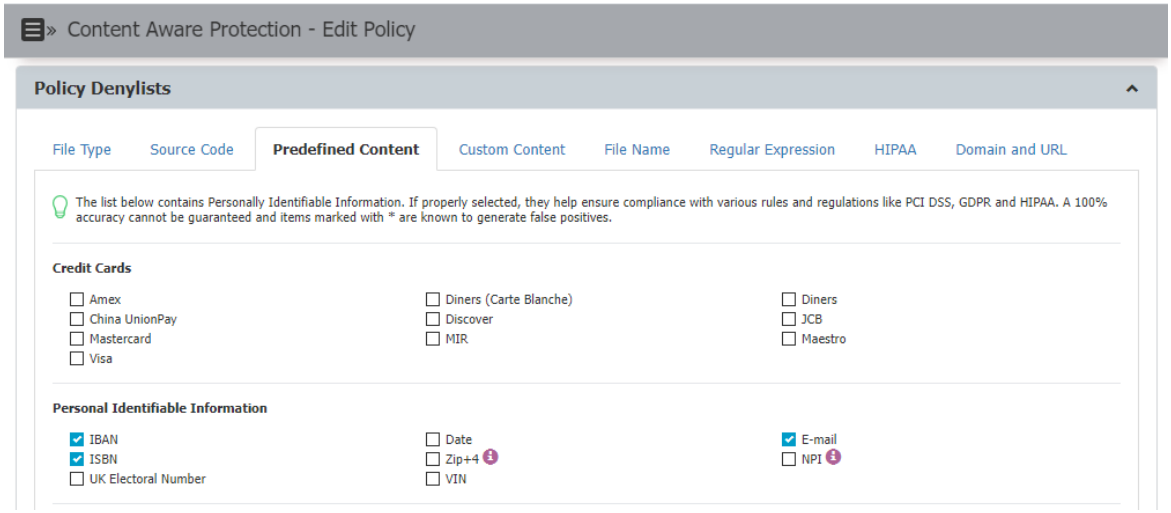
Como hemos ido viento a lo largo de los diferentes controles definidos, desde la sección Reports and Analysis > Content Aware Report, podemos revisar los eventos relacionados con las políticas de protección de contenido. EPP permite realizar diferentes filtros para acotar el listado de eventos. Los principales son el tipo de evento (amenaza detectada, bloqueada, remediación activa o cancelada por el usuario), equipo, ip principal, nombre de usuario, nombre de política, y fecha, aunque se puede llegar a un gran nivel de detalle filtrando por tipo de destino, nombre de fichero, y otros.



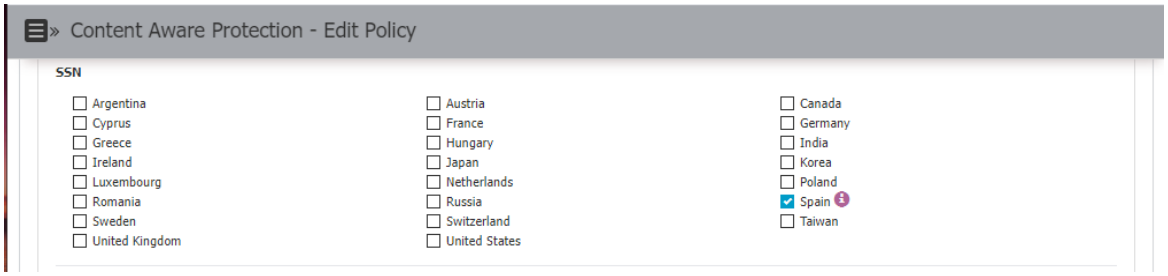
Estos eventos se pueden exportar en formato Excel, PDF o CSV. En el Anexo III se muestra un ejemplo de informe.

PBC.11. Cumplir con las normativas legales que apliquen (RGPD, HIPAA)

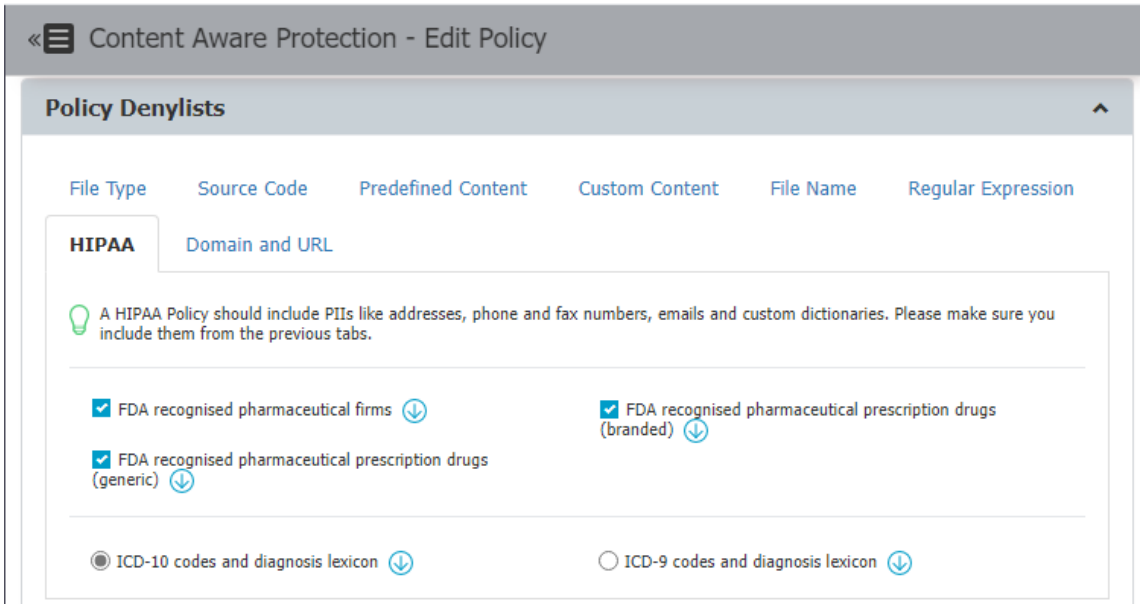
EPP proporciona contenido predefinido para realizar filtrado en las políticas de protección basadas en contenido. Este permite cumplir con diferentes normativas legales como RGPD o HIPAA:



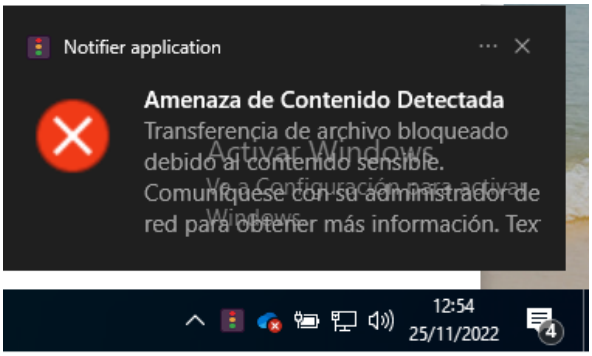
Como veíamos en el control PBC.2, podemos establecer también filtros por DNI y número de la seguridad social:



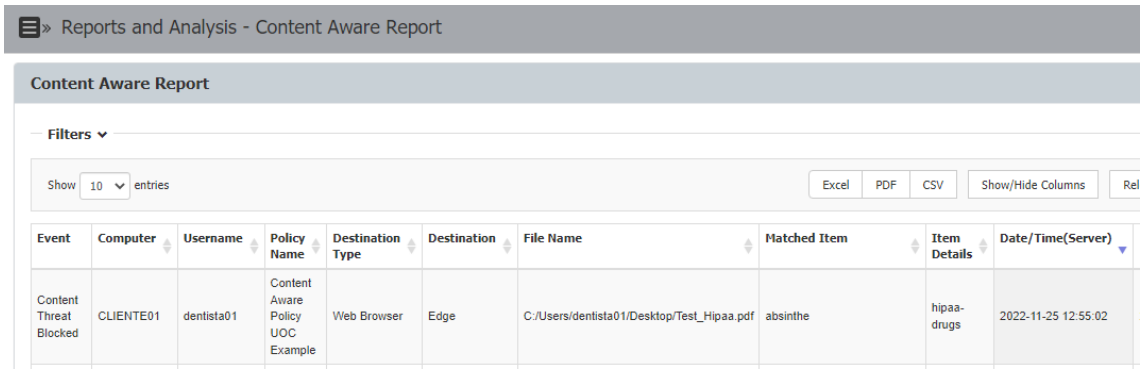
Finalmente, y aunque no es de aplicación en la Unión Europea, EPP incorpora diferentes diccionarios para filtrar contenido al que aplique la normativa HIPAA (Ley de Portabilidad y Responsabilidad de Seguros de Salud en Estados Unidos), tales como medicamentos, farmacéuticas, realizados por el FDA (Food and Drug Administration) y el ICD (International Classification of Diseases):



Evaluamos la política en un cliente intentando enviar por correo un archivo PDF que :



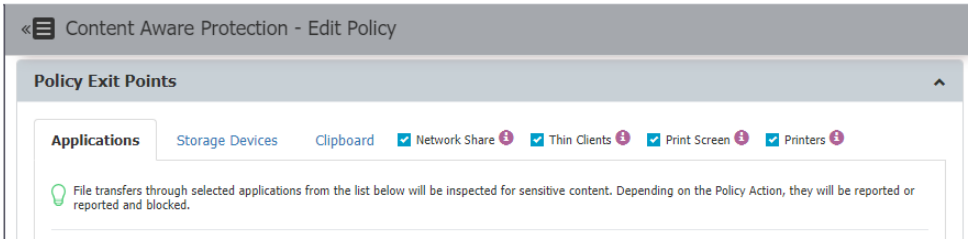
Confirmamos en la sección Reports and Analysis > Content Aware Report que la amenaza ha sido detectada y bloqueada:



PBC.12. Configurar políticas para limitar el uso de impresoras

Las políticas de protección basadas en contenido permiten definir diferentes puntos de salida por los que detectar y/o bloquear fugas de información. Para ello, en la definición de la política seleccionamos la opción *printers*.

El caso de uso establecido para esta política sería limitar la impresión de cualquier documento que contenga información confidencial fuera de horas. Para ello, marcaríamos la política de tipo Outside Hours.



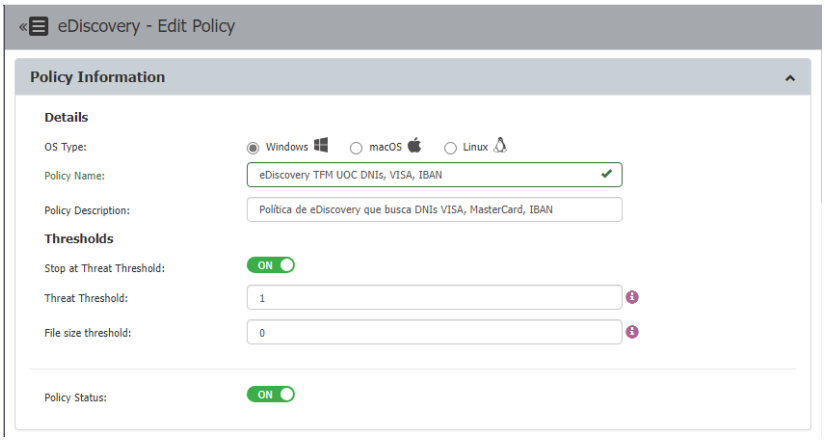
3.3.4. eDiscovery

Las políticas de protección basadas en eDiscovery son utilizadas para escanear los datos almacenados en clientes con el agente de EPP (Windows, MAC o Linux), de manera que se pueda forzar la política de almacenamiento de información confidencial, y gestionar los riesgos asociados a su exfiltración. La forma de mitigar esto es descubriendo información confidencial almacenada en reposo:

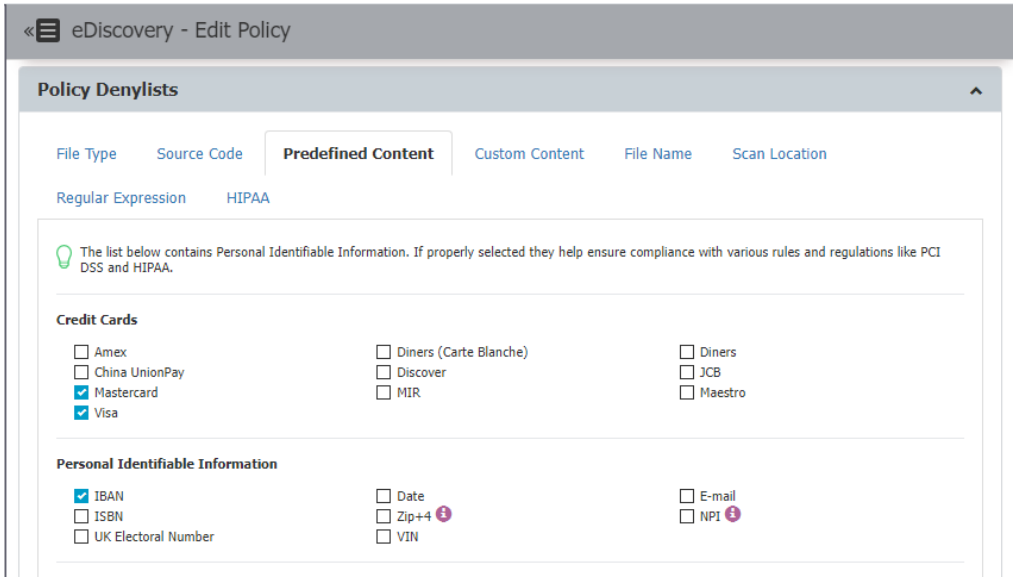
- **Datos personales (PII)**: números de seguridad social, documentos de identificación (DNI), números de pasaporte, direcciones de correo electrónico.
- **Información financiera o asociada a tarjetas de crédito**: números de tarjeta de crédito para VISA, MasterCard, American Express, JCB, o números de cuenta bancaria.
- **Ficheros confidenciales**: informes de ventas o marketing, documentos técnicos, contabilidad, bases de datos de clientes.

ED.1. Cifrado de datos en reposo que contengan información confidencial

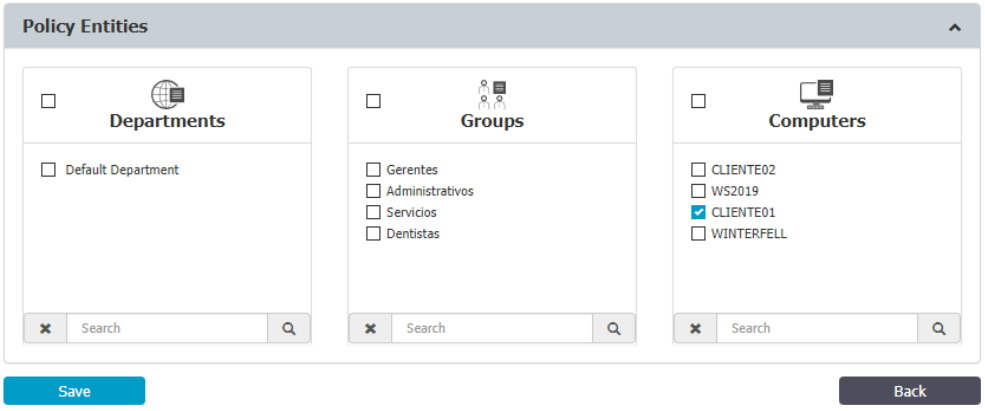
En la sección eDiscovery > Policies and Scans, podemos crear nuevas políticas de tipo eDiscovery. Creamos una política para clientes de tipo Windows:



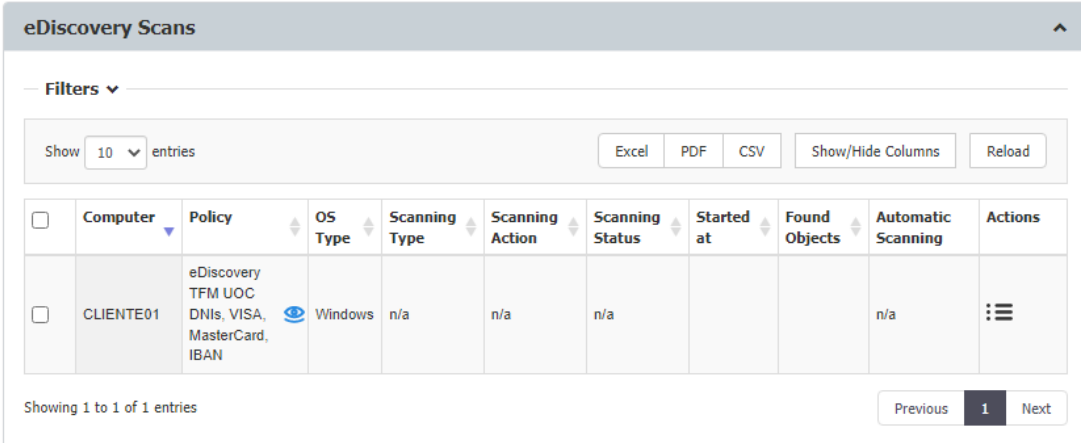
Configuramos la política para que localice DNIs, números de cuenta, números de tarjeta VISA y MasterCard:



Para evaluar la política la asignamos únicamente a uno de los clientes:

