Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Tema

Seguridad en dispositivos de almacenamiento extraíble y transferencia de datos

Título

Segurización de dispositivos de almacenamiento extraíble y transferencia de datos.

Autor: Ing. Federico Pierro
Tutor: Dr. Pedro Hecht

Año 2019
Cohorte 2018

Declaración Jurada de origen de los contenidos:

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual".

FIRMADO

1 Resumen

El Trabajo Final de la Especialización consistirá en documentar todos los pasos que se llevaron a cabo en el proyecto del ámbito profesional.

El tema de estudio será la seguridad en dispositivos de almacenamiento extraíble y de transferencia de información. Este tema toma relevancia debido al auge de los ciberataques, más precisamente ataques con malware. Estos tipos de ataques, si bien tienen varios vectores de ingreso, uno de los más utilizados y más efectivos son los dispositivos de almacenamiento extraíble como ser Pendrives, Discos Externos o Memorias SD.

A nivel mundial, la gran parte de las empresas que tomaron acciones sobre este tipo de vector de ataque, optaron por soluciones extremistas, llevando al bloqueo total de la utilización de estos dispositivos. En este proyecto se buscó una solución que mitigue el riesgo de ataque, pero que siga permitiendo la utilización de estos dispositivos para casos de uso de negocio de la empresa para los cuales no exista, hoy en día, una solución más efectiva implementada.

Para ello se realizó una investigación a nivel internacional, para conocer las implementaciones de sistemas de control que permitan alcanzar el objetivo del proyecto. En varios casos encontramos un factor común de soluciones, con la utilización de herramientas de Data Loss Prevention (DLP) y Device Control (DC), la cual por un lado permite la gestión de los dispositivos que se conectan a los equipos como también la información y las acciones que se hacen con los mismos.

Dado que la información relevada no es suficiente para armar modelos de configuración, se optó por un diseño de cero, en base a un relevamiento a nivel organizacional con los casos de usos de estos dispositivos para las tareas laborales de los empleados.

Palabras Clave: Data Loss Prevention, Malware, Dispositivos de Almacenamiento Extraible

Contenido

1 Resumen ..... - 2 -

2 Fundamentación del tema elegido ..... - 4 -

3 Objetivos y alcance ..... - 5 -

4 Situación Actual ..... - 6 -

5 Fases del proyecto. ..... - 7 -

5.1 Etapa de planificación ..... - 7 -

5.3 Etapa de relevamiento ..... - 10 -

5.3.1 Necesidad de compartir información con internos ..... - 11 -

5.3.2 Necesidad de compartir información con externos ..... - 12 -

5.3.3 Descargar imágenes/videos de cámaras digitales ..... - 13 -

5.3.4 Descargar imágenes/videos de celulares. ..... - 13 -

5.3.5 Conectar dispositivos que no son para transferencia de información. . - 14 -

5.3.6 Pasar Videos a los televisores corporativos ..... - 14 -

5.3.7 Transferir información con dispositivos industriales o corporativos, pero fuera de red ..... - 15 -

5.5 Etapa de desarrollo ..... - 16 -

5.5.1 Device Control ..... - 16 -

5.5.2 Data Protection ..... - 25 -

5.7 Etapa de implementación ..... - 36 -

6 Logros, Contratiempos y Mejoras Futuras ..... - 37 -

6.1 Logros ..... - 37 -

6.2 Contratiempos ..... - 37 -

6.3 Mejoras Futuras ..... - 38 -

7 Conclusión ..... - 39 -

8 Bibliografía ..... - 41 -

2 Fundamentación del tema elegido

Los dispositivos de almacenamiento extraíble son un complemento más en el día a día de muchos usuarios de PCs, casi tan imprescindibles como el mismo ordenador o teléfono móvil, pero a la vez tan pequeños y discretos que no les prestamos el nivel de atención y seguridad necesarios.

Muchas veces se suele pedir un dispositivo USB o algún otro dispositivo para poder compartir un archivo sin saber lo que este puede contener o bien lo que podría llegar a generar si infectará nuestra PC. Este tipo de cosas, que a veces, suelen parecer normales pueden llegar a tener consecuencias indeseadas y mucho más aún si no tomamos medidas de seguridad adecuadas.

En los últimos años el crecimiento de los ataques e infecciones con Malware a las empresas fue exponencial. Es por lo que las áreas de seguridad de la información de las empresas se encuentran en constante investigación para poder afrontar estos ataques de la mejor manera posible y teniendo el menor impacto posible.

Los usuarios desestiman el riesgo que corren al conectar un dispositivo de almacenamiento del cual conocemos o no donde fue conectado previamente, el cual supone ser igual o en ocasiones mayor al de conectarse a internet en cuanto a la distribución de malware o software malicioso.

Es por lo mencionado anteriormente, que cada organización, debe disponer de una política de uso de dispositivos de almacenamiento externo que indique cuestiones sobre si su uso está o no permitido, y en caso de que sí esté permitido, que tipo de información puede y no almacenarse en ellos. Y en el caso de que no esté permitido el Por qué.

3 Objetivos y alcance

El objetivo de este trabajo es documentar las distintas etapas del proyecto profesional que lideré, en el cual se definió un modelo de seguridad aplicado a los dispositivos de almacenamiento extraíble, que permita el uso de los mismos para casos de uso para los cuales aún no se cuente con una alternativa que no implique el uso de estos dispositivos, y que al mismo tiempo proteja a la empresa de posibles ataques de malware por estos medios. Por temas de confidencialidad de la empresa, ciertos datos se verán ofuscados o modificados, pero para el trabajo en cuestión, no es necesario contar con los datos reales.

El alcance del trabajo incluye la explicación del desarrollo del proyecto, explicando técnicamente la estructura de reglas que se configuraron. No incluye la explicación de la instalación de la herramienta ya que la misma se encontraba instalada en la organización y solo se hizo una mejor configuración de las reglas de bloqueo y auditoria del tráfico de información.

4 Situación Actual

La empresa cuenta con 7000 PC conectadas a la red interna de la compañía. Gran cantidad de los usuarios de esas PCs tienen la necesidad de utilizar dispositivos cuyo tipo de conexión es USB, con la finalidad de recibir o compartir información, configurar dispositivos industriales como ser PLCs, lectores de temperatura, etc. Si se imagina una situación en la cual los dispositivos USB para compartir información, solo se utilizan en PCs de la compañía, el único riesgo que se corre es la fuga de información, si uno de esos pendrives. Pero la realidad es distinta, los usuarios comparten información por medio dispositivos USB de gente externa, y ahí es donde el problema comienza, al desconocer la situación a nivel seguridad de la PC a la que se conectará o se conectó el dispositivo.

Para mitigar los riesgos que generan estos tipos de uso de los dispositivos, en un proyecto anterior la empresa decidió por medio de una herramienta de Data Loss Prevention (DLP) con una configuración muy simple, empezaron a limitar los accesos, solo otorgando permisos de Lectura o de Lectoescritura bajo demanda y con una justificación apropiada, la cual no siempre se cumplía.

A esto ultimo se le suma que la situación actual a nivel mundial en lo que respecta a los ataques de malware, estaba tendiendo a utilizar los dispositivos USB como llave de entrada a una empresa. Si bien un dispositivo infectado de por si solo, puede provocar daño en la compañía, si se le suma ingeniería social y otros ataques posteriores al ingreso del malware, el daño puede ser mucho peor y hasta irreversible.

5 Fases del proyecto.

5.1 Etapa de planificación

El origen del proyecto se dio por las sucesivas noticias de ataques de malware a nivel mundial. Los ataques constan en enviar un archivo infectado con un malware vía correo electrónico o vía dispositivos USB, como ser pendrives, o discos externos. En el caso de las infecciones vía dispositivos USB de almacenamiento, hay varias formas de lograr la infección, pero las más frecuentes son infecciones directas o indirectas.