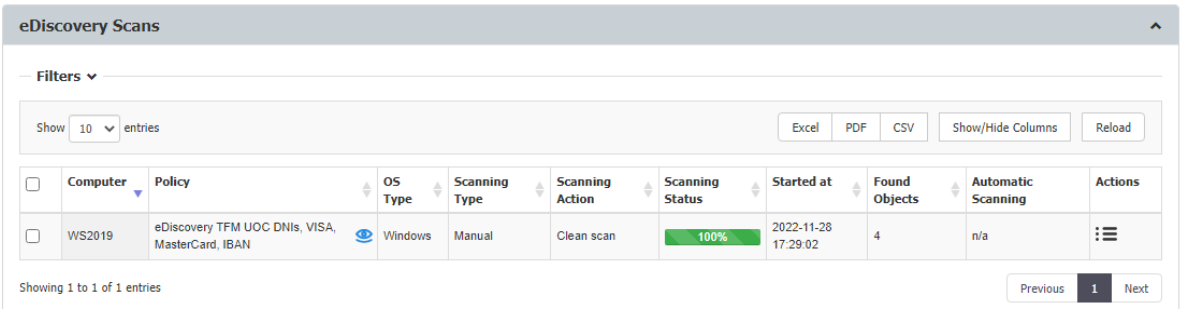


En esta misma sección, una vez guardamos la política de eDiscovery podemos ver un listado de las políticas guardadas y ejecutar acciones sobre ellas:

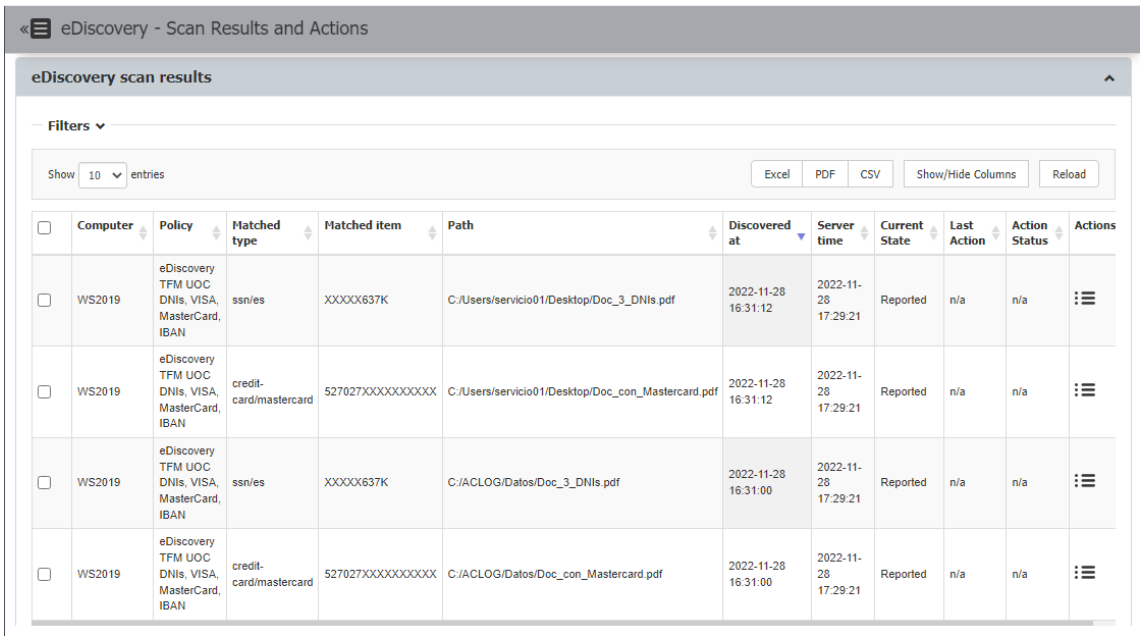


Ejecutamos el escaneo desde el menú actions > start clean scan. El escaneo no encuentra ningún resultado que viole la política de eDiscovery definida.

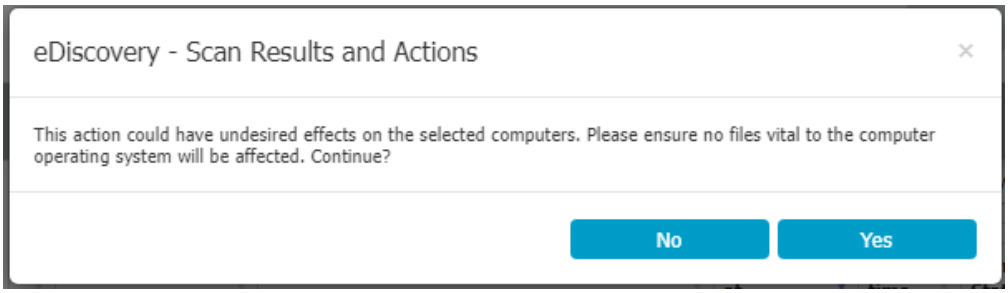
A continuación, modificamos la política para que escanee el servidor WS2019. Tras ejecutarla, vemos que encuentra cuatro objetos que la incumplen:



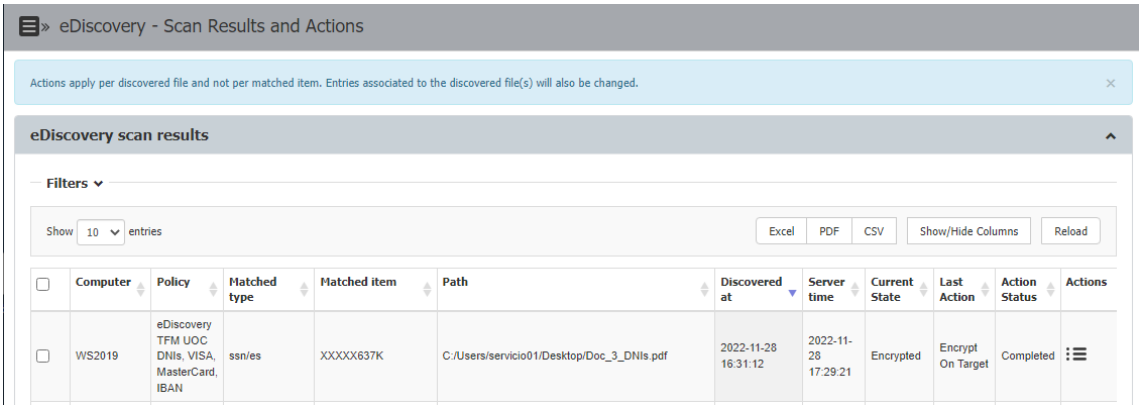
En la sección eDiscovery > Scan Results encontramos los objetos que violan la política de eDiscovery creada:



En el menú actions de cada objeto encontrado podemos ejecutar tres acciones: encriptar, desencriptar o eliminar en el objetivo. Para este caso de uso, seleccionamos la opción *Encrypt on target* para el primer objeto. El servidor de EPP muestra una advertencia:



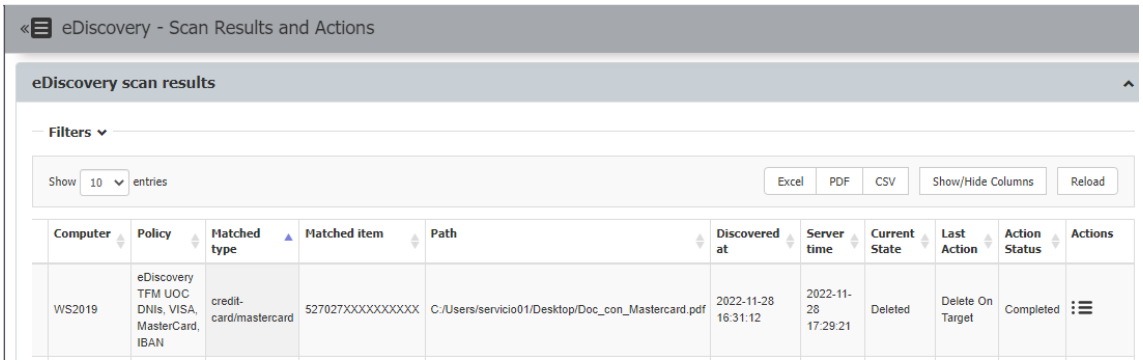
Tras aceptarlo, y esperar unos segundos, vemos que la acción es completada:



Se comprueba en el servidor WS2019 que el fichero es encriptado y renombrado a Doc_3_DNIs.pdf.epp_encrypted.

ED.2. Eliminar datos que supongan una violación de la política de seguridad en dispositivos finales

Siguiendo el ejemplo anterior, realizamos la acción *Delete on target* en el objeto encontrado con un número de tarjeta de crédito MasterCard:



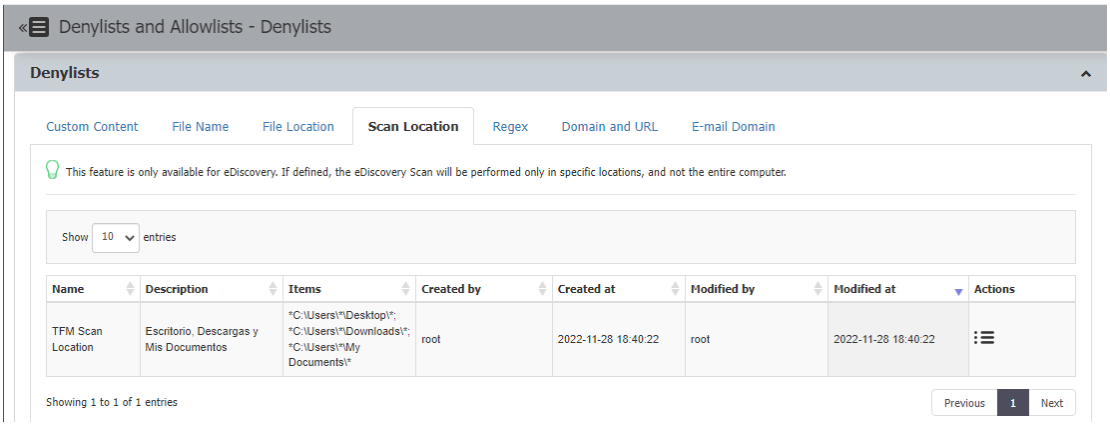
Se comprueba en el servidor WS2019 que el fichero es eliminado.

ED.3. Escanear rutas predefinidas como base, evitando el escaneo redundante de datos en reposo

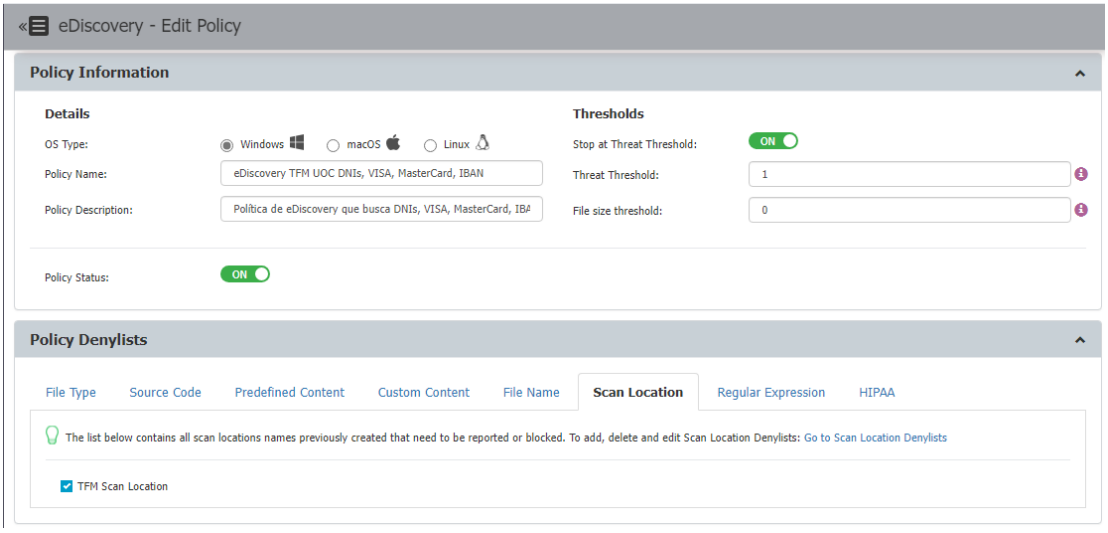
Si las ubicaciones donde pueden almacenar datos los usuarios están limitadas (escritorio, descargas, mis documentos), podemos crear una lista que defina dónde se realizará el escaneo. Para ello, en la sección Denylists and Allowlists > Denylists, desde la pestaña Scan Location creamos una nueva lista llamada TFM Scan Location que contiene las ubicaciones:

- *C:\Users*\Desktop*
- *C:\Users*\Downloads*

- *C:\Users*\My Documents*



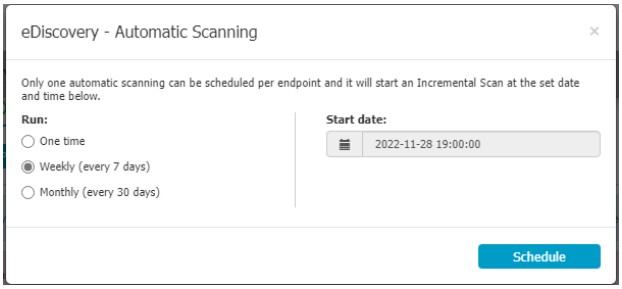
A continuación, podemos seleccionar esta ubicación en la política de eDiscovery creada:



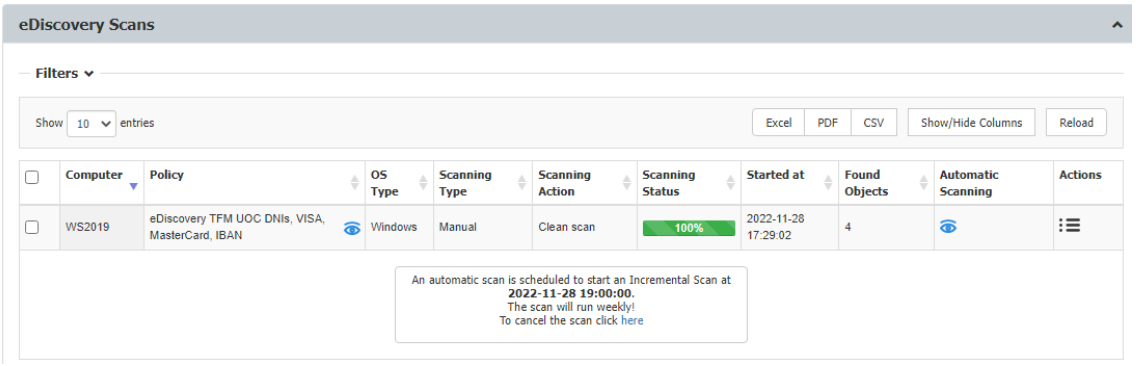
Esta configuración permite evitar el escaneo redundante y repetitivo de los diferentes ficheros del sistema operativo.

ED.4. Planificar escaneos automáticos periódicos

Los escaneos de eDiscovery pueden ser planificados de forma puntual, semanal o mensual. Para ello, en la sección eDiscovery > Policies and Scans, seleccionamos el cliente que queremos planificar en la tabla de escaneos, y seleccionamos Automatic scanning. Después seleccionamos la frecuencia deseada:

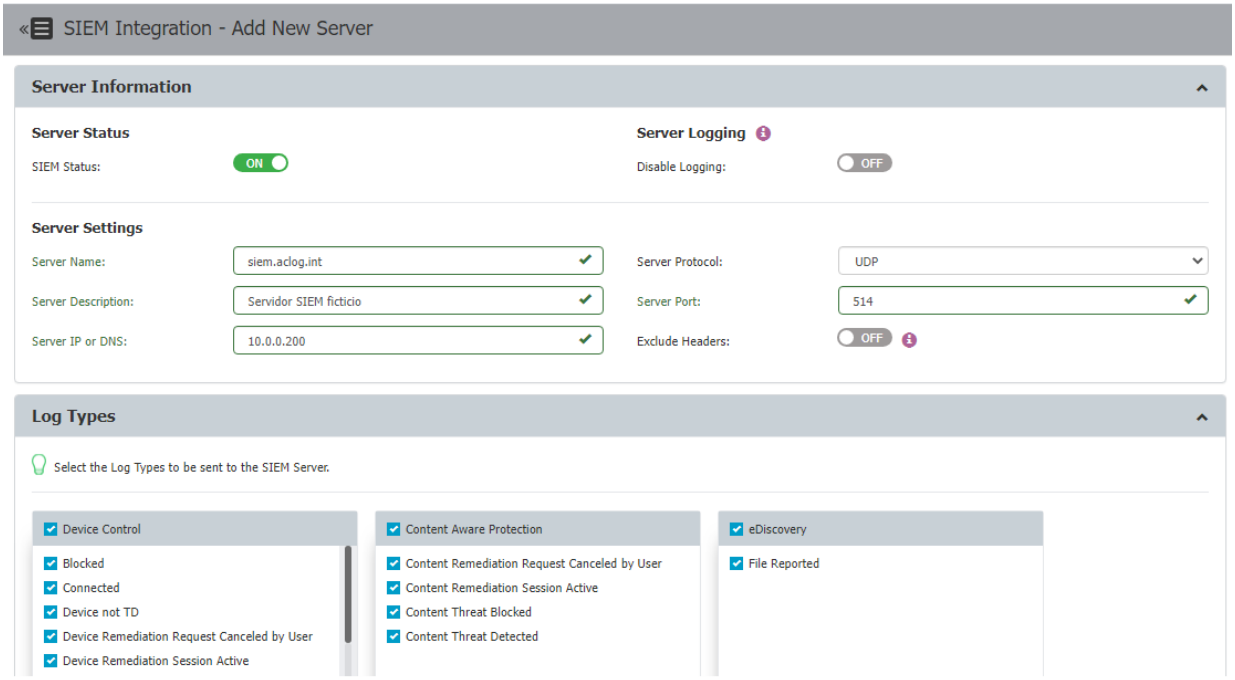


Comprobamos que el escaneo queda planificado:



ED.5. Ejecutar acciones tras escaneo. Exportar eventos a un SIEM

EPP permite integrar un SIEM al que exportar los diferentes eventos registrados en la herramienta. Esto se configura en la sección Appliance > SIEM Integration:

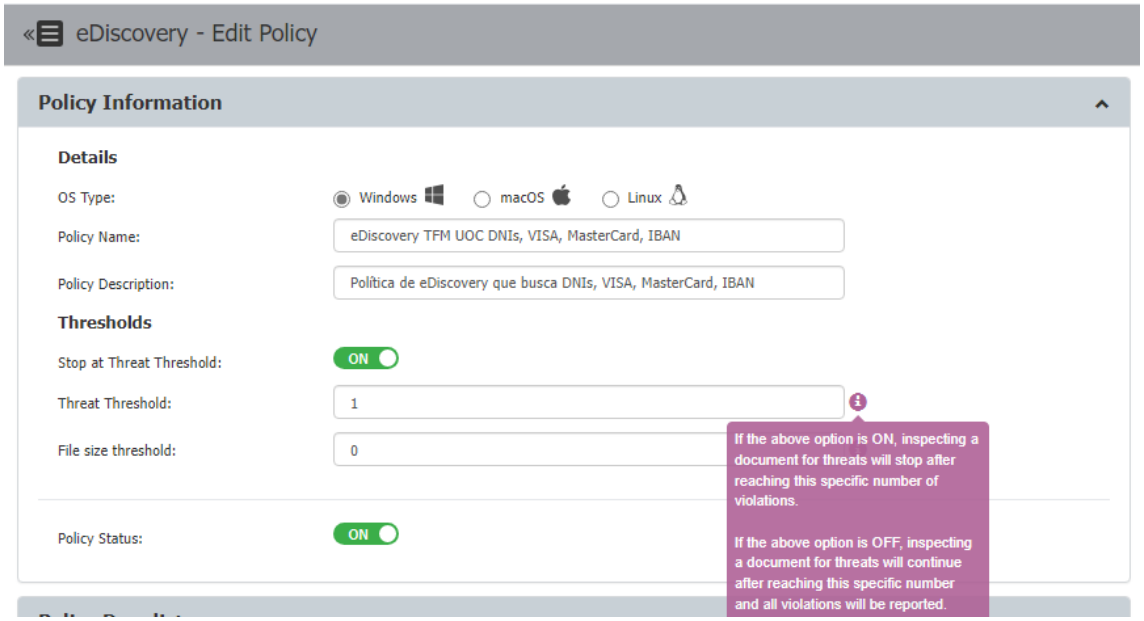


Con esta configuración, nos aseguramos de enviar a un servidor centralizado los eventos de EPP, pudiendo establecer correlaciones con otros eventos o definir alertas mediante un sistema corporativo.

EPP permite la configuración de hasta cuatro servidores SIEM, aunque en nuestro caso solo hemos integrado uno ficticio. La comprobación de recepción de eventos excede el alcance de este trabajo y no ha sido realizada.

ED.6. Limitar el número de violaciones que puede tener un archivo para que se aplique la política de seguridad y se notifique al servidor

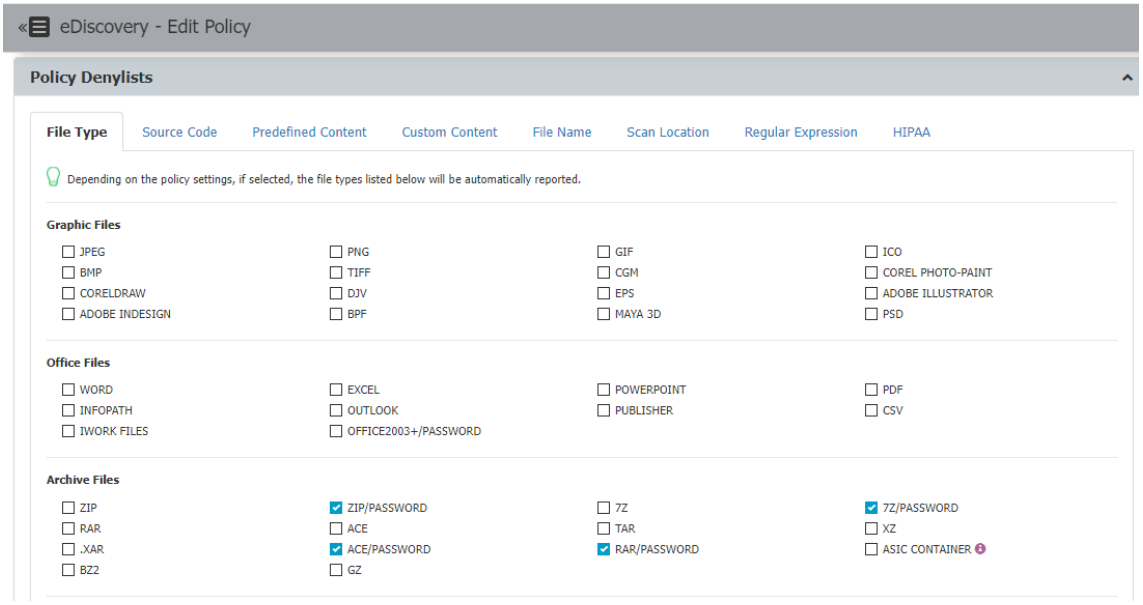
EPP permite configurar las políticas de eDiscovery para que se detenga la inspección de los archivos una vez se detecta el enésimo incumplimiento. Si elegimos detener la política, únicamente se reportará al servidor el primer incumplimiento identificado en el escaneo mediante la opción *Threat Threshold*:



Como vemos en la imagen, también se puede establecer un límite de tamaño para que sea reportado todo fichero que supere un determinado tamaño en MB (File size threshold).

ED.7. Bloquear documentos basándose en el tipo real del archivo

EPP permite excluir determinados tipos de fichero basándose en su extensión. Esto se configura a nivel de política de eDiscovery, en la sección Policy Denylists, pestaña File Type. El caso de uso aplicado a esta política es el de identificar ficheros comprimidos protegidos con contraseña:



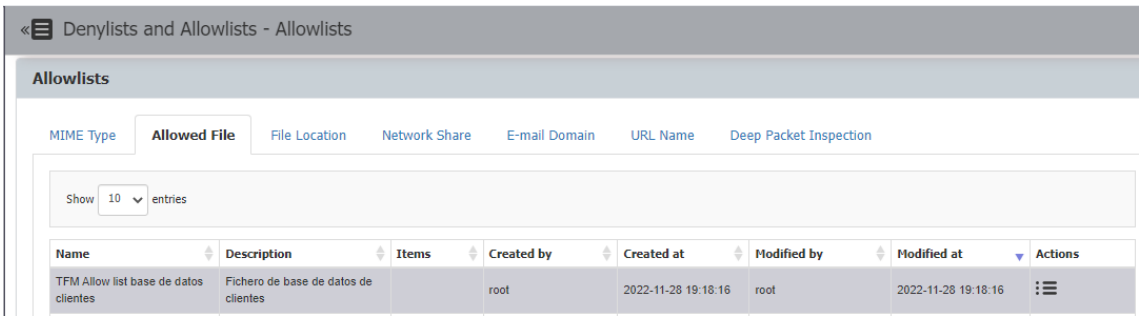
Para verificar la eficacia de esta política, incorporamos varios ficheros 7z en el servidor WS2019 y realizamos un escaneo incremental, siendo identificados:

Computer	Policy	Matched type	Matched item	Path	Discovered at	Server time	Current State
WS2019	eDiscovery TFM UOC DNIs, VISA, MasterCard, IBAN	7z	application/x-7z-compressed	C:/Users/servicio01/Desktop/Cloud.7z	2022-11-28 19:55:05	2022-11-28 20:36:33	Reported
WS2019	eDiscovery TFM UOC DNIs, VISA, MasterCard, IBAN	7z	application/x-7z-compressed	C:/Users/servicio01/Downloads/Test_7z_password.7z	2022-11-28 19:55:06	2022-11-28 20:36:33	Reported

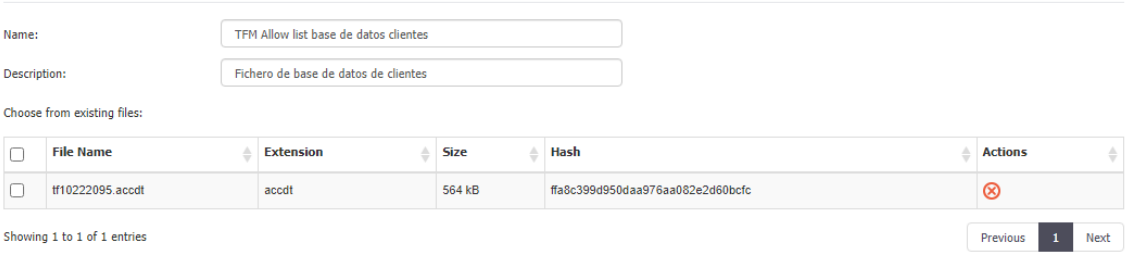
A partir de este escaneo, se podrían realizar las acciones que el administrador considerara oportunas.

ED.8. Excluir determinados archivos del escaneo para mejorar la productividad y rendimiento de la herramienta

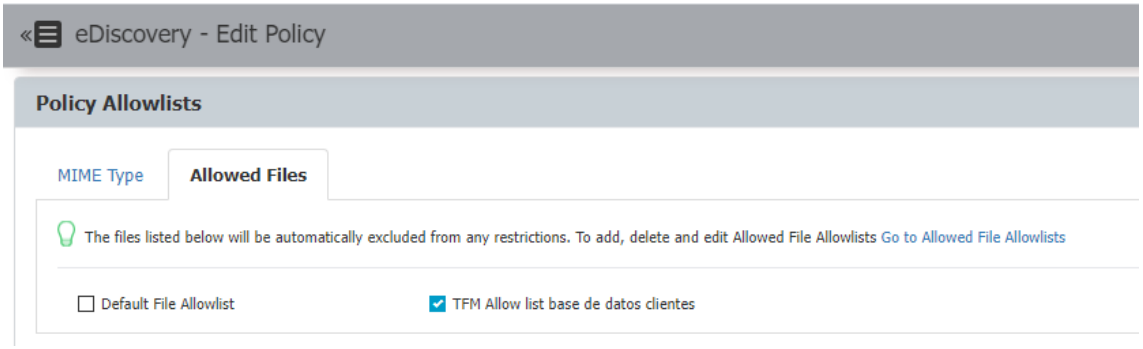
EPP permite crear listas de ficheros permitidos para los escaneos de eDiscovery. Esto es realizado desde la sección Denylists and Allowlists > Allowlists, definiendo un nuevo listado de Allowed File:



Al que hemos añadido el fichero de base de datos de clientes:

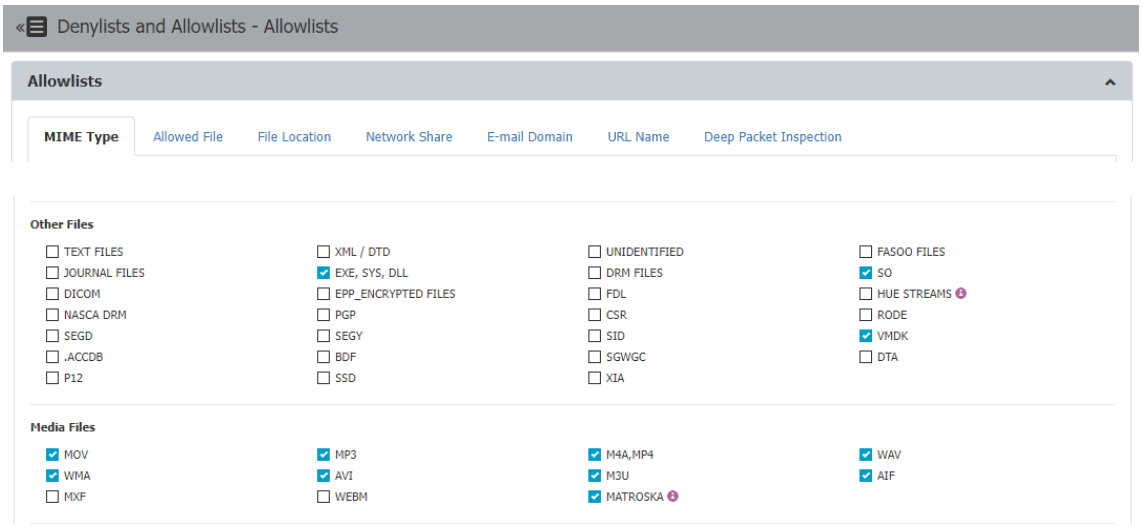


Posteriormente, se edita la política de eDiscovery y se incorpora en la sección de Policy Allowlists, en la pestaña Allowed files:

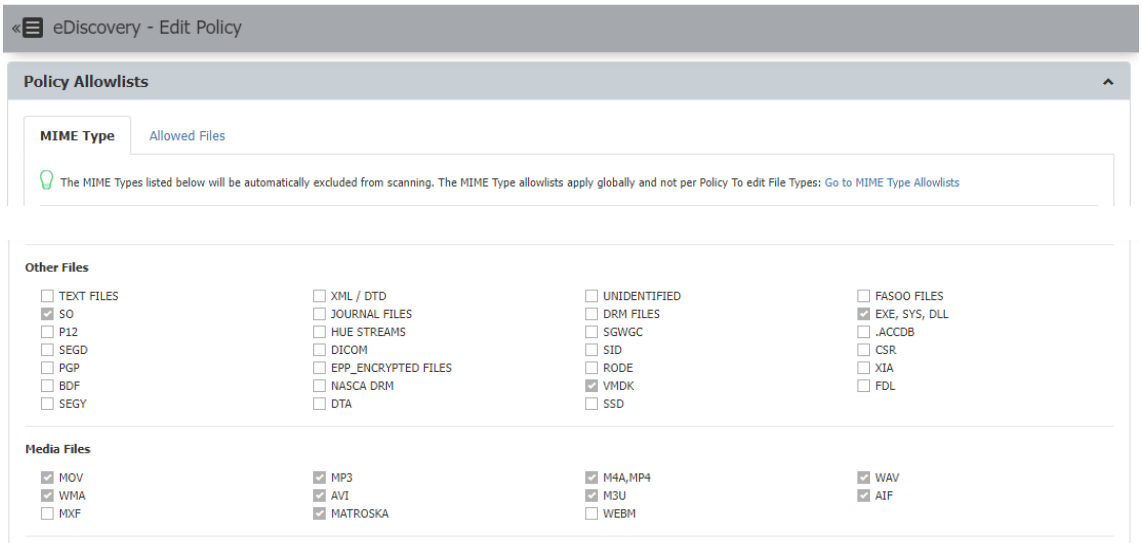


ED.9. Excluir determinados archivos según su tipo MIME del escaneo para mejorar la productividad y rendimiento de la herramienta

EPP permite excluir determinados archivos de los escaneos de eDiscovery desde la sección Denylists and Allowlists > Allowlists, en la pestaña MIME Type, y esta configuración aplica automáticamente a todas las políticas de eDiscovery. Establecemos como permitidos los ficheros de sistema operativo, ejecutables, audio, o vídeo.



Verificamos que en la política de eDiscovery se muestran asimismo como permitidos:



Con esta configuración aplicada, en los sucesivos escaneos de políticas de eDiscovery no se inspeccionarán los ficheros de este tipo.

3.4. Contextualización legal

3.4.1. Normativa

Se han de tener en cuenta los aspectos jurídicos y normativos en la ejecución de un proyecto de DLP, para que la implementación esté dentro de la legalidad y no se incurra en delitos por violación de la privacidad de los trabajadores. Es necesario analizar y considerar el marco legal que aplica en la relación laboral entre empleador y empleado, y los derechos y obligaciones que protegen los intereses de ambos.

De acuerdo con el Grupo de Trabajo del artículo 29 (GT Art.29) (2017), es importante tener en cuenta que el trabajador en raras ocasiones está en condiciones de dar, denegar o revocar el consentimiento a la aplicación de medidas técnicas de control, debido a la dependencia resultante de su relación con el empresario.

Por parte del empresario, existe un interés lícito para proteger la información corporativa, tal y como se ha analizado en los primeros capítulos del trabajo. Este se encuentra en su derecho de establecer medidas de protección, siempre que respeten la privacidad de los trabajadores y cumplan los principios de proporcionalidad y subsidiariedad.

Por tanto, los empresarios deben apoyarse en un fundamento jurídico diferente del consentimiento, y la utilización de una herramienta DLP debe estar justificada de forma que exista un equilibrio entre el respeto a la privacidad de los trabajadores, y los intereses

legítimos de la organización. Es vital señalar que, según el GT Art.29, las reglas establecidas para reportar o bloquear correos electrónicos o transferencias de archivos deben ser transparentes para los usuarios.

El empresario está amparado por la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, que define el secreto empresarial como "cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero […] y tenga un valor empresarial, ya sea real o potencial, precisamente por ser secreto, y haya sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto". El objetivo de esta ley es proteger a los titulares de datos empresariales (propiedad intelectual, conocimiento técnico, industrial, científico, comercial o financiero, entre otros) frente a la obtención o revelación de estos por parte de terceros no autorizados.

El derecho a la privacidad de los trabajadores se encuentra regulado en el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), el Estatuto de los trabajadores y la Constitución Española.