Las infecciones directas son aquellas en las que el atacante hace llegar de alguna manera un dispositivo infectado con el malware a un usuario de la compañía destino. Las formas de entregarlos pueden ser como regalo o bien un proveedor que simula el paso de información.

Es por lo anteriormente mencionado que el CISO de la empresa en la que se desarrolló el proyecto, propuso el desarrollo del proyecto de reducción de habilitaciones USB. El objetivo de este era llegar a dejar tan solo un 5% de los usuarios actualmente habilitados, con permisos para utilizar dispositivos USB. Dicho proyecto ya se había intentado realizar 2 años antes, y no tuvo el éxito que se esperaba. La razón más importante del fracaso es la falta de herramientas que puedan saciar las necesidades de los usuarios que iban a quedar insatisfechas con el bloqueo de dispositivos USB.

El escenario del cual se partió era que un 35% de la compañía contaba con permisos para poder cargar, descargar y ejecutar archivos de cualquier tipo a cualquier tipo de dispositivo extraíble. Esto generaba muchos problemas. El más visible y reiterativo era la detección de dispositivos infectados con algún tipo de programa malicioso el cual solía venir de otro dispositivo infectado al cual se le conecto el dispositivo extraíble previamente. Muchos usuarios usaban el mismo dispositivo en el ambiente laboral y en su domicilio, donde sus equipos no contaban con las medidas de seguridad necesarias para evitar estos tipos de infecciones. Otro caso de uso, que se quería descontinuar es el hecho de que los usuarios realizan backup de su información personal y laboral en la PC corporativa y en medios de almacenamiento extraíbles como pendrives o grandes discos externos. Acá

podemos ver dos puntos importantes; por un lado, el activo informático que la empresa brinda es solo para uso laboral y no debe contener información personal como imágenes o archivos personales. Por otro lado, el hecho de guardar información de la empresa en un medio de almacenamiento externo no es recomendable ya que el dispositivo se puede romper en cualquier momento, provocando la pérdida total de la información almacenada en él, o bien puede ser extraviado y al no estar segurizado, información confidencial puede caer en manos incorrectas generando un alto riesgo para la empresa.

Otro de los usos, que se encuentra relacionado en cierta manera a los dos mencionados anteriormente, es el hecho de enviar y recibir información con gente ajena a la empresa. Un caso muy común es que un proveedor venga a la empresa y necesite compartir información con alguien interno, y dicha información la trae en un pendrive. El problema en este caso es, que no conocemos el origen de dicho dispositivo y donde fue conectado previamente, por lo que hay grandes posibilidades de que el mismo se encuentre infectado.

Ahora bien, para poder administrar la utilización de los dispositivos de almacenamiento extraíble es necesario contar con una herramienta especializada. En este caso se utilizó un módulo de DLP del antivirus corporativo. Dicho modulo te permite definir reglas de utilización de los dispositivos y asociarlos a toda la compañía o bien individualmente por usuario.

Al momento de planificar los primeros pasos del proyecto se tuvo que relevar la mayor cantidad de casos de uso posible y al mismo tiempo ir pensando si podía ser saciada con alguna de las herramientas disponibles en la compañía. Al ser una empresa muy grande, las necesidades son variadas, desde gente que necesita compartir información con externos, pasando por operarios que necesitan pasar información a PLCs industriales hasta usuarios que trabajan en zonas sin conectividad y utilizan pendrives para compartir información.

Otra de las pautas definidas por el CISO es que el tiempo límite para realizar la adecuación de permisos es el 31/12, fecha para la cual debemos contar tan solo con el 5% de las habilitaciones actuales, definidas. La etapa del relevamiento fue llevada a cabo por mi junto con mi líder. En

dicha etapa fuimos relevando con las distintas áreas de la compañía, las necesidades de cada uno de ellos. Una vez relevadas las mismas, se armó un grupo de trabajo involucrando al especialista de la herramienta que soportará el control de los permisos, un especialista de la mesa de ayuda, ya que son los que tienen el primer contacto con los usuarios y conocen gran cantidad de necesidades de los usuarios y del lado del área de seguridad participe yo junto a mi líder.

Una vez armado el equipo de trabajo, se definió un plan de trabajo que dividía al proyecto en 3 grandes partes.

- Una primera parte en la cual se realizó un análisis profundo de las necesidades de todas las áreas de la empresa
- Una segunda etapa en la cual se definieron soluciones a cada una de dichas necesidades
- Una tercera en la cual se realizaron pruebas unitarias e integrales con distintos usuarios claves de las áreas identificadas y por último la implementación de las nuevas políticas.

5.3 Etapa de relevamiento

Siendo una de las etapas más importantes, como equipo se buscó invertir gran parte del tiempo del proyecto en el relevamiento de las necesidades a nivel compañía, de utilizar dispositivos USB. Para ello nos contactamos con usuarios claves o gerentes de las distintas áreas como RRHH, Seguridad Patrimonial, Ventas, Mantenimiento, Ingeniería y mismos sistemas.

En todos los contactos que tuvimos con las distintas áreas, se fueron relevando gran cantidad de necesidades. Muchas eran compartidas pero cada una contaba con alguna particularidad la cual detallo a continuación:

- RRHH
  - Cargar videos institucionales a los televisores corporativos
  - Recibir curriculum de gente externa.
- Seguridad Patrimonial
  - Descargar información de los CCTV de las distintas plantas de la compañía
  - Enviar información a juzgados por causas.
  - Backup de información sensible y confidencial
- Ventas
  - Compartir folletos de ventas a los clientes o distribuidores
  - Relevar información de los distintos puntos de venta y bajarlo a la PCs
- Mantenimiento
  - Recibir manuales de maquinaria.
  - Enviar y recibir propuestas y cotizaciones de reparaciones.
- Ingeniería
  - Recibir aplicativos para maquinarias o PLCs de las plantas.
  - Pasaje de archivos de planos o layouts de gran tamaño
- Sistemas
  - Recibir nuevos releases de aplicaciones
  - Recibir parches o iso de distintas aplicaciones
- Compartidas
  - Compartir información con usuarios externos, de variado tamaño.

- Compartir información con usuarios internos, de variado tamaño.
- Descargar información de dispositivos celulares corporativos o personales.
- Descargar información de cámaras digitales.
- Utilización de impresoras con conexión USB
- Utilización de Tokens o llaves de autenticación.
- Utilización de dispositivos industriales (Cámara termográficas, Sensores de temperatura, presión)

Una vez relevados los casos, se buscó normalizar los casos de uso de tal manera que no se repitan casos de uso con pequeñas variantes. Dicha normalización dio como resultado 5 grandes casos de uso:

- Necesidad de compartir información con internos.
- Necesidad de compartir información con externos.
- Descargar imágenes/videos de cámaras digitales
- Descargar imágenes/videos de celulares.
- Conectar dispositivos que no son para transferencia de información.
- Pasar Videos a los televisores corporativos.
- Transferir información con dispositivos industriales o corporativos, pero fuera de red.

Una vez que se tuvo el detalle de los casos de uso se realizó un primer acercamiento a la solución de cada caso.

5.3.1 Necesidad de compartir información con internos

Esta solución ya se encontraba satisfecha con herramientas de la familia Office 365. A nivel compañía se implementó la plataforma Office 365 para lo que es Correo electrónico y herramientas como Onedrive, Sharepoint y Office. En este caso, la herramienta que suple la necesidad es Onedrive. Cada usuario tiene un espacio determinado para poder almacenar sus documentos de trabajo y los mismos se encuentran respaldados en la nube. El dia que el usuario cambia de equipo ya sea por renovación o por rotura, toda su información se encuentra en la nube y puede ser accedida, por él, desde cualquier PC. Ahora bien, también existe la necesidad de realizar equipos de trabajo y compartir información entre varias personas. Para ello se

utiliza la alternativa llamada Grupos Colaborativos, que consta en tener una estructura de carpetas en la nube, compartida con las personas que el dueño del grupo permita.

El problema que tenía esta herramienta era que, al momento del lanzamiento de la misma, no se había promocionado de manera efectiva, por lo que gran parte de los usuarios no lo aprovechaban. Viendo esta situación, desde el proyecto se planificó el armado de una campaña de promoción de la herramienta por medio de videos.

5.3.2 Necesidad de compartir información con externos

Este caso de uso no contaba con una solución de la plataforma Office365 implementada. El equipo realizó un análisis de las herramientas disponibles y se llegó a la selección de Sharepoint. Dicha herramienta ya era utilizada de manera interna pero no podía ser accedida por usuarios externos y menos por fuera de la red de la empresa. Es por lo que para que se pueda reutilizar la herramienta, tan solo se tuvo que trabajar en seteos de configuración de la misma. La configuración básica de Sharepoint consta en la creación de un Site Collection, que básicamente es como una burbuja que contiene sitios, que tiene una configuración especifica que es heredada por los distintos sitios contenidos en él. Una de las configuraciones más importantes que se hace a nivel Site Collection es el hecho de quien accede y quien no a los sitios.

Para poder contar con una gestión controlada de los sitios se tomaron las siguientes definiciones técnicas y funcionales:

- Los sitios que se creen para compartir con usuarios externos se llamará Sitio para Externos.
- Los sitios para externos podrán ser solicitados y administrados solo por Gerentes de áreas.
- Solo se permitirá compartir a dominios privados. Esto busca evitar la fuga de información con cuentas personales.
- Por cada sitio para externos que se cree se va a crear un site collection. Esto permitirá que las configuraciones para cada sitio sean únicas y no

se compartan, como, por ejemplo, los dominios autorizados para compartir, que serán particulares de cada sitio.

- Todos los sitios tendrán como dueño del mismo, al gerente del área solicitante. El dueño tendrá la potestad de invitar nuevos miembros internos y externos.
- Se recomienda generar carpetas por proveedor o por proyecto.

5.3.3 Descargar imágenes/videos de cámaras digitales

Esta necesidad surge en la mayoría de los casos de los usuarios de las plantas industriales, donde se encuentran constantemente sacando fotos a maquinas, procesos productivos, accidentes con el fin de armar reportes o analizar ciertas situaciones. En este caso, se procedió a analizar los tipos de conexiones que tienen las cámaras digitales y se detectaron 3 tipos distintos:

- Modo de conexión MTP: es un modo de conexión extensión del protocolo de transferencia de imágenes (PTP) que permite su uso en otros dispositivos además de las cámaras digitales convencionales, permitiendo la transferencia de archivos de multimedia en general y no limitándose solo a imágenes.
- Modo de conexión PTP: es un modo de conexión que permite solo la transferencia de imágenes.
- Modo de conexión Almacenamiento Masivo: es un modo de conexión que simula la conexión de la memoria interna de la maquina como medio de almacenamiento extraíble. Este modo permite el tráfico entrante y saliente de cualquier tipo de

5.3.4 Descargar imágenes/videos de celulares.

Para el caso de la descarga de imágenes y video desde dispositivos celulares se optó por 2 alternativas. Por un lado, la utilización de Google Fotos, plataforma donde se suben las imágenes de los dispositivos con sistema operativo Android, y por otro lado una aplicación corporativa que permite a teléfonos gestionados por el Sistema de Gestión de dispositivos (MDM) que permite la transferencia de archivos entre el celular y el Onedrive del usuario.

5.3.5 Conectar dispositivos que no son para transferencia de información.

Esta necesidad surge cuando los usuarios necesitan conectar dispositivos que no son de almacenamiento de información. Dentro de estos dispositivos se encuentran los tokens para la firma de documentación o bien para autenticar en bancos. Otro tipo de dispositivo que requieren de habilitación, son los instrumentos de medición industrial como ser densitómetros, termómetros, cámaras termográficas; estos requieren ser configurados vía USB o puerto Serial. La solución que se da para estos requerimientos es la habilitación por 2 valores del dispositivo llamados Vendor ID (VID) y Product ID (PID). Este tipo de habilitación tiene como ventaja, que, si en toda la empresa se utiliza un mismo tipo y modelo de dispositivo, tan solo con una habilitación el dispositivo se encuentra habilitado y funcionando correctamente. Este tipo de habilitación no es recomendable para cuando se habiliten pendrives o discos externos ya que se estaría habilitando a todos un modelo y marca especifico de dispositivo.

5.3.6 Pasar Videos a los televisores corporativos

En el esquema previo de administración de permisos sobre dispositivos USB, muchas personas de RRHH o Jefes de Planta, contaban con permisos para poder conectar cualquier tipo de dispositivo sin ninguna restricción de seguridad, cuando lo único que necesitaban era cargar archivos de video a un pendrive para luego conectarlos a televisores corporativos distribuidos en las distintas oficinas o plantas de la empresa. Para ello se dio como solución un permiso que tan solo permite traficar archivos del tipo video solo a dispositivos de almacenamiento. El sistema solo permitirá transferir archivos del tipo video desde la PC al dispositivo extraíble. El filtro de tipo de archivo lo aplica teniendo en cuenta el True File Type del archivo y la extensión del mismo. Este último filtro evita que el usuario final cambie la extensión de otro tipo de archivo con el fin de poder transferirlo, si bien el True File Type se basa en el Media Type del archivo, el cual también puede ser alterado, se considera una capa más de seguridad. Esta solución es temporal, ya que hay un proyecto

en curso en la empresa que busca implementar un sistema de cartelería digital el cual no requiere de traspaso de información vía pendrive ya que es un sistema centralizado que permite gestionar todos los dispositivos de proyección desde un mismo lugar.

5.3.7 Transferir información con dispositivos industriales o corporativos, pero fuera de red

Este último caso es el más riesgoso ya que existe la necesidad de transferir cualquier tipo de información a un dispositivo industrial corporativo fuera de la red corporativa. Al no contar con una red industrial similar a la corporativa, es necesario que el traspaso de información se haga con dispositivos como pendrives o discos externos. La transferencia en este caso es bidireccional ya que en algunos casos se cuenta con una PC aislada de la red, conectada directamente a una impresora industrial, a la cual se le cargan los diseños de impresión de los envoltorios de los productos. Y en otros casos hay dispositivos conectados a la línea de producción los cuales toman información de la propia línea y luego deben ser extraídos y analizados en una PC. Esa extracción se realiza con pendrives o memorias SDs. Al ser una solución de alto riesgo, porque sigue latente la posibilidad de fuga de información o bien de que un malware que logre evadir los controles de seguridad e infecte la PC, hay un proyecto corporativo en el cual se busca armar una red industrial a la cual todos los dispositivos industriales se conecten a ella y la red cuente con cierta visibilidad con la red corporativa y así poder transmitir información sin necesidad de utilizar dispositivos extraíbles de almacenamiento.

5.5 Etapa de desarrollo

Teniendo el relevamiento de las necesidades y sus soluciones propuestas y la herramienta seleccionada, se procedió a configurar las reglas de bloqueo y de auditoria. Antes de detallar las reglas es necesario explicar los tipos de reglas, donde encontramos 2 grupos:

- Device Control
    - Se encuentra orientada a todo lo relacionado a la gestión de conexión de dispositivos, detección de los mismos y ejecución de archivos en ellos. Dentro de este grupo encontramos subtipos:
        - Plug and Play: se encarga de permitir o no, la conexión de cualquier tipo de dispositivo
        - Removable Storage Device: se encarga de permitir o no, la utilización de un dispositivo conectado.
        - Removable Storage File Access: se encarga de permitir o no, la ejecución de archivos en un dispositivo conectado y detectado.
- Data Protection
    - Se encuentra orientada a la gestión y auditoria del tráfico de información entre la PC y el dispositivo.