El RGPD define en el artículo 5 los principios generales para el tratamiento de datos, haciendo referencia al **principio de minimización de datos**:

> *b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines;*
>
> *c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»).*
>
> *e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales;*

El artículo 20 del Estatuto de los Trabajadores indica que "el empresario puede adoptar las medidas más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales", pero "guardando en su adopción y aplicación la consideración debida a su dignidad".

El artículo 87 de la LOPDGDD establece que "el empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos

efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos". Este además indica que "los empleadores deberán establecer criterios de utilización de los dispositivos digitales" que cumplan con las siguientes premisas:

- Que respeten, en todo caso, los estándares mínimos de protección de la intimidad del trabajador de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente.
- Que, en su elaboración, participen los representantes legales de los trabajadores.
- Que si se controlan dispositivos digitales respecto a los que el empresario ha admitido su uso con fines privados, se especifiquen los usos autorizados y se establezcan las garantías para preservar la intimidad de los trabajadores como, por ejemplo, los períodos en que los dispositivos pueden utilizarse para fines privados.

3.4.2. Propuesta de implantación

Para la implantación de este proyecto de DLP, se propone el siguiente plan de trabajo:

La gerencia debe elaborar y/o revisar la política de uso de los sistemas de información donde se establezcan las reglas de uso de los dispositivos, correo electrónico, e información corporativa. En el caso de la Clínica Dental, todos los dispositivos utilizados por los trabajadores son propiedad de la organización, y el trabajo se realiza de forma presencial. No se permite el uso de los dispositivos digitales con fines privados.

Se debe informar de forma transparente, mediante el envío de un correo y una sesión informativa con los trabajadores, sobre la necesidad de establecer medidas de protección, el funcionamiento de las soluciones DLP, y los controles establecidos dentro de la solución EPP. Se debe garantizar e informar de que estos controles no serán en ningún caso exhaustivos ni generalizados, al definirse sobre contenido sensible, determinados tipos de fichero, o establecer impedimentos técnicos en el movimiento de datos corporativos a dispositivos extraíbles.

¿Qué datos se van a proteger?

Datos especialmente sensibles:

- Números de la seguridad social y/o DNIs.
- Historiales médicos.
- Datos de tarjetas de crédito.

Datos de la empresa:

- Bases de datos de clientes.
- Bases de datos de Recursos Humanos.
- Información económica de la Clínica.
- Información relacionada con campañas de marketing.

Tal y como exige el RGPD, se debe elaborar un Registro de datos que identifique dónde se almacena la información y quién tiene acceso a ella.

Se debe realizar una evaluación de impacto de la protección de datos personales (EIPD), que permita evaluar los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con ellos.

Se deben evaluar los controles en modo informe/advertencia antes de que se configuren en modo bloqueo, de manera que se verifique su efectividad y supongan la menor intrusión posible.

Se deben valorar mecanismos de prevención que sean igualmente eficaces, pero sean menos intrusivos para los usuarios: por ejemplo, se deberán revisar los roles y permisos de los usuarios para garantizar que estos no tienen acceso a más datos de los necesarios, y que siempre se cumple el principio de mínimo privilegio.

El acceso a los registros derivados del uso de los dispositivos debe ser confidencial y restringido al mínimo número de personas: únicamente deberán acceder a ellos los responsables de Gerencia y Servicios.

Finalmente, y de acuerdo con la AEPD, se debe establecer un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento de los datos generados a partir de la implantación de la herramienta de DLP.

3.4.3. Otras consideraciones

La pandemia mundial de la COVID-19 ha potenciado en el sector laboral nuevas formas de trabajar, que impactan de manera significativa en los riesgos a los que se enfrentan las empresas, en las medidas de control que estas deben implantar para garantizar la confidencialidad de sus datos, y por ende, en los aspectos legales que pueden afectar a la privacidad de los trabajadores.

Teletrabajo: cada vez más empleados prestan sus servicios de forma remota, desde el exterior de las sedes corporativas, por regla general desde el domicilio. Los riesgos que se presentan pueden ser mayores o menores dependiendo de si el empleado utiliza un dispositivo corporativo para trabajar, o lo hace mediante sus propios medios.

BYOD: (*Bring Your Own Device*). Las empresas permiten a los empleados utilizar, de forma voluntaria, sus dispositivos personales (portátiles, terminales móviles, tabletas, etc.), para acceder a recursos corporativos como el correo electrónico, o realizar algunas labores propias de su puesto de trabajo.

Ambas tendencias requieren de la implantación de medidas técnicas que prevengan la fuga de datos, y de la consideración de los aspectos legales que garanticen la privacidad de los trabajadores.

Tal y como señala la AEPD (2021), se debe definir una política de protección de la información para situaciones de teletrabajo, que se base a su vez en la política de protección de datos de la entidad y forme parte de ella. Se debe prestar especial atención al perfilado de dispositivos que pueden acceder a la red interna, y a los recursos accesibles por parte de los empleados.

En el ordenamiento jurídico, la Ley 10/2021, de 9 de julio, de trabajo a distancia recoge los derechos y obligaciones que deben cumplir empresario y trabajador dentro de esta modalidad. En ella se presenta el "Acuerdo de Teletrabajo", y en él se recuerda el cumplimiento de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen y de forma general a los principios y garantías de protección de datos de carácter personal.

De esta ley, cabe destacar también que "*las empresas estarán obligadas a dotar de los medios, equipos, […] que exige el desarrollo del trabajo a distancia.*"

3.5. Valoración económica

Para obtener la valoración total del proyecto se han de agregar los costes de infraestructura, licencias software, y servicios profesionales para el despliegue de la herramienta. Estos servicios deben incluir el análisis de la información confidencial a proteger, el análisis del comportamiento de los usuarios y la implementación de los controles específicos acordados con la dirección de seguridad.

Se presentan a continuación de forma agregada los mismos:

Concepto	Descripción	Coste unitario	Coste total
Infraestructura	Máquina virtual de EPP en un clúster de alta disponibilidad con almacenamiento compartido. (300 GiB)	-	2.500 €
Licencias	Licencias EPP. Paquete mínimo 150 licencias.	40 €	6.000 €
Servicios profesionales	Consultoría e implementación de proyecto DLP. Estimación 20 jornadas.	480 €	9.600 €
TOTAL			31.300 €

Tabla 9. Valoración económica (Elaboración propia)

4. Resultados

Tras la realización del trabajo, se han alcanzado los siguientes resultados:

- Se ha realizado una revisión del estado del arte en materia de soluciones DLP: se han descrito los principales tipos y sus características generales, se han detallado sus funcionalidades técnicas, y cómo estas pueden ayudar a cumplir los objetivos de prevención de fugas de información que pueda tener una organización interesada en implementar un proyecto de este tipo.
- Se ha realizado un análisis comparativo de la principales soluciones DLP comerciales, fundamentado en fuentes confiables de referencia en el sector tecnológico (Gartner), los propios fabricantes, y analistas independientes.
- Se ha realizado una guía de implementación de la solución CoSoSyS Endpoint Protector, se han detallado sus métodos de despliegue, puesta en marcha y configuración inicial para desarrollar el trabajo. Se han definido e implementado un conjunto de controles de seguridad desplegados en un entorno de laboratorio, que ponen en valor las capacidades de la solución, fácilmente aplicables a una Clínica Dental de ejemplo.
- Se ha analizado el marco legal de interés para la implantación de un proyecto DLP, se han identificado las principales leyes que son de aplicación, su contenido, y se ha emitido un conjunto de recomendaciones que deben servir como guía a una organización que realice un proyecto de este tipo.

5. Conclusiones

5.1. Balance del grado de consecución de objetivos

En el presente trabajo se ha conseguido el objetivo general de evaluar el uso de una solución de seguridad que prevenga la fuga y pérdida de datos en una clínica dental, a través de la herramienta DLP Endpoint Protector de CoSoSys. En línea con los resultados obtenidos, cabe destacar lo siguiente:

Se ha justificado la necesidad de instalar una herramienta DLP en una organización definiendo los diferentes riesgos y amenazas a las que esta se enfrenta, y los casos de uso típicos en los que una herramienta de este tipo puede ofrecer soluciones técnicas que disminuyan el riesgo de fuga de datos.

Se ha expuesto el funcionamiento general de las herramientas DLP, clasificándolas y explicando los diferentes niveles de protección que pueden ofrecer en las organizaciones. Para ello, se han analizado y comparado las principales herramientas DLP en el mercado, seleccionando Endpoint Protector (EPP) de CoSoSys para el desarrollo del Trabajo.

La implantación de la solución EPP en un entorno de pruebas se ha realizado con éxito, permitiendo la evaluación de los controles de seguridad definidos a lo largo del trabajo. Se han mostrado diferentes casos de uso donde la herramienta ha funcionado tal y como se esperaba: han quedado patentes sus grandes capacidades para establecer políticas de control que impiden la fuga de datos y funcionan de forma real, verificando como estas se aplicaban a usuarios independientemente de en qué equipo hubiera iniciado sesión (políticas asignadas a usuarios/grupos de usuarios), o a equipos, independientemente de qué usuario hubiera iniciado sesión en él (políticas asignadas a equipos/grupos de equipos).

Finalmente, se ha establecido el contexto legal de interés para una organización que implementa un proyecto de este tipo, debido a los riesgos que aparecen con el establecimiento de controles. Merece la pena señalar que las políticas de control de dispositivos no suponen un riesgo para la privacidad de los trabajadores, pero hay que prestar especial atención a las políticas basadas en contenido, que pueden interceptar comunicaciones personales. Para mitigar este riesgo se proporcionan un conjunto de recomendaciones que deben acompañar al proyecto de implantación tecnológica.

5.2. Reflexión crítica sobre el trabajo realizado

A nivel personal, el Trabajo Final de Máster es el culmen a un periodo de algo más de un año cursando el Máster de Ciberseguridad y Privacidad. El nivel de conocimiento de partida en cuanto soluciones de este tipo era bajo, aunque se ha encontrado una cantidad notable de documentación en repositorios institucionales, analistas independientes, y publicada por los propios fabricantes de tecnologías DLP. No se han encontrado grandes dificultades en la implantación de la herramienta y la evaluación de los controles en el laboratorio controlado, si bien es cierto que un proyecto de este tipo habría tenido unos resultados mucho más cercanos a la realidad en el caso de poder implantarse en un entorno corporativo. Esto no ha sido posible por no haber conseguido que ninguna organización se preste a evaluar la herramienta en su infraestructura, sin embargo, considero que sí se ha ilustrado el funcionamiento general de las soluciones DLP, y de manera concreta, proporcionar una guía de implantación para EPP que cubre la mayor parte de sus funcionalidades.

Las mayores dificultades las he encontrado en el análisis y redacción de los aspectos legales que afectan a un proyecto de este tipo, debido al amplio espectro de leyes y normas existentes, y al elevado volumen de cambios que se han producido a nivel legal en los últimos cinco años: entrada en vigor de RGPD, LOPDGDD, etc. A diferencia de los aspectos técnicos, que en la mayoría de las ocasiones funcionan o no de forma binaria, los aspectos normativos deben ser interpretados y adaptados según el escenario concreto en el que se trabaje. No obstante, considero adecuada la contextualización realizada, y las recomendaciones proporcionadas podrían servir como punto de partida a una organización que se enfrente a un proyecto como este.

5.3. Propuestas de mejora y líneas de trabajo futuras

La principal propuesta de mejora para el presente trabajo es llevarlo a la práctica en un entorno real, de manera que se puedan evaluar sus resultados, y mediante la retroalimentación obtenida se puedan ajustar las diferentes políticas.

Como líneas de trabajo futuras, se podrían seguir explorando las soluciones DLP de tipo Network y Cloud, con el objetivo de monitorizar y proteger las fugas de información desde un punto diferente al puesto cliente, en el que se ha enfocado este trabajo.

Las soluciones Network DLP se centran en la protección de la información en tránsito que viaja por la red de las organizaciones. Un subconjunto de estas soluciones son las Cloud DLP, cuyo objetivo específico es proteger de fugas de datos almacenadas o procesadas en servicios de nube.

6. Glosario

API

Application Programming Interface. Conjunto de definiciones y protocolos utilizados para desarrollar integrar el software de una aplicación.

CASB

Cloud Access Security Broker. Es un punto de imposición de políticas de seguridad, ya sea en las instalaciones físicas o en la nube, situado entre los consumidores de servicios en la nube y los proveedores de servicios en la nube, cuyo propósito es combinar e interponer políticas de seguridad corporativas cuando se acceda a los recursos en la nube.

Confidencialidad

Propiedad que garantiza que los datos solo son accedidos por los usuarios autorizados.

Datos

Activo de valor incalculable para cualquier organización, su pérdida puede suponer graves problemas legales, reputacionales, y/o competitivos.

Disponibilidad

Propiedad que garantiza que los sistemas de información están accesibles para los usuarios siempre que los necesiten.

DLP

Proceso de seguridad que tiene como objetivo prevenir la fuga o robo de información corporativa.

EDR

Acrónimo de *Endpoint Detection and Response*. Solución de seguridad que monitoriza continuamente un equipo para ofrecer detección de amenazas en tiempo real y respuesta a las mismas.

File Shadowing

Característica que permite al servidor de DLP almacenar una copia de un fichero transferido al exterior por un usuario a través de un dispositivo extraíble, almacenamiento en nube o correo

Integridad

Propiedad que garantiza que los datos no son modificados por usuarios no autorizados.

Lista blanca

Lista de objetos que obtienen algún privilegio por el mero hecho de encontrarse en ella

Lista negra

Lista de objetos que deben ser discriminados de algún modo de otros que no están en la lista.

RTO

*Recovery Time Objective. T*iempo máximo que puede transcurrir desde un fallo en un servicio o sistema hasta su recuperación

SaaS

Software as a Service. Modalidad de consumo en la nube donde el cliente consume un determinado producto ofrecido por un proveedor, siendo este último responsable de la infraestructura física, sistema operativo y aplicación.

SIEM

Security and Information Event Management. Sistema de seguridad que tiene como objetivo la centralización de registros de seguridad con fines de análisis, envío de alertas de seguridad, auditoría o análisis forense.

SIEM

Acrónimo de *Security Information and Event Management.* Sistemas de seguridad que centralizan la gestión de eventos, con capacidad de correlacionar los mismos y poder generar alertas. También son utilizados para poder reconstruir incidentes de seguridad.

UEBA

Acrónimo de *User and Entity Behavior Analytics,* Analítica de comportamiento de usuarios y entidades, utilizado para mejorar la predicción del comportamiento de los usuarios y detectar anomalías que puedan suponer riesgos de seguridad.

7. Bibliografía

Agencia Española de Protección de Datos. (2021). *Teletrabajo y protección de datos en el ámbito digital.* Recuperado el 12 de diciembre de 2022, de https://www.aepd.es/es/prensa-y-comunicacion/blog/teletrabajo-y-pd-en-el-ambito-digital

Computer World. (2022). *Broadcom define la futura andadura junto con VMware*. Recuperado el 1 de noviembre de 2022, de https://www.computerworld.es/empresas/broadcom-define-la-futura-andadura-junto-con-vmware

CoSoSys. (s.f.a). *Hoja de datos 5.5.0. Solución de Prevención de Pérdida de Datos (DLP) Líder en la Industria*. Recuperado el 15 de octubre de 2022, de https://www.endpointprotector.com/support/pdf/datasheet/Data_Sheet_Endpoint_Protector_5_CoSoSys_ES.pdf

CoSoSys. (s.f.b). *How to setup a Data Loss Prevention in less than 30 days*. Recuperado el 25 de octubre de 2022, de https://www.endpointprotector.com/white_papers/Endpoint-Protector-Guide-How-to-setup-a-DLP-in-less-than-30-days-EN.pdf

Crowdsrike. (2022). *What is Data Loss Prevention (DLP)?*. Recuperado el 2 de octubre de 2022, de https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/

De Groot, J. (2022). *What is Data Loss Prevention (DLP)? Definition, Types & Tips*. Recuperado el 2 de octubre de 2022, de https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

Dictamen 2/2017 sobre el tratamiento de datos en el trabajo. (2018). Grupo de trabajo sobre la protección de datos del Artículo 29. https://www.aepd.es/es/documento/wp249es.pdf

Digital Guardian. (s.f.). *Digital Guardian Technical Overview*. Recuperado el 2 de noviembre de 2022, de https://info.digitalguardian.com/rs/768-OQW-145/images/digital-guardian-technical-overview.pdf

Gartner (2017). *Magic Quadrant for Enterprise Data Loss Prevention*. Recuperado el 22 de octubre de 2022, de https://www.gartner.com/document/3606038

Gartner (2018). *Market Guide for Data Loss Prevention*. Recuperado el 22 de octubre de 2022, de https://www.gartner.com/document/code/349685

Gartner (2021). *Market Guide for Data Loss Prevention*. Recuperado el 23 de octubre de 2022, de https://www.gartner.com/document/code/742074

Haller, K. (2014). *When data is a risk*. Recuperado el 11 de octubre de 2022, de http://www.klaushaller.net/wp-content/uploads/2013/03/07_haller_dlp_usenix.pdf

INCIBE. (2017). *Insider, las dos caras del empleado*. Recuperado el 30 de septiembre de 2022, de https://www.incibe-cert.es/blog/insider-las-dos-caras-del-empleado

INCIBE. (2019). *DLP protege tus datos contra fugas de información*. Recuperado el 30 de septiembre de 2022, de https://www.incibe.es/protege-tu-empresa/blog/dlp-protege-tus-datos-fugas-informacion