5.5.1 Device Control

Al momento de configurar las reglas se partió por la configuración de los dispositivos que se podrán conectar y se definieron las siguientes reglas de Device Control – Plug and Play:

- Plug and Play – Bloquear las conexiones MTP y PTP.
- Plug and Play – Bloquear Bluetooth
- Plug and Play – Bloquear CD/DVDs
- Plug and Play – Bloquear todo disp. Almacenamiento.
- Plug and Play – Monitorea todo

Luego se procedió a configurar las reglas de Device Control – Removable Storage Device:

- Removable Storage Device – Bloquear modo almacenamiento para cámaras y celulares.
- Removable Storage Device – Bloquear todo
- Removable Storage Device – Bloquear CD/DVDs
- Removable Storage Device – Monitorea todo

Por último, se configuraron las siguientes reglas de File Access:

- Removable Storage File Access – Bloquear Ejecutables
- Removable Storage File Access – Bloquear todo menos Imágenes y videos.

5.5.1.1 Plug and Play – Bloquear las conexiones MTP y PTP.

Esta regla busca bloquear todas las conexiones del tipo MTP y PTP, utilizada por las celulares y cámaras digitales.

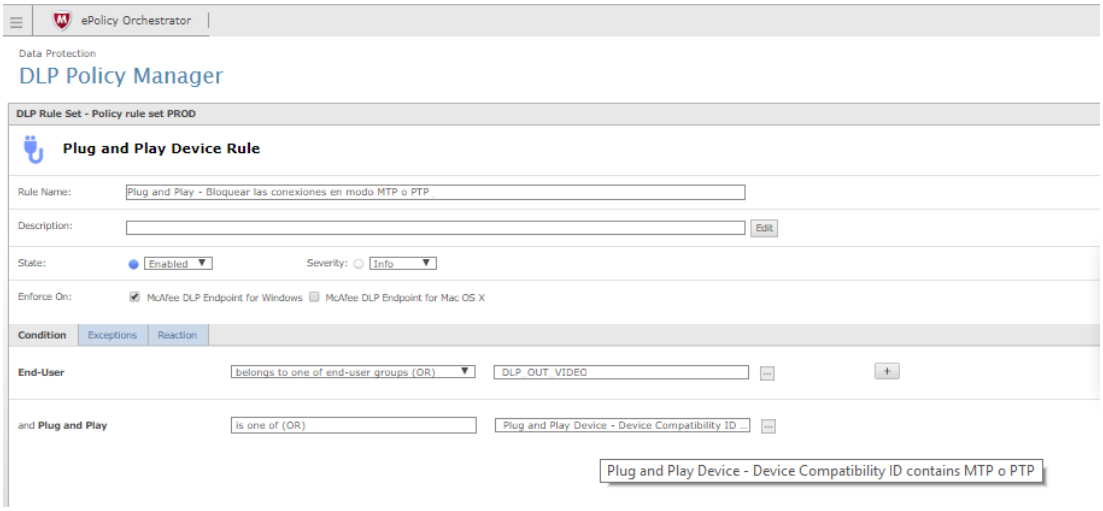

Ilustración 1 Regla Plug and Play - Bloquear las conexiones MTP y PTP - Condición

Tiene como condición que pertenezca al grupo de usuarios del caso “pasar Videos a los televisores corporativos” y que el tipo de conexión sea MTP o PTP. En la sección de excepción no se encuentra configurado nada para este caso.

5.5.1.2 Plug and Play – Bloquear Bluetooth

En este caso se bloquean todas las conexiones del tipo bluetooth ya que no están permitidas para ningún usuario.

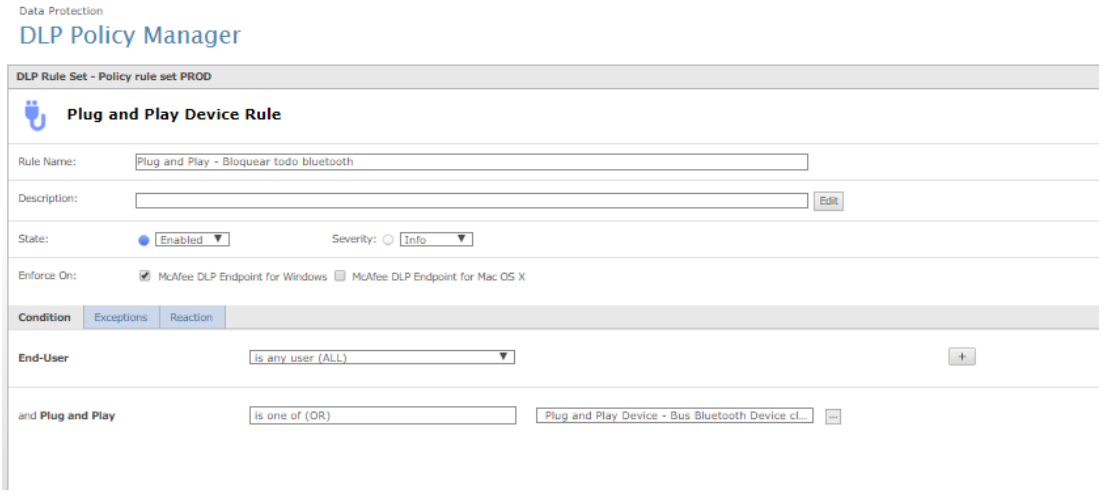

Ilustración 2 Plug and Play – Bloquear Bluetooth - Condición

El usuario final no verá ni siquiera la placa de bluetooth disponible como dispositivo.

5.5.1.3 Plug and Play – Bloquear CD/DVDs

El bloqueo de CD/DVDs es similar al de bluetooth, pero en la solapa de excepciones se encuentra configurado el grupo de usuarios que si debe contar con permisos.

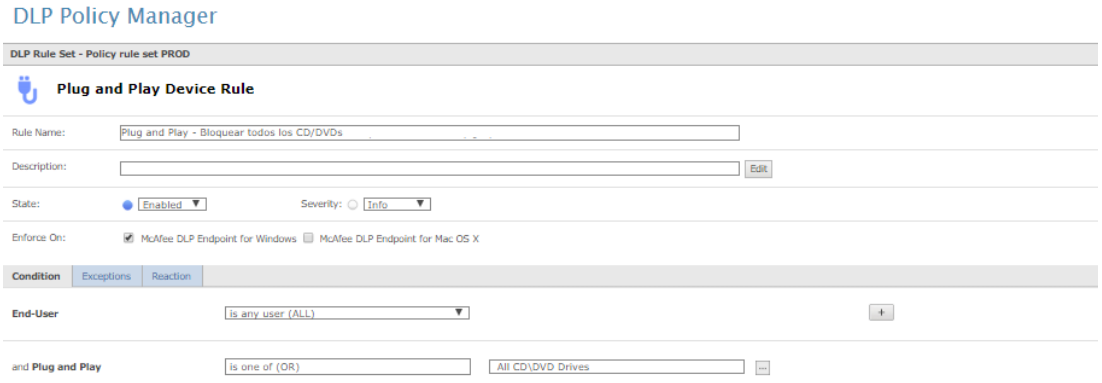

Ilustración 3 Plug and Play - Bloquear CD/DVDs - Condición

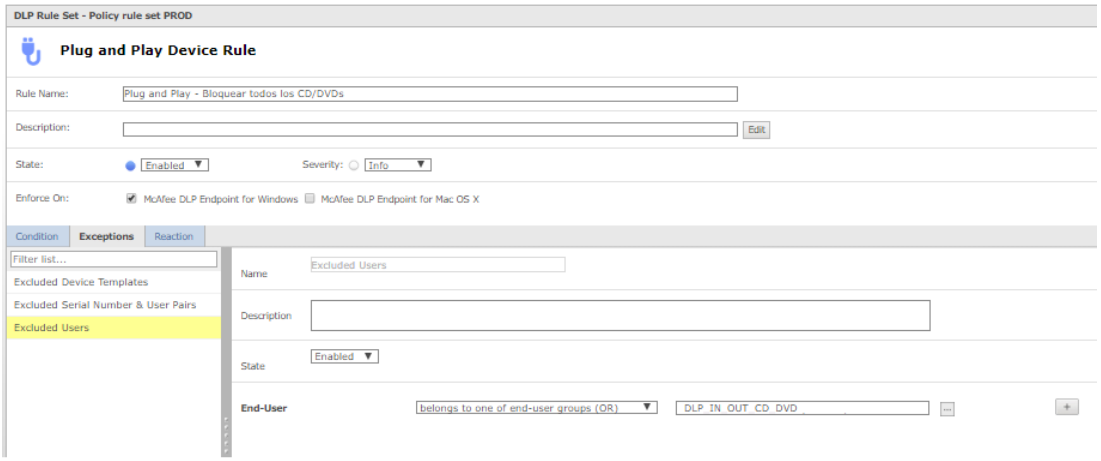

Ilustración 4 Plug and Play - Bloquear CD/DVDs – Excepción

5.5.1.4 Plug and Play – Bloquear todo disp. Almacenamiento.

Esta regla es general y busca bloquear todos los eventos de conexión, o también llamados plug and play, de todo tipo de dispositivo, a todos los usuarios excepto a los miembros de algún grupo de los que requieren un permiso en particular. El alcance son todos los usuarios de la compañía y para un grupo de dispositivos que excluye los dispositivos conectados internamente en una PC.

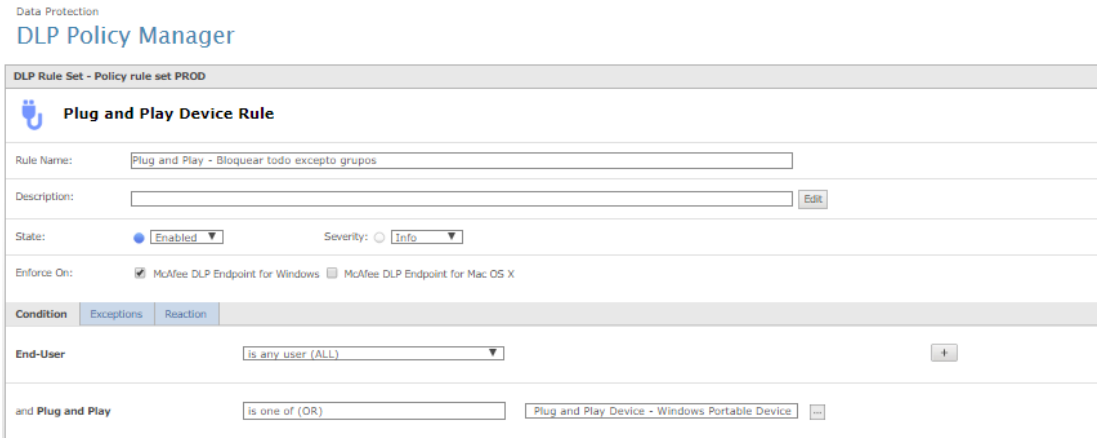

Ilustración 5 Plug and Play – Bloquear todo disp. Almacenamiento - Condición

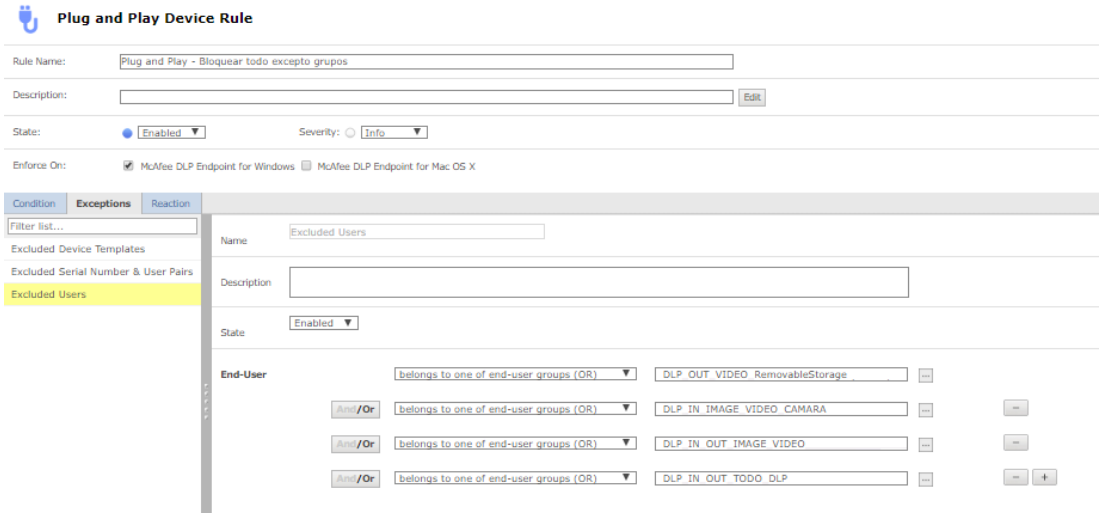

Ilustración 6 Plug and Play – Bloquear todo disp. Almacenamiento - Excepción

5.5.1.5 *Plug and Play – Monitorea todo*

Esta regla se configura con el fin de dejar registrado todo lo que conecte a una PC. Si bien las reglas anteriores registran, hay que tener en cuenta que solo registran lo que la condición dice y la excepciones no excluyen, por ende, esta regla tiene la condición más abarcativa y no tiene excepciones.

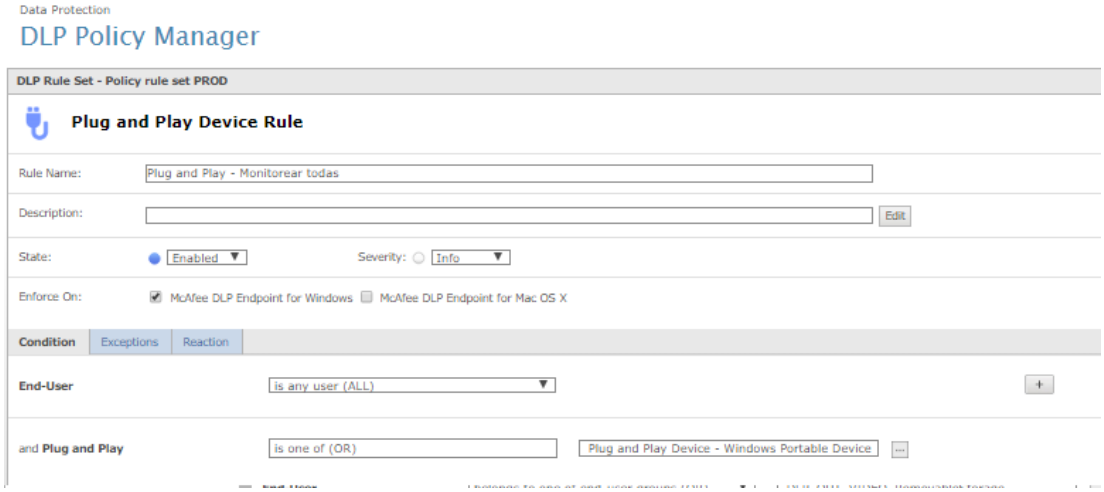

Ilustración 7 Plug and Play – Monitorea todo - Condición

5.5.1.6 *Removable Storage Device – Bloquear modo almacenamiento para cámaras y celulares*

Ya pasando a las reglas del tipo Removable Storage Device, se configura la siguiente regla para que aquellos usuarios que se le habilite el uso de cámaras digitales o celulares no puedan conectar dispositivos de almacenamiento y puedan ser utilizados. Tiene como alcance a todos los

usuarios que cuenten con el grupo de permisos para cámaras y celulares y no tiene excepciones.