Imperva (s.f.). Data Loss Prevention (DLP). Recuperado el 1 de octubre de 2022, de https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado, 294*, de 6 de diciembre de 2018, pp. 119788-119857. https://www.boe.es/eli/es/lo/2018/12/05/3/dof/spa/pdf

Ley 1/2019, de 20 de febrero, de Secretos Empresariales. *Boletín Oficial del Estado, 45*, de 21 de febrero de 2019, pp. 16713-16727. https://www.boe.es/boe/dias/2019/02/21/pdfs/BOE-A-2019-2364.pdf

Ley 10/2021, de 9 de julio, de trabajo a distancia. *Boletín Oficial del Estado, 164*, de 10 de julio de 2021, pp. 82540-82583. https://www.boe.es/boe/dias/2021/07/10/pdfs/BOE-A-2021-11472.pdf

Lord, N. (2022). *Data Protection: Data In transit vs. Data At Rest*. Recuperado el 4 de septiembre de 2022, de https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest

McAfee. (2017). *McAfee DLP Versions: Feature Comparison Chart*. Recuperado el 30 de octubre de 2022, de https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-dlp-comparison.pdf

McAfee. (2020). *Mcafee Data Loss Prevention Endpoint. Ficha técnica*. Recuperado el 30 de octubre de 2022, de https://www.mcafee.com/enterprise/es-es/assets/data-sheets/ds-dlp-endpoint.pdf

Netskoe (s.f.). ¿Qué es un Cloud Access Security Broker (CASB)? Recuperado el 15 de noviembre de 2022, de https://www.netskope.com/es/security-defined/what-is-casb

Rabbaglio, M. (2022). *Data Loss Prevention: Tools and Recommendations for Companies*. Recuperado el 1 de octubre de 2022, de https://www.boolebox.com/data-loss-prevention-tools-for-companies/

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. *Boletín Oficial del Estado, 255*. https://www.boe.es/buscar/pdf/2015/BOE-A-2015-11430-consolidado.pdf

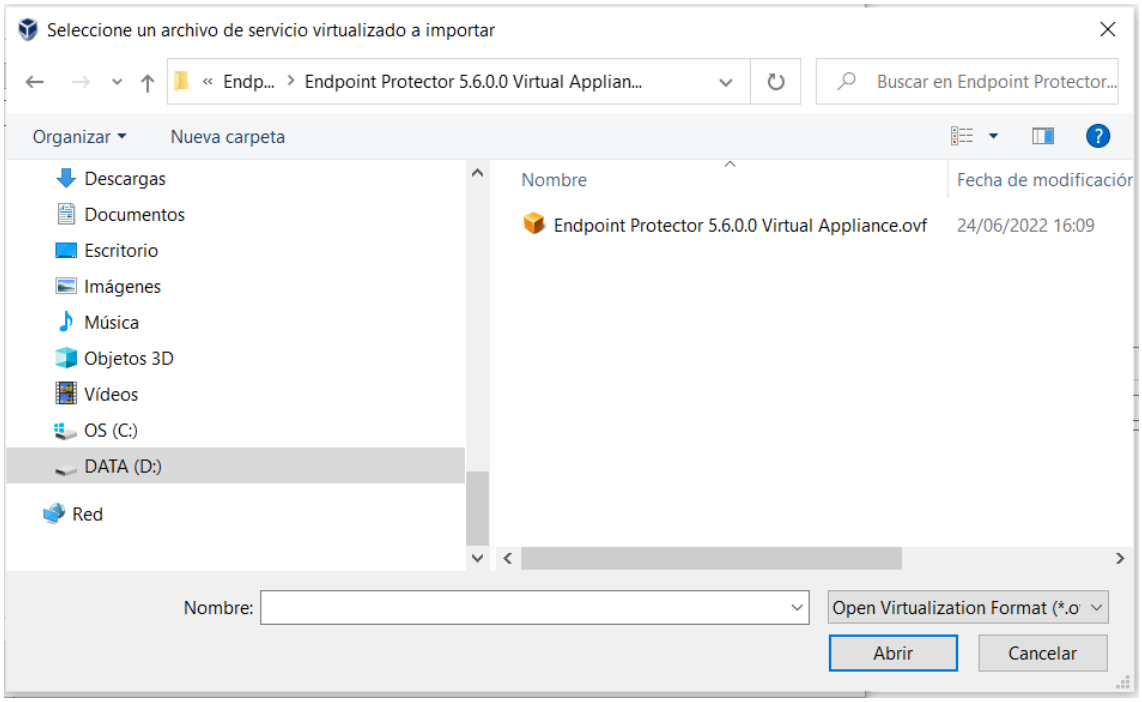
Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea.* https://www.boe.es/doue/2016/119/L00001-00088.pdf

Symantec. (2022). *Symantec Data Loss Prevention Product Brief.* Recuperado el 1 de noviembre de 2022, de https://docs.broadcom.com/doc/data-loss-prevention-family-en

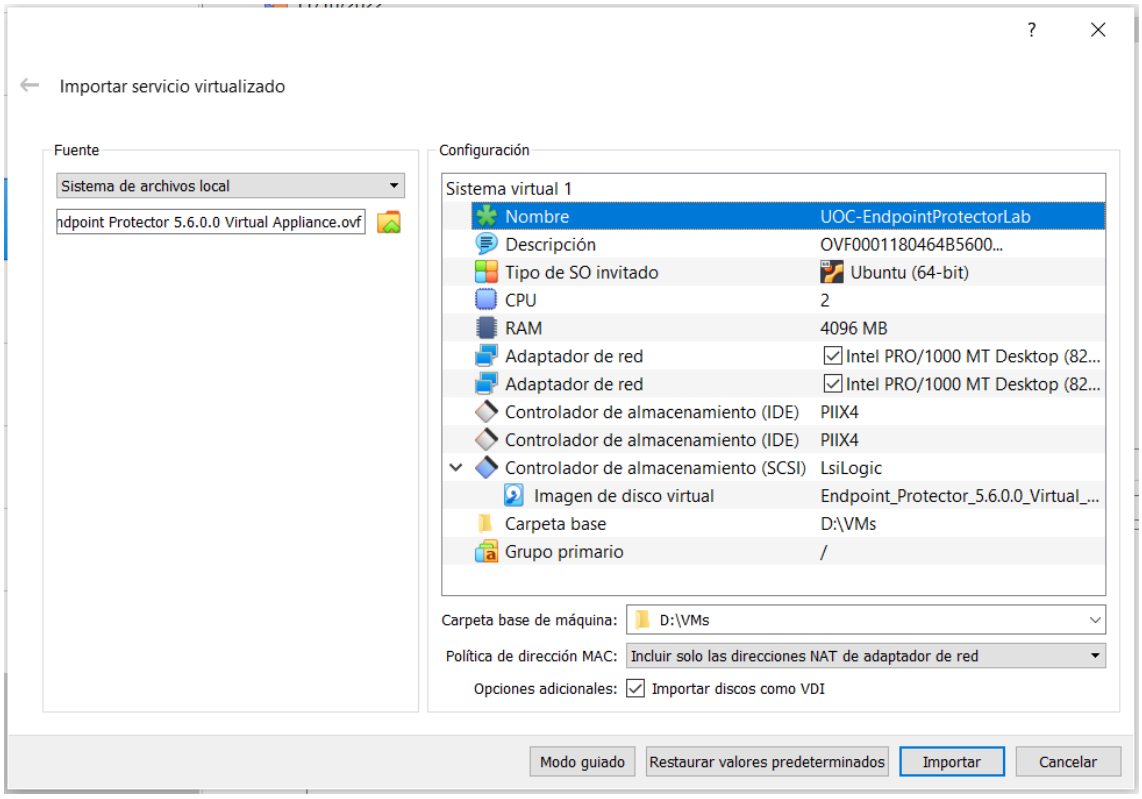
8. Anexos

Anexo I. Despliegue de appliance Endpoint Protector

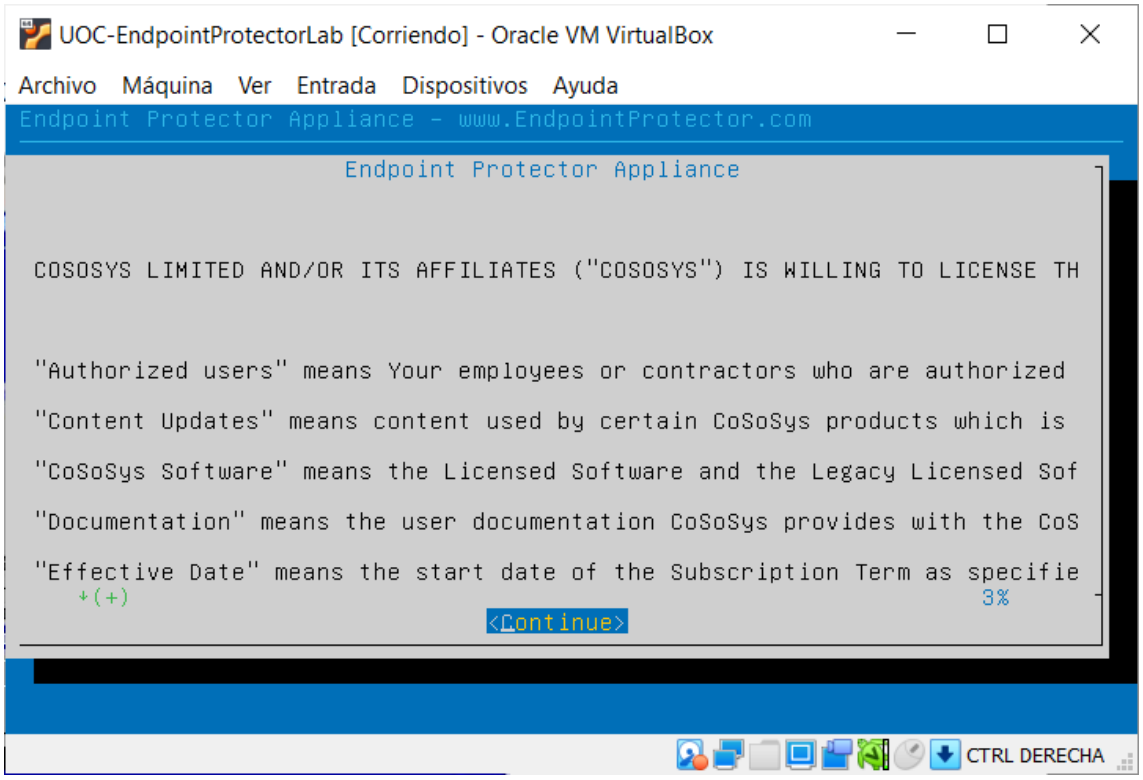
1. Importamos el servicio virtualizado en Oracle VirtualBox:

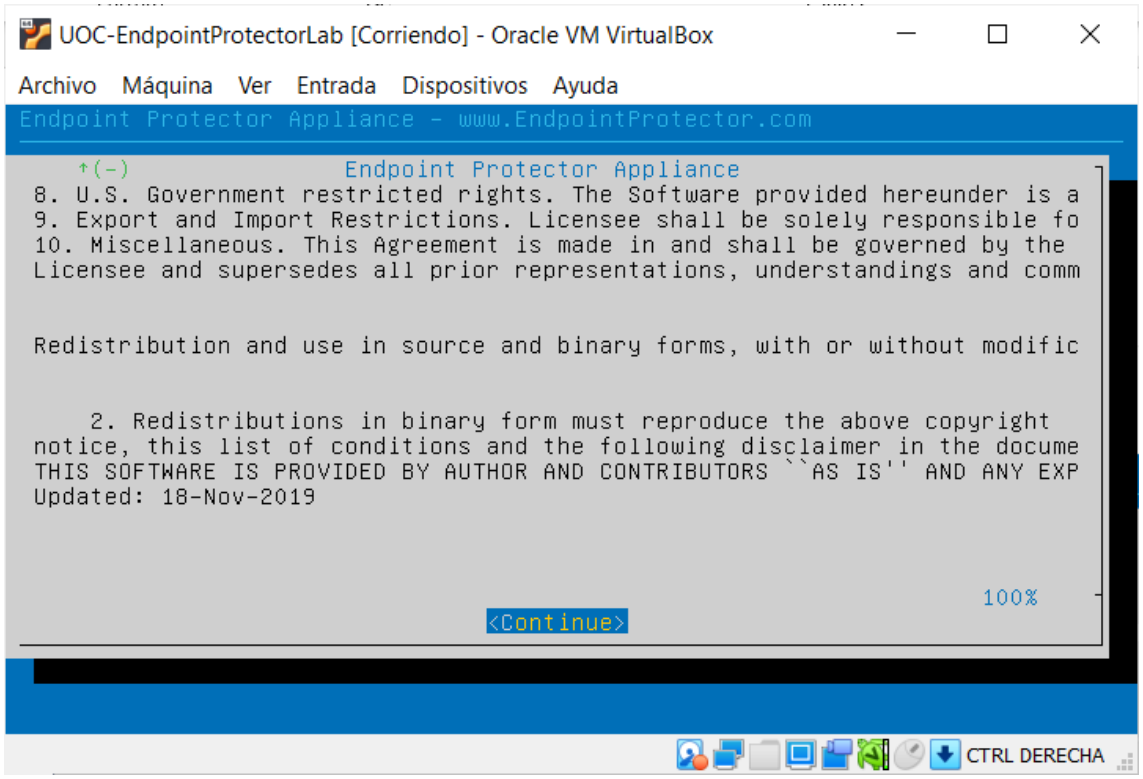


2. Revisamos y aceptamos la configuración:

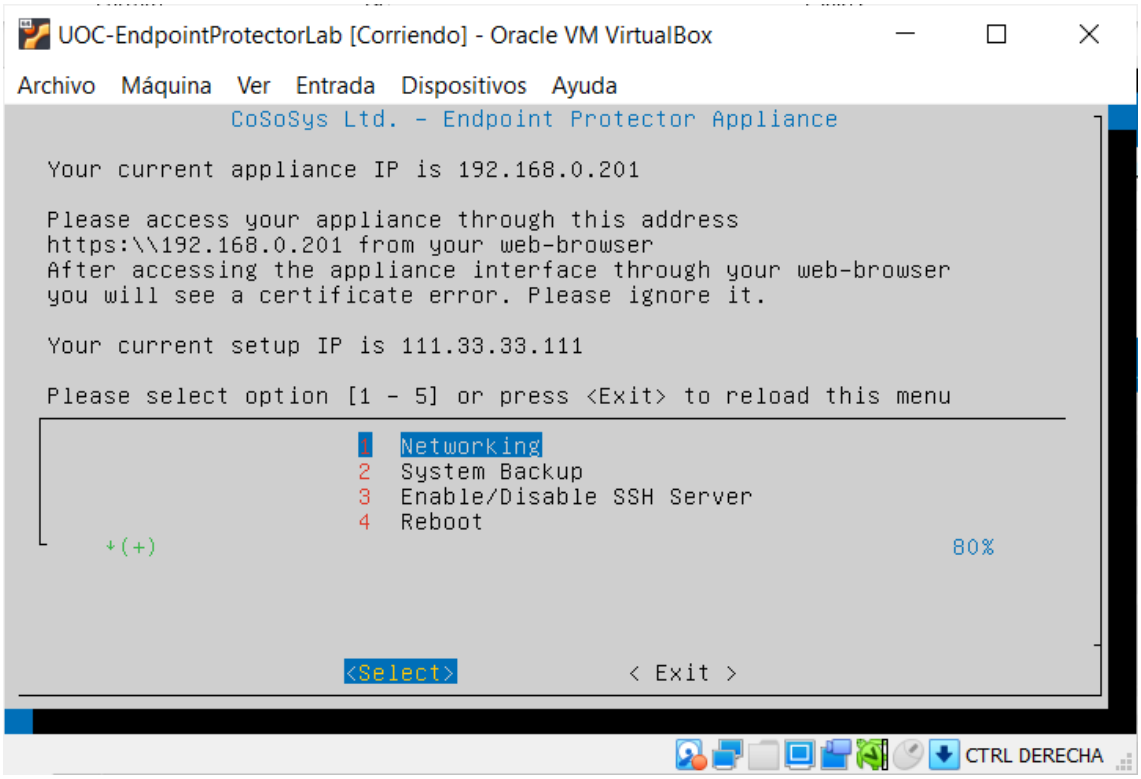


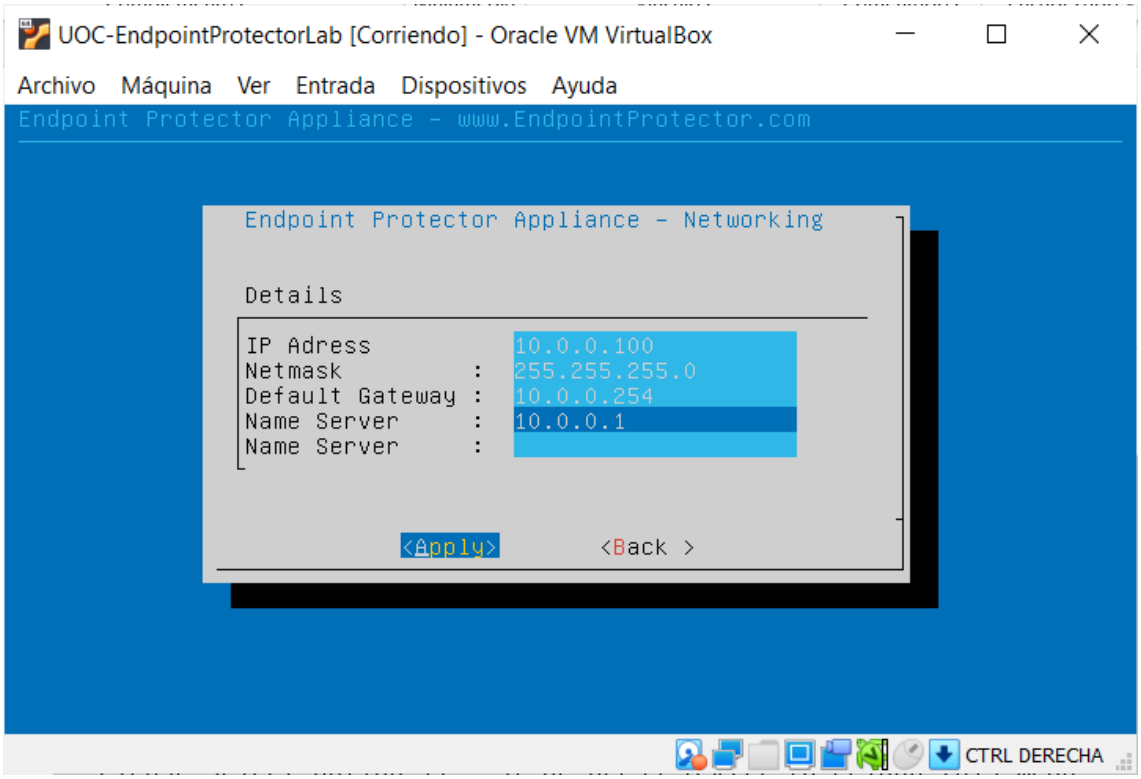
3. Arranque inicial de la máquina. Aceptación del EUA