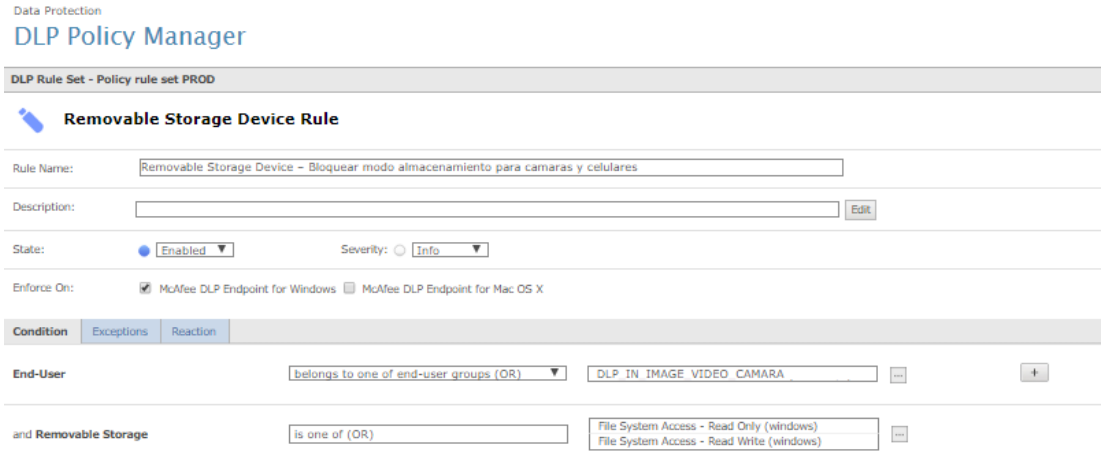

Ilustración 8 Removable Storage Device – Bloquear modo almacenamiento para cámaras y celulares - Condición

5.5.1.7 Removable Storage Device – Bloquear todo

Al igual que la regla Plug and Play – Bloquear todo, esta regla busca bloquear todo dispositivo conectado por cualquier usuario que no pertenezca a algún grupo de los exceptuados por esta misma regla. Tiene como alcance a todos los usuarios finales y a los dispositivos que permita la lectura y escritura de información en ellos.

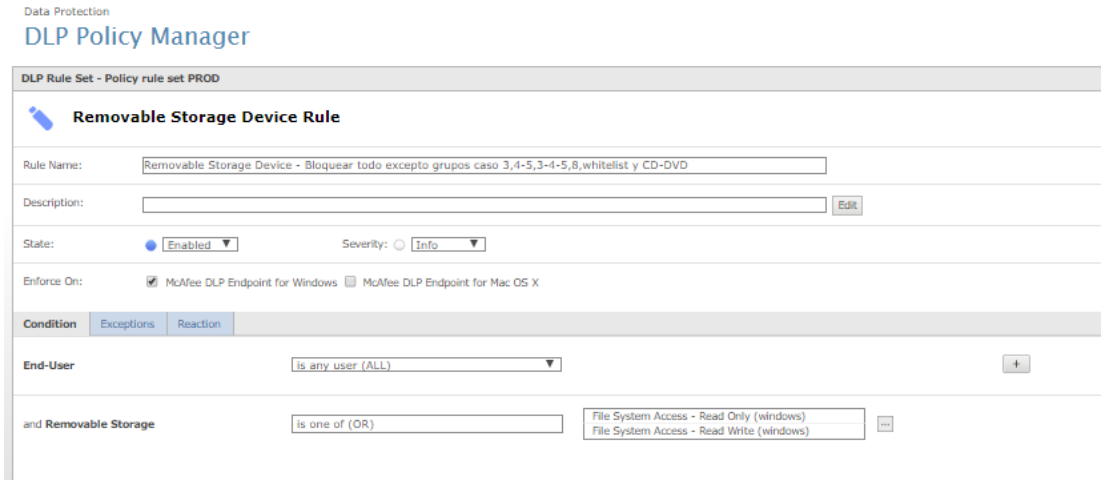

Ilustración 9 Removable Storage Device – Bloquear todo - Condición

Con respecto a las excepciones, se encuentran excluidos de esta regla a los usuarios que pertenezcan a alguno de los grupos de permisos, tal como se ve en la ilustración 10.

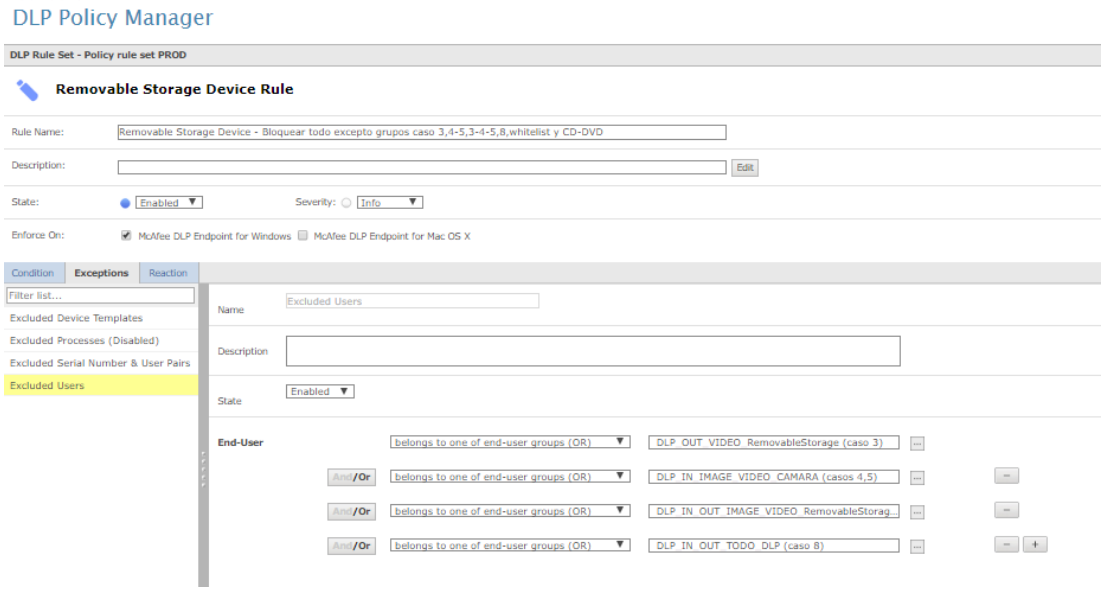

Ilustración 10 Removable Storage Device – Bloquear todo – Excepción

5.5.1.8 Removable Storage Device – Bloquear CD/DVDs

Esta regla corresponde a un segundo nivel de permiso con respecto a la lecto escritura de CDs/DVDs. Si por alguna razón la herramienta de DLP le permite el Plug and Play de una lectora de CD/DVD a un usuario no autorizado, esta segunda regla no le permitirá acceder a la misma y la arrojará un mensaje de “Acceso denegado”. Al igual que la regla a de Plug and Play de CD/DVD tiene como alcance a todos los usuarios y dispositivos de este tipo, y como excepción a los usuarios que pertenecen al grupo de autorizados a utilizar dichos dispositivos.

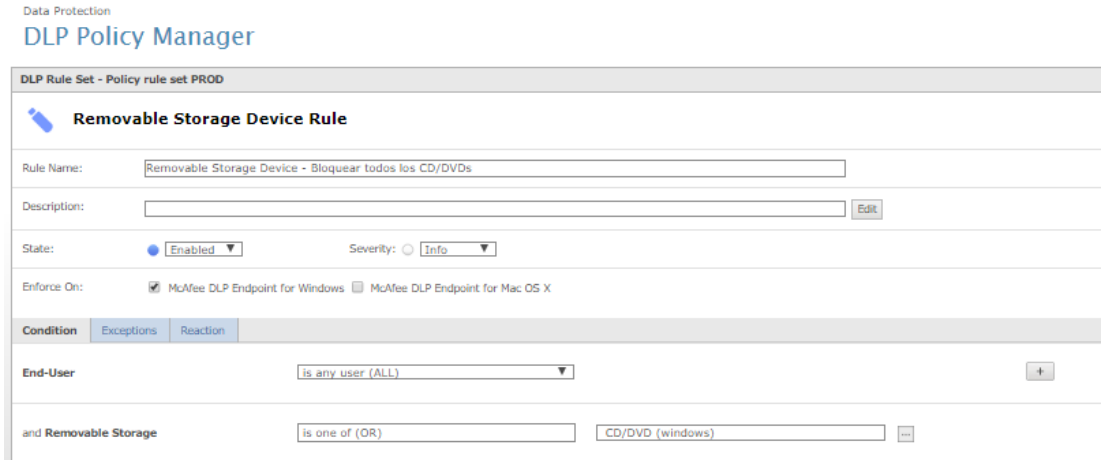

Ilustración 11 Removable Storage Device – Bloquear CD/DVDs - Condición

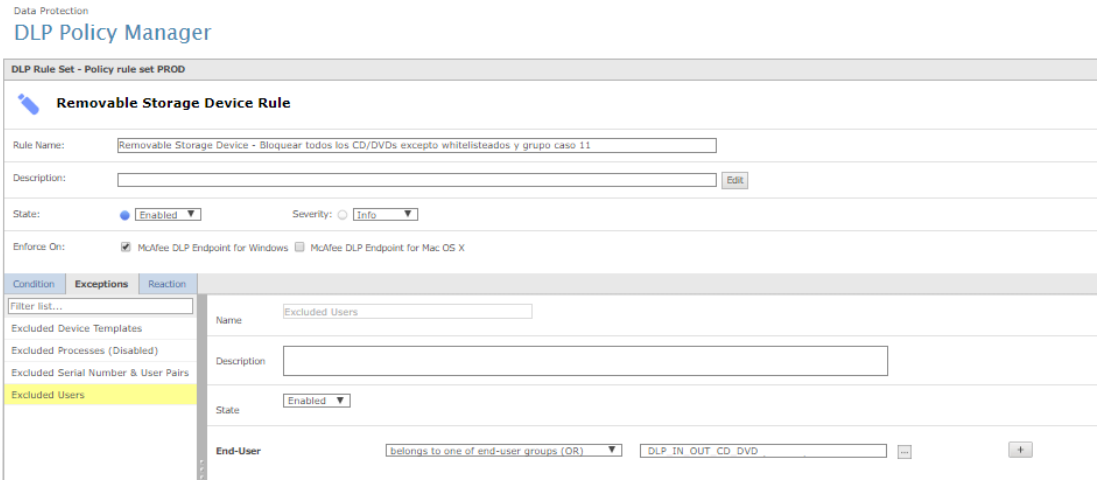

Ilustración 12 Removable Storage Device – Bloquear CD/DVDs - Excepción

5.5.1.9 Removable Storage Device – Monitorea todo

Como ultima regla, para este tipo, se configura la regla de monitoreo, con condición todos los dispositivos y sin exceptuados.

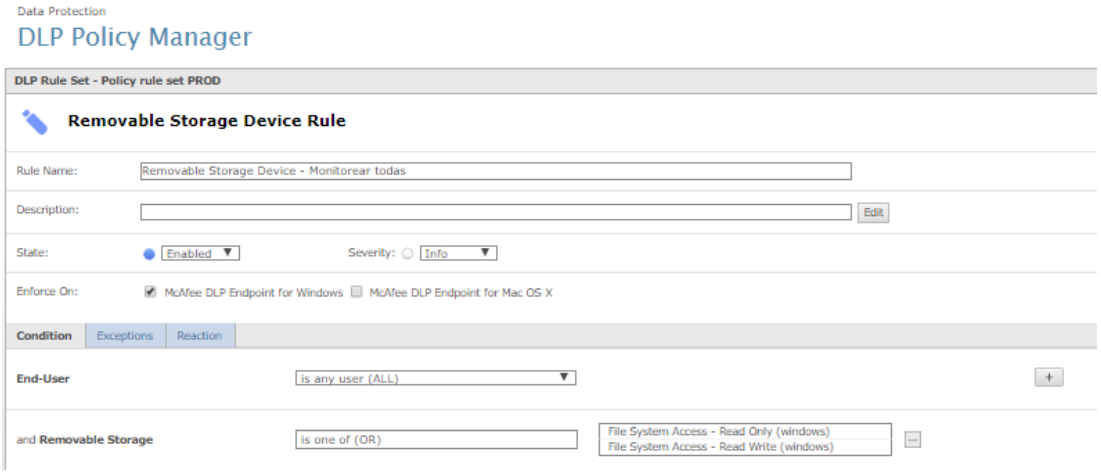

Ilustración 13 Removable Storage Device – Monitorea todo - Condición

5.5.1.10 Removable Storage File Access - Bloquear Ejecutables

Pasando al tipo de regla de File Access, se definió una de las reglas mas importantes, la cual tiene como objetivo principal la ejecución de Malware o cualquier tipo de archivo malicioso desde el dispositivo. Para ello se bloquea el acceso, copia y ejecución de cualquier tipo de archivo ejecutable o script. Esta regla tiene como varias de las anteriores un doble control de archivo, ya que mira por extensión de archivo y por True File Type. A diferencia de las otras reglas, para esta no hay excepción, es decir todo usuario se verá afectado por esta regla, en caso de requerir acceso a un archivo ejecutable

que se encuentre en un medio de almacenamiento externo, se deberá buscar otra alternativa en la nube para ello.

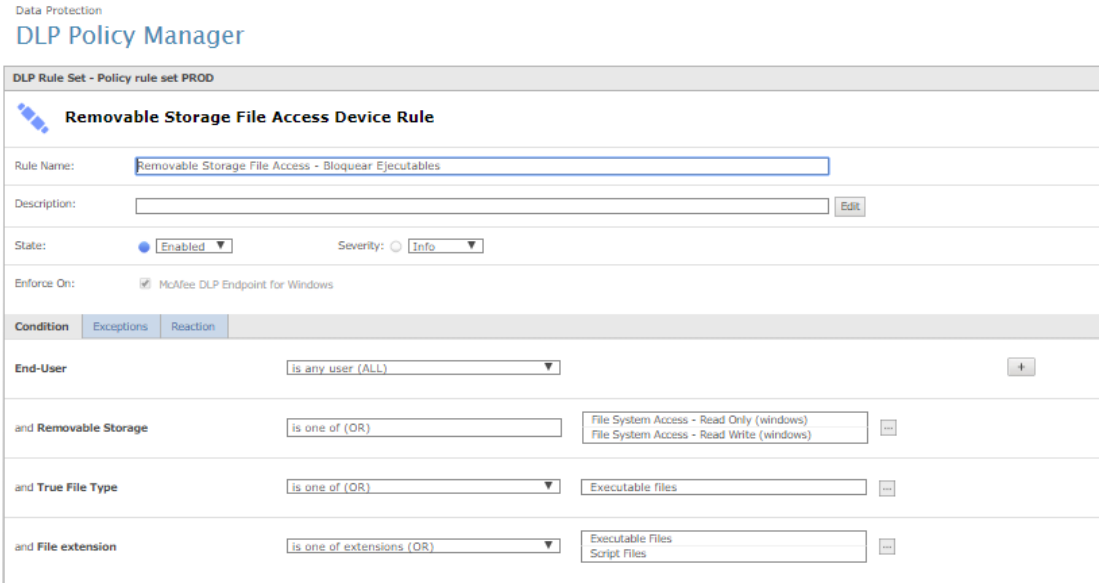

Ilustración 14 Removable Storage File Access - Bloquear Ejecutables - Condición

5.5.1.11 Removable Storage File Access - Bloquear todo menos Imágenes y videos

Esta regla al igual que la anterior busca impedir la ejecución y copia de cierto tipo de archivos. Básicamente lo hace sobre todos los tipos de archivos y extensiones que no sean imágenes y videos. La única excepción es un grupo de usuarios que se ve reflejado en la ilustración 16.