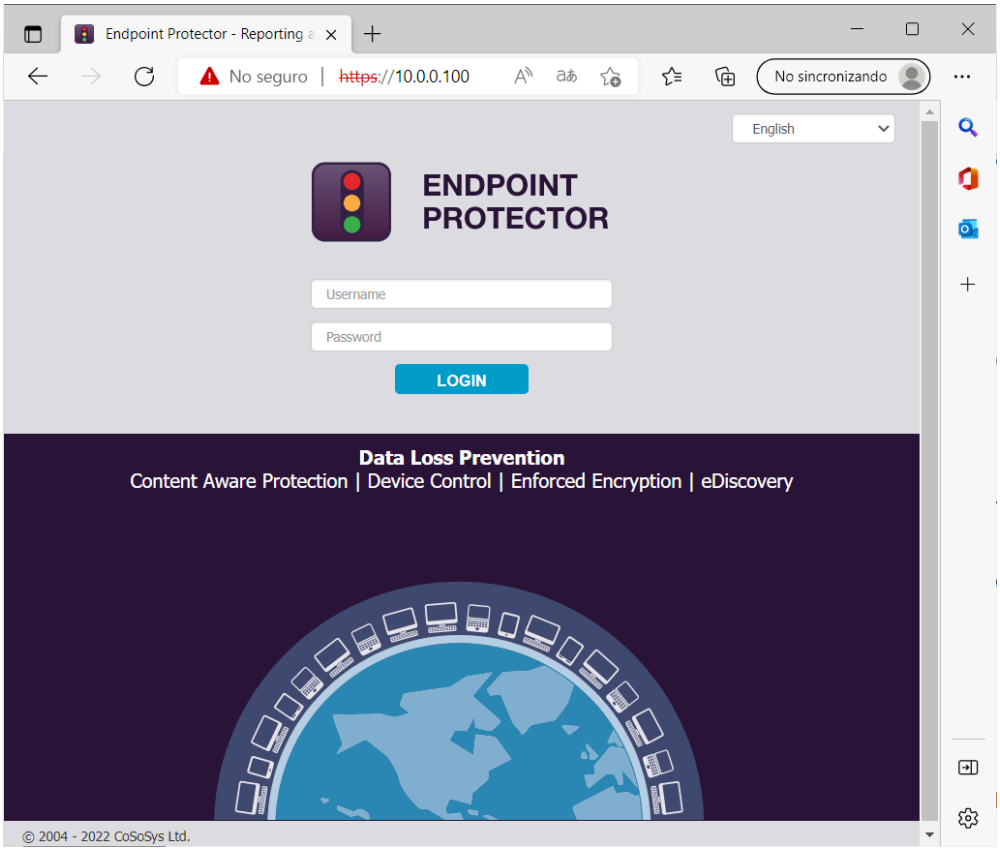


4. Configuración de red

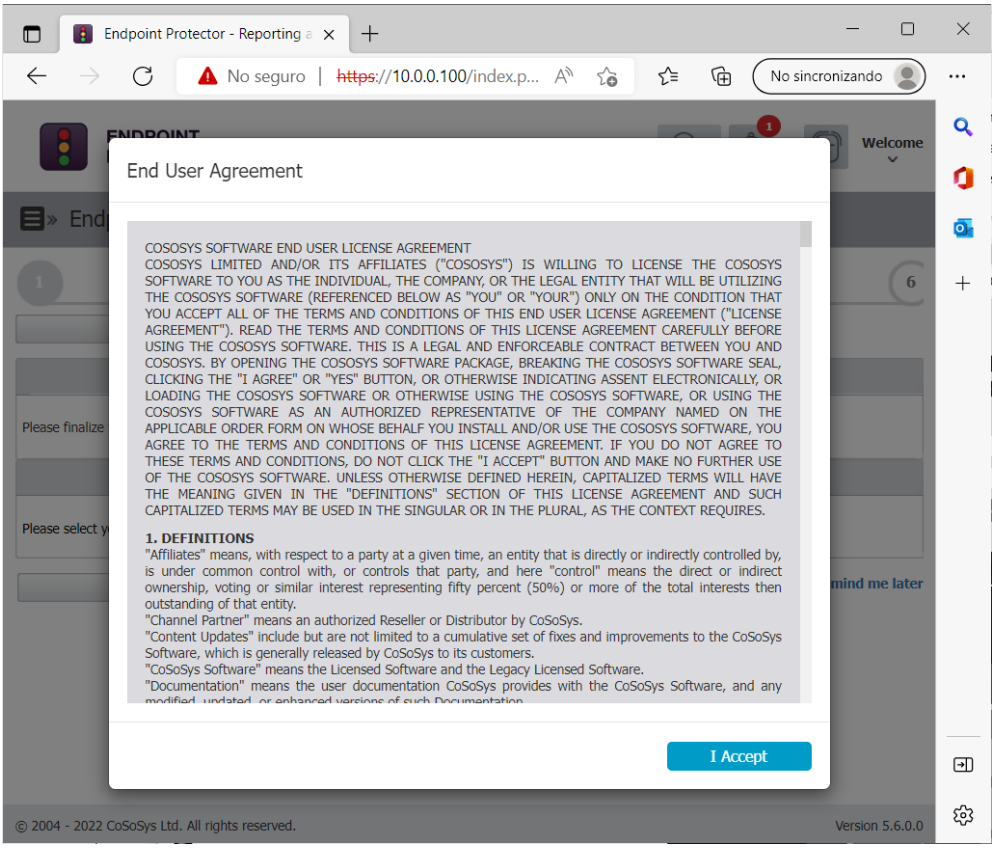




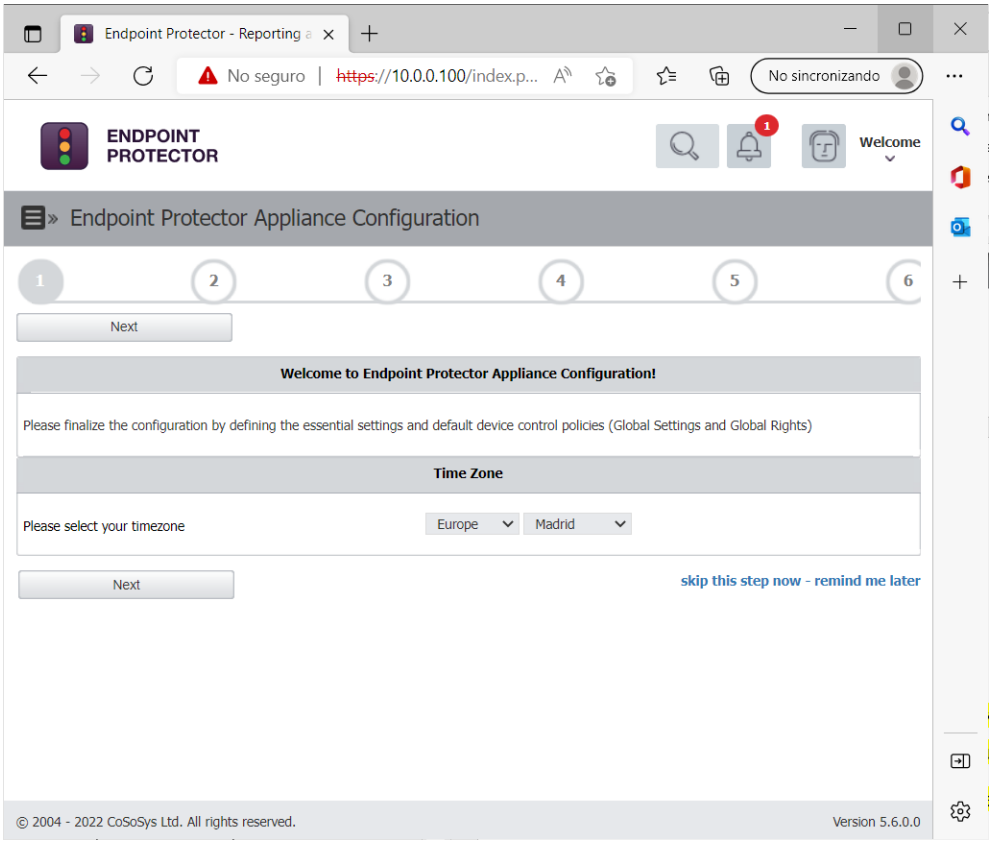
5. Login inicial



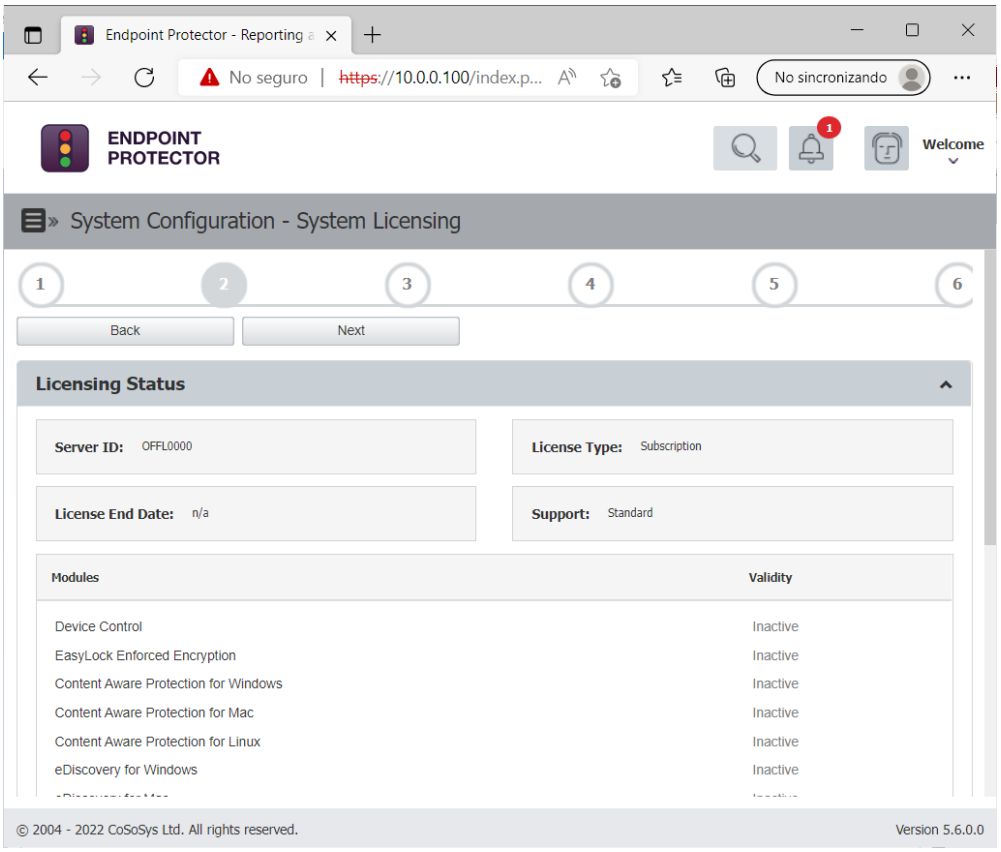
Tras el login, se muestra nuevamente el EUA, que aceptamos:

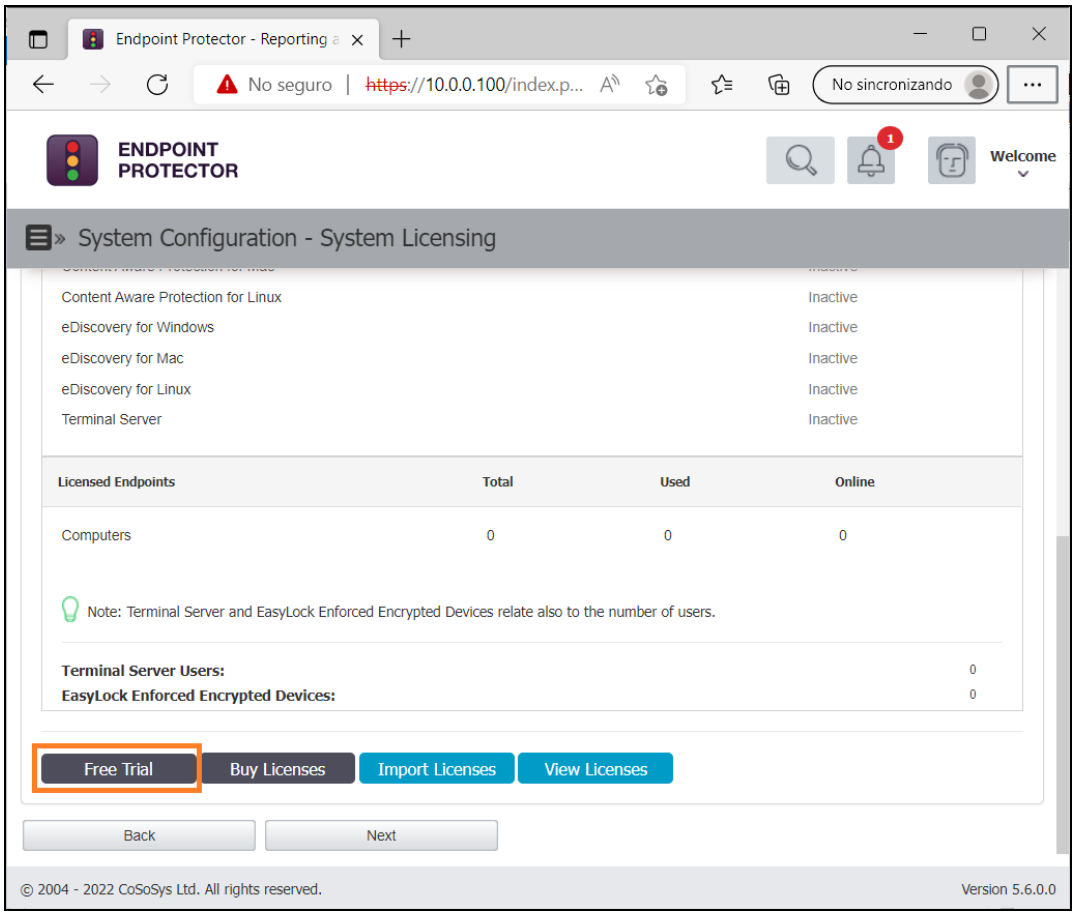


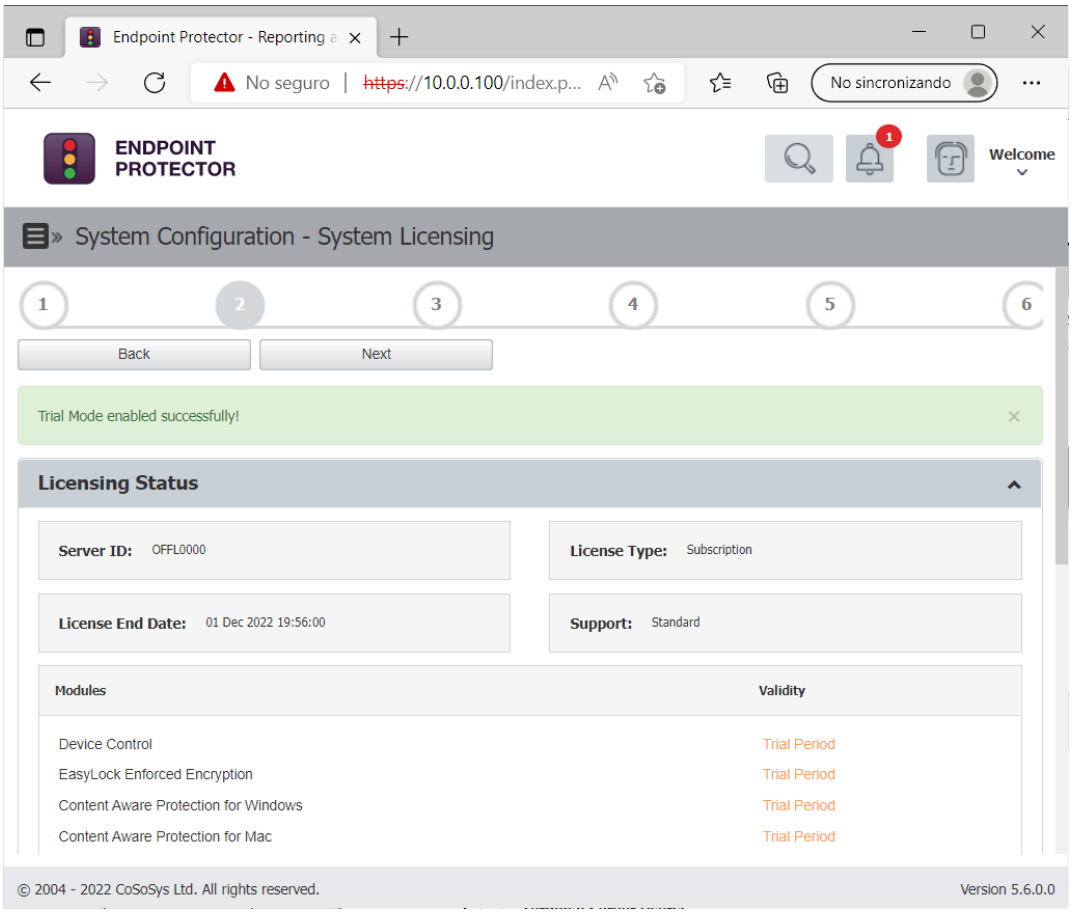
6. Configuración de zona horaria



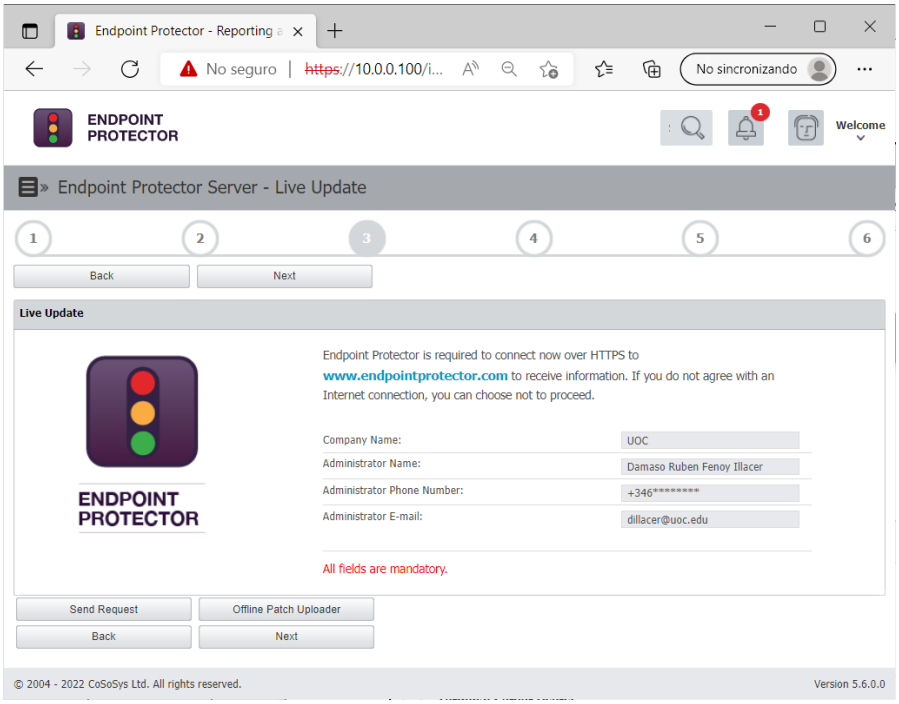
7. Configuración de licencia de evaluación:



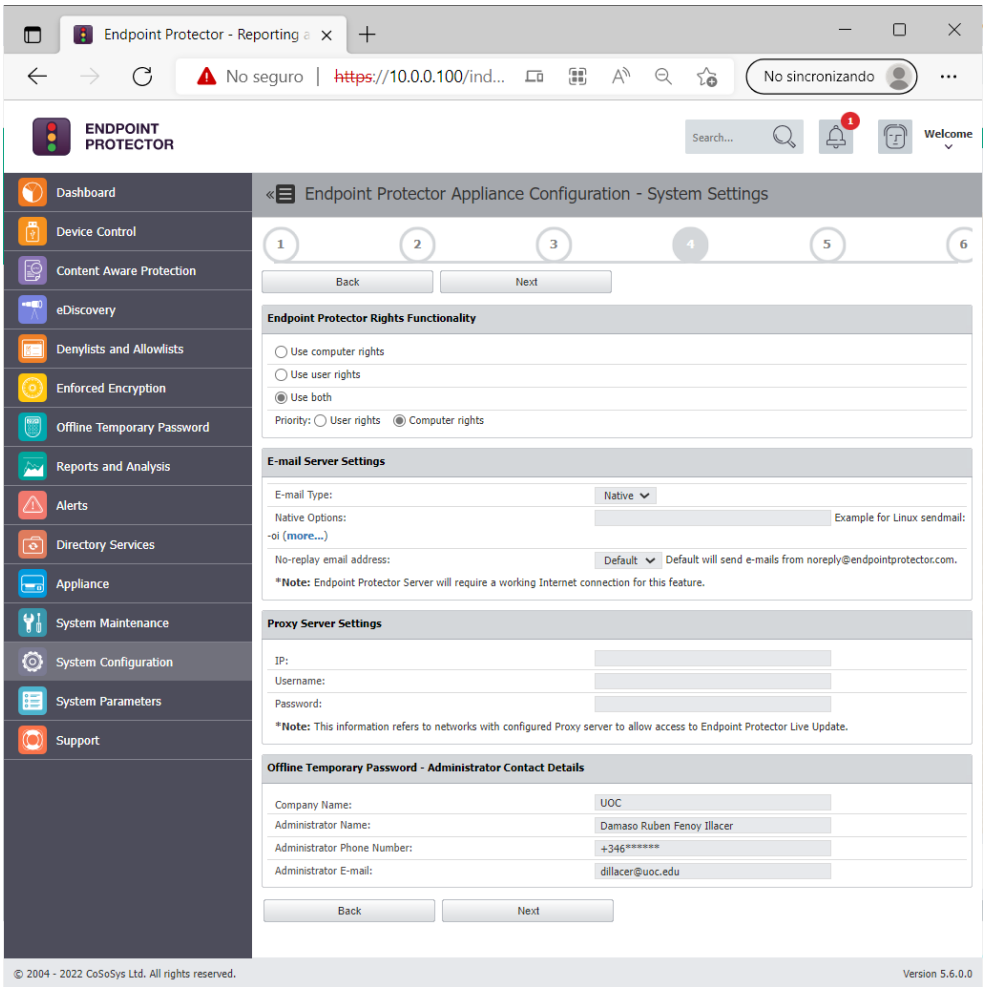

Endpoint Protector - Reporting
No seguro | https://10.0.0.100/index.p...
No sincronizando
ENDPOINT PROTECTOR
Welcome
System Configuration - System Licensing
Content Aware Protection for Linux Inactive
eDiscovery for Windows Inactive
eDiscovery for Mac Inactive
eDiscovery for Linux Inactive
Terminal Server Inactive
Licensed Endpoints Total Used Online
Computers 0 0 0
Note: Terminal Server and EasyLock Enforced Encrypted Devices relate also to the number of users.
Terminal Server Users: 0
EasyLock Enforced Encrypted Devices: 0
Free Trial
Buy Licenses
Import Licenses
View Licenses
Back
Next
© 2004 - 2022 CoSoSys Ltd. All rights reserved.
Version 5.6.0.0


Endpoint Protector - Reporting
No seguro | https://10.0.0.100/index.p...
No sincronizando
ENDPOINT PROTECTOR
Welcome
System Configuration - System Licensing
1 2 3 4 5 6
Back
Next
Trial Mode enabled successfully!
Licensing Status
Server ID: OFFL0000
License Type: Subscription
License End Date: 01 Dec 2022 19:56:00
Support: Standard
Modules Validity
Device Control Trial Period
EasyLock Enforced Encryption Trial Period
Content Aware Protection for Windows Trial Period
Content Aware Protection for Mac Trial Period
© 2004 - 2022 CoSoSys Ltd. All rights reserved.
Version 5.6.0.0

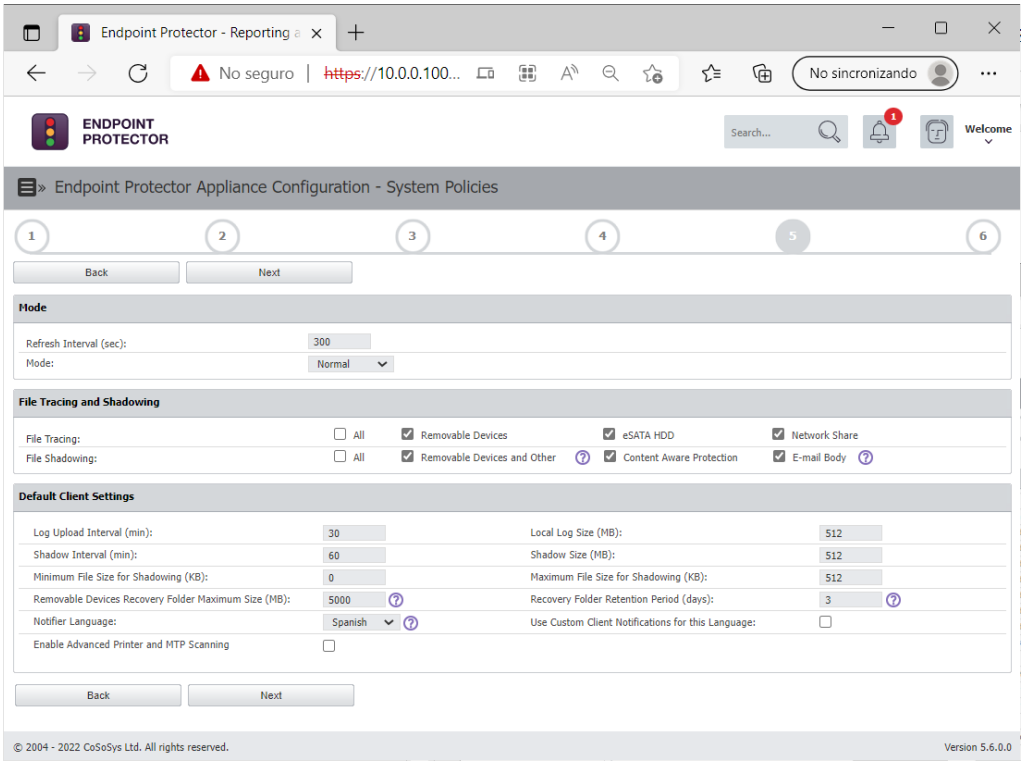
8. Datos de contacto y actualización automática

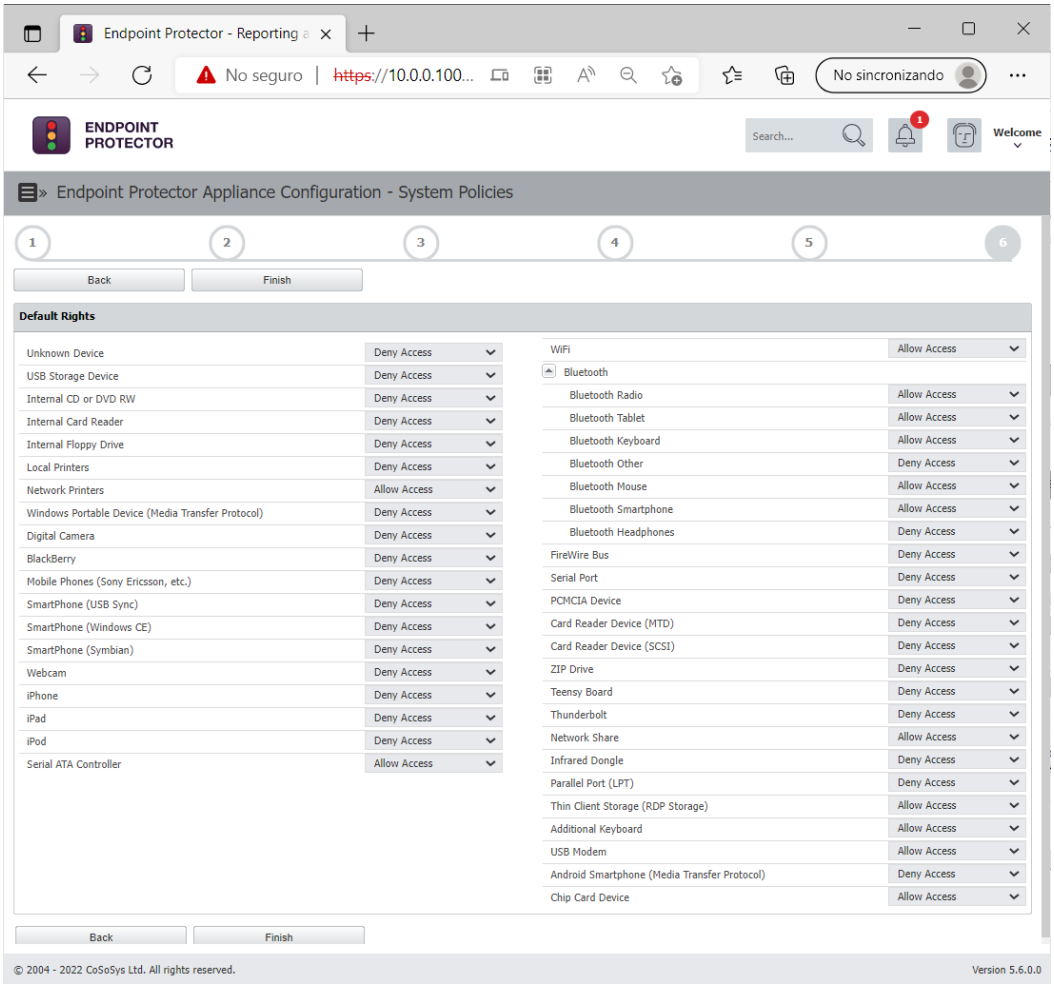


9. Configuración del sistema

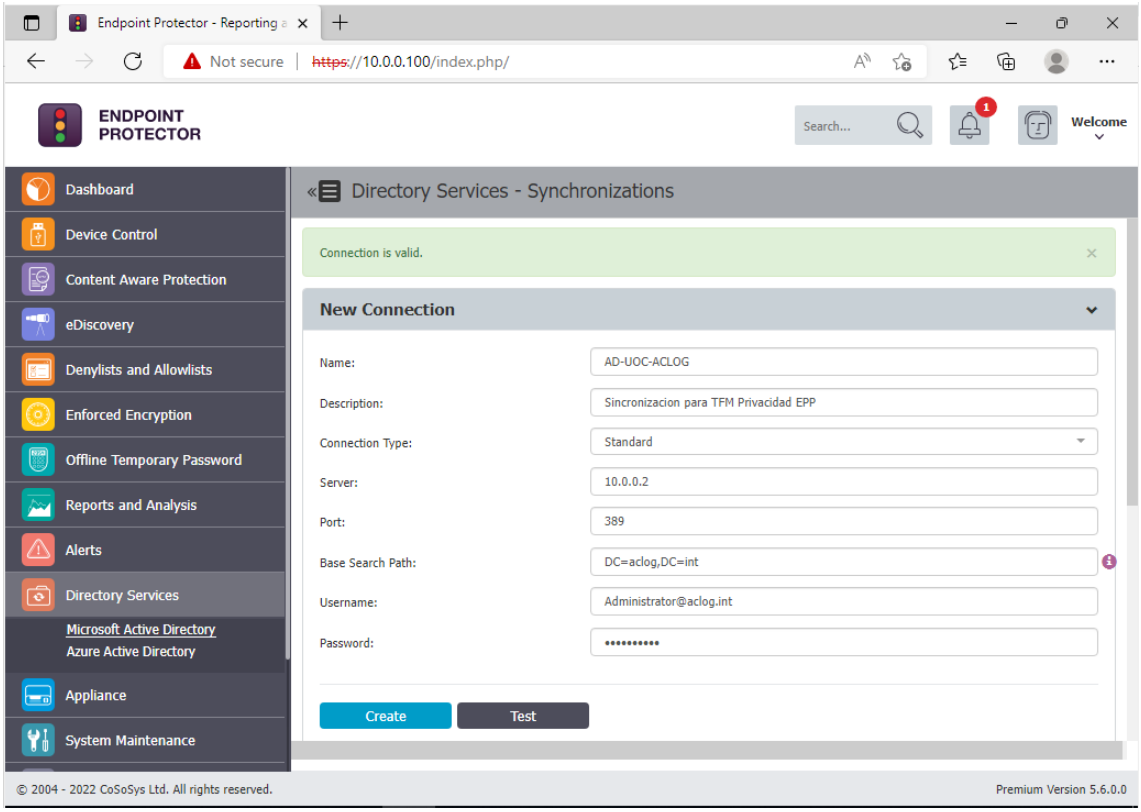


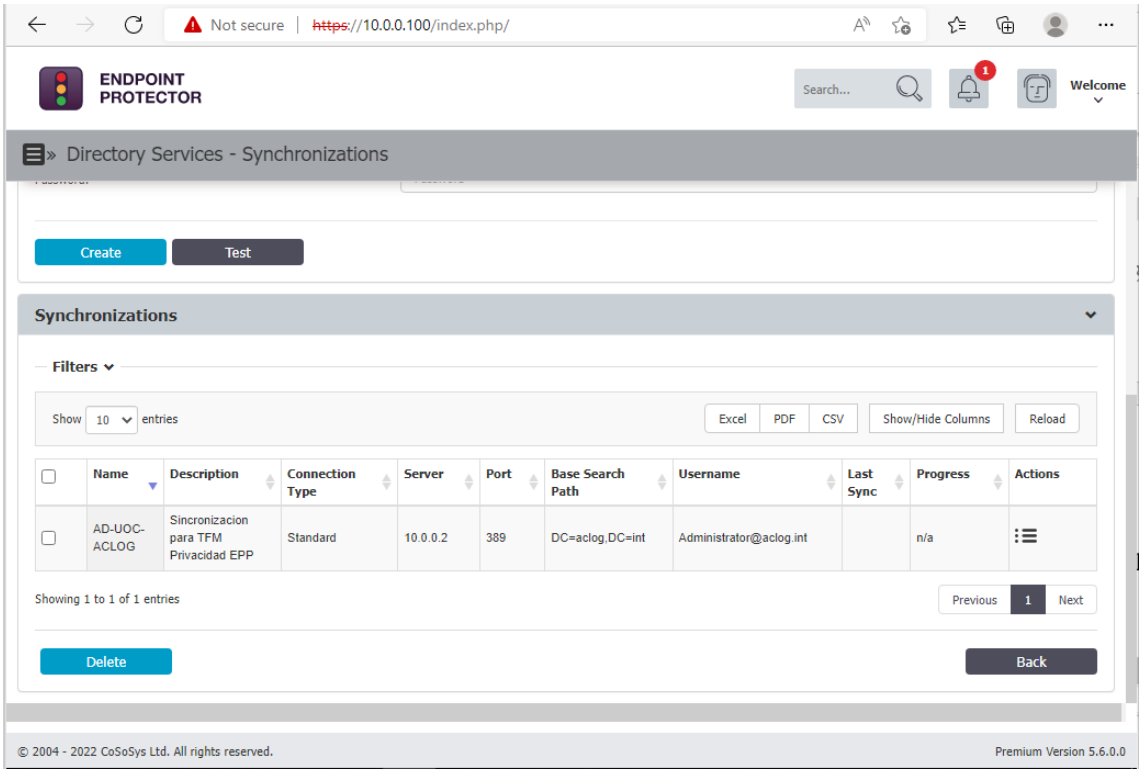
10. Políticas iniciales del sistema





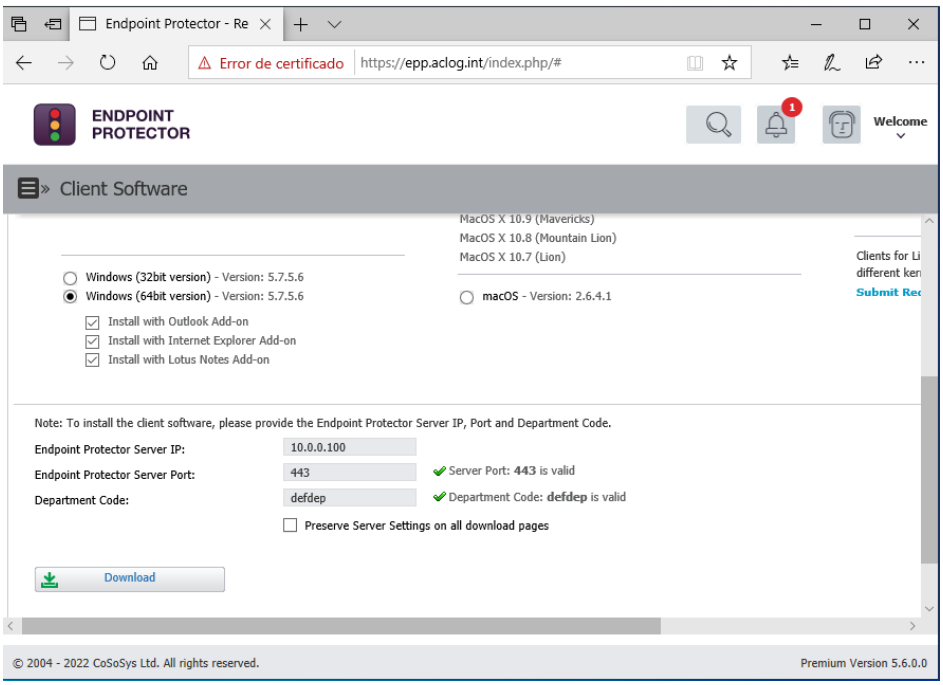
11. Integración con Directorio Activo de laboratorio



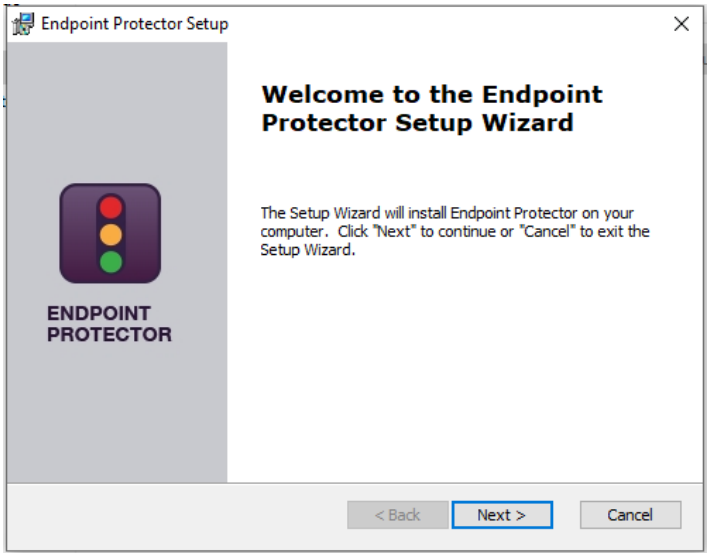


Anexo II. Instalación de agente de Endpoint Protector

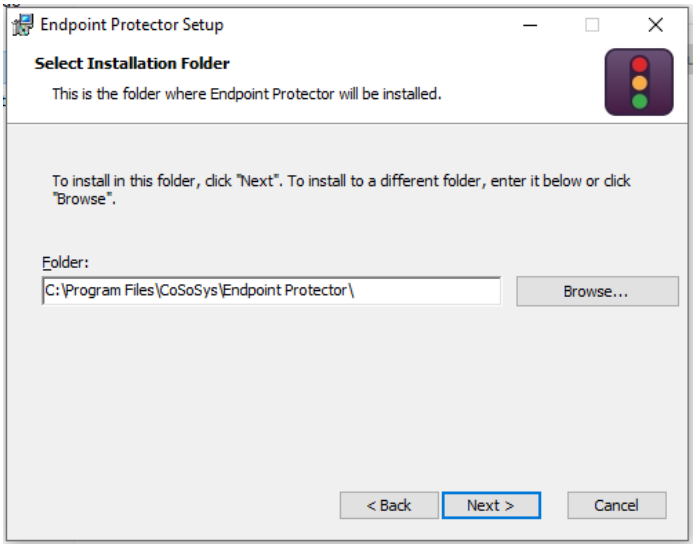
1. Descarga del agente desde el portal de EPP



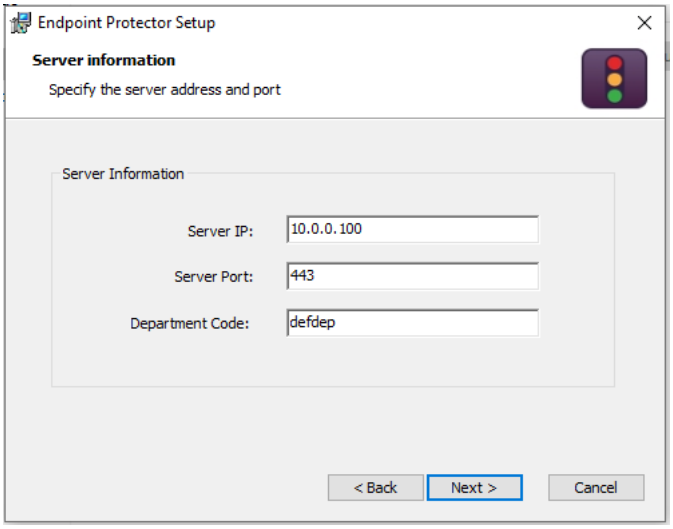
2. Instalación del agente. Página inicial



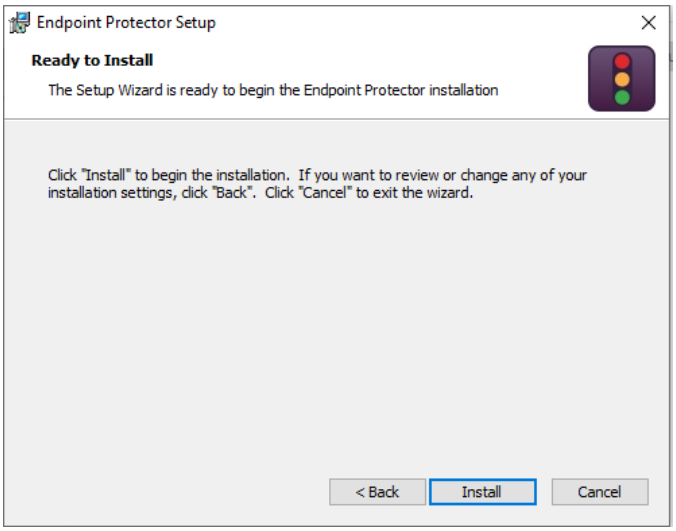
3. Ubicación de la instalación



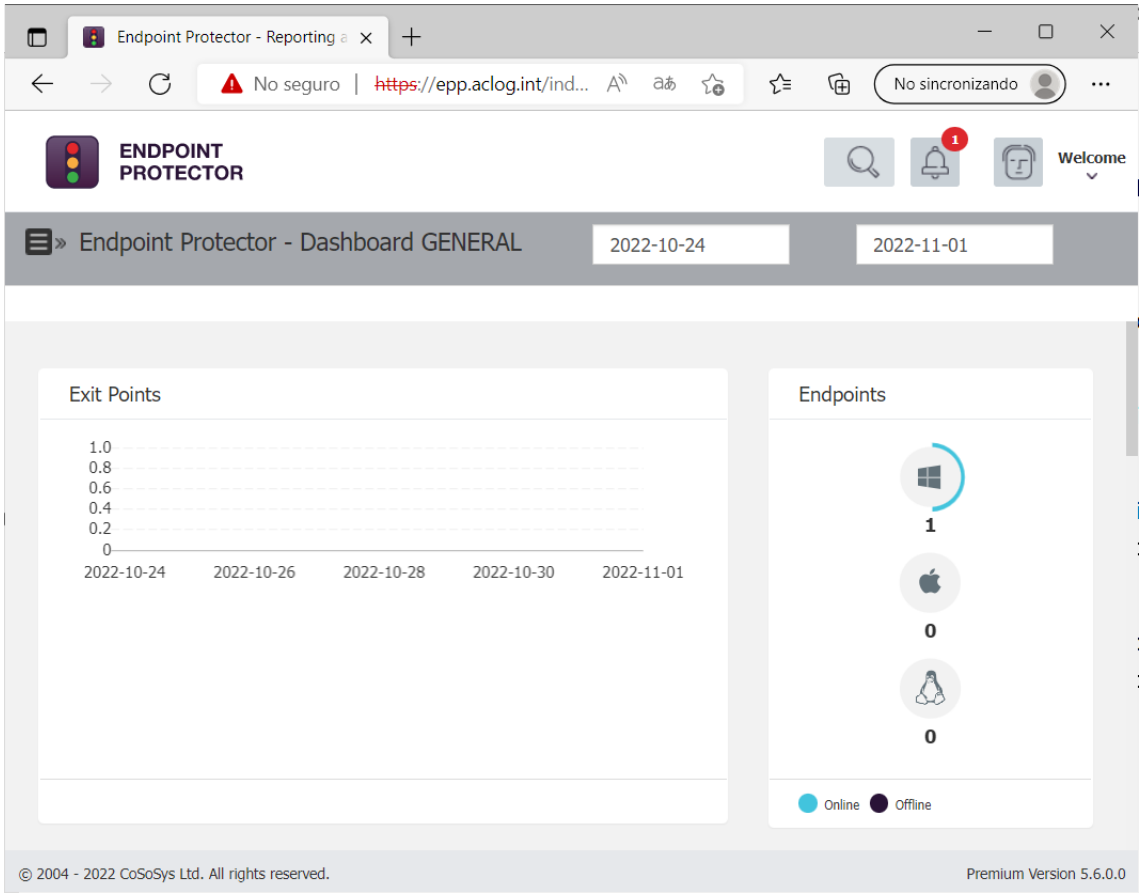
4. Configuración del servidor



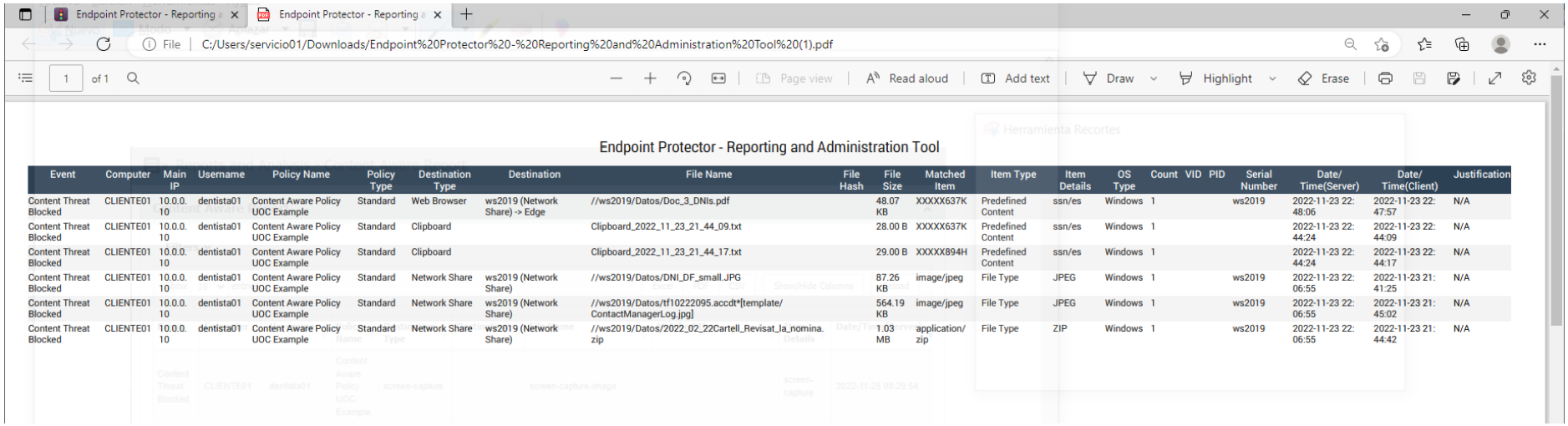
5. Resumen de la instalación



6. Verificación del agente instalado en la consola de EPP



Anexo III. Informes



Endpoint Protector - Reporting and Administration Tool

Event	Computer	Main IP	Username	Policy Name	Policy Type	Destination Type	Destination	File Name	File Hash	File Size	Matched Item	Item Type	Item Details	OS Type	Count	VID	PID	Serial Number	Date/ Time(Server)	Date/ Time(Client)	Justification
Content Threat Blocked	CLIENTE01	10.0.0.10	dentista01	Content Aware Policy UOC Example	Standard	Web Browser	ws2019 (Network Share) -> Edge	//ws2019/Datos/Doc_3_DNIs.pdf		48.07 KB	XXXXX637K	Predefined Content	ssn/es	Windows	1			ws2019	2022-11-23 22:48:06	2022-11-23 22:47:57	N/A
Content Threat Blocked	CLIENTE01	10.0.0.10	dentista01	Content Aware Policy UOC Example	Standard	Clipboard		Clipboard_2022_11_23_21_44_09.txt		28.00 B	XXXXX637K	Predefined Content	ssn/es	Windows	1				2022-11-23 22:44:24	2022-11-23 22:44:09	N/A
Content Threat Blocked	CLIENTE01	10.0.0.10	dentista01	Content Aware Policy UOC Example	Standard	Clipboard		Clipboard_2022_11_23_21_44_17.txt		29.00 B	XXXXX894H	Predefined Content	ssn/es	Windows	1				2022-11-23 22:44:24	2022-11-23 22:44:17	N/A
Content Threat Blocked	CLIENTE01	10.0.0.10	dentista01	Content Aware Policy UOC Example	Standard	Network Share	ws2019 (Network Share)	//ws2019/Datos/DNI_DF_small.JPG		87.26 KB	image/jpeg	File Type	JPEG	Windows	1			ws2019	2022-11-23 22:06:55	2022-11-23 21:41:25	N/A
Content Threat Blocked	CLIENTE01	10.0.0.10	dentista01	Content Aware Policy UOC Example	Standard	Network Share	ws2019 (Network Share)	//ws2019/Datos/tf10222095.accdt*[template/ContactManagerLog.jpg]		564.19 KB	image/jpeg	File Type	JPEG	Windows	1			ws2019	2022-11-23 22:06:55	2022-11-23 21:45:02	N/A
Content Threat Blocked	CLIENTE01	10.0.0.10	dentista01	Content Aware Policy UOC Example	Standard	Network Share	ws2019 (Network Share)	//ws2019/Datos/2022_02_22Cartell_Revisat_la_nomina.zip		1.03 MB	application/zip	File Type	ZIP	Windows	1			ws2019	2022-11-23 22:06:55	2022-11-23 21:44:42	N/A