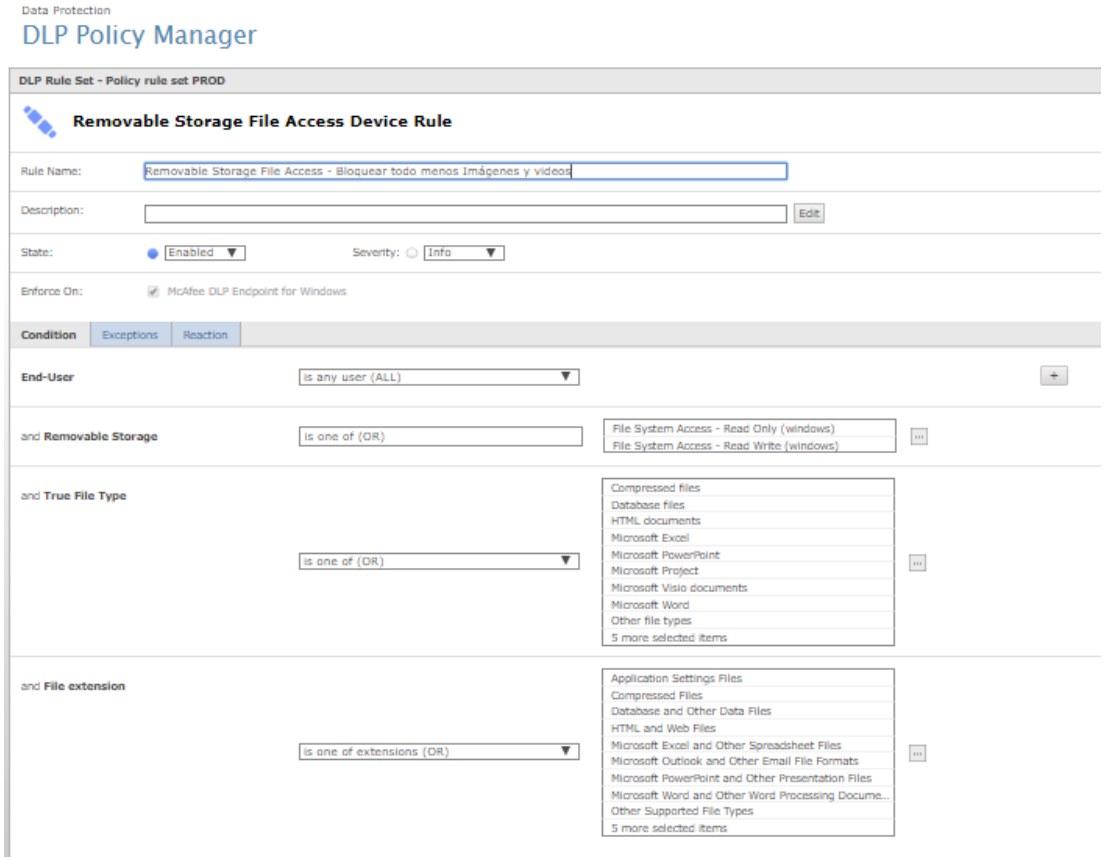

Ilustración 15 Removable Storage File Access - Bloquear todo menos Imágenes y videos - Condición

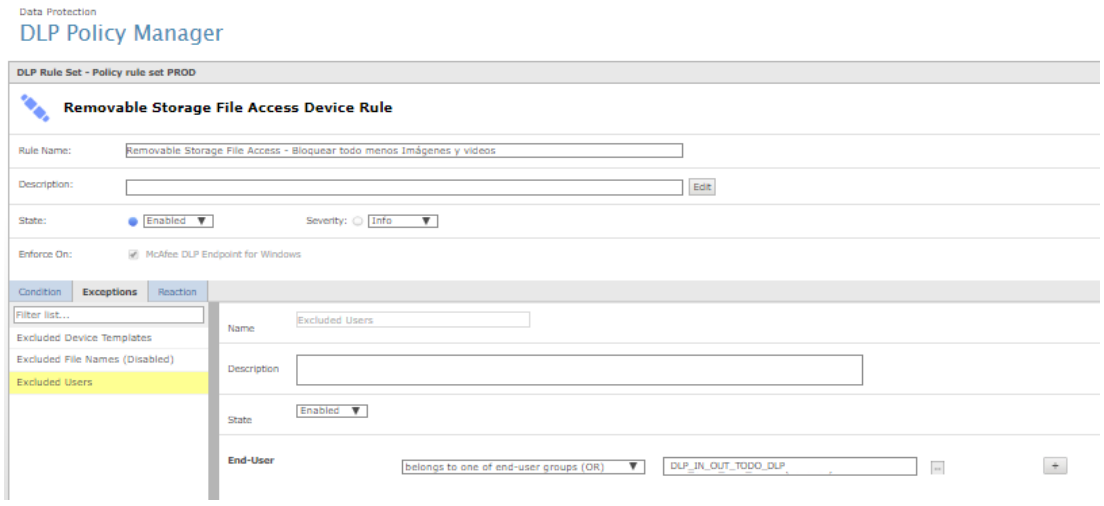

Ilustración 16 Removable Storage File Access - Bloquear todo menos Imágenes y videos - Excepción

5.5.2 Data Protection

El otro grupo de reglas que complementa a las reglas de Device Control, son las de Data Protection. Estas buscan controlar y monitorear el tráfico

saliente y/o entrante de información a los distintos dispositivos. En esta sección se generaron las siguientes reglas:

- Data Protection - Bloquear copia hacia y desde todos los almacenamientos excepto CD/DVD
- Data Protection - Bloquear copia hacia y desde todos los CD/DVD
- Data Protection - Monitorear copia imagen-video desde todos los almacenamientos.
- Data Protection - Monitorear copia imagen-video desde-hacia los almacenamientos
- Data Protection - Monitorear copia todo desde-hacia todos los almacenamientos
- Data Protection - Monitorear copia todo desde-hacia todos los CD/DVD
- Data Protection - Monitorear copia video hacia todos los almacenamientos

En esta categoría de regla es necesario configurar una regla de bloqueo por cada tipo de medio de almacenamiento (Almacenamiento Extraíble o CD) y dentro de ellas se hacen excepciones y luego por cada excepción hay que hacer una regla de monitoreo para auditar todo lo que se transfiera.

5.5.2.1 Data Protection - Bloquear copia hacia y desde todos los almacenamientos excepto CD/DVD

La principal regla de Data Protection busca bloquear todo el trafico de información, ya sea entrante (inbound) o saliente (outbound), exceptuando a los miembros de los distintos grupos de usuarios autorizados.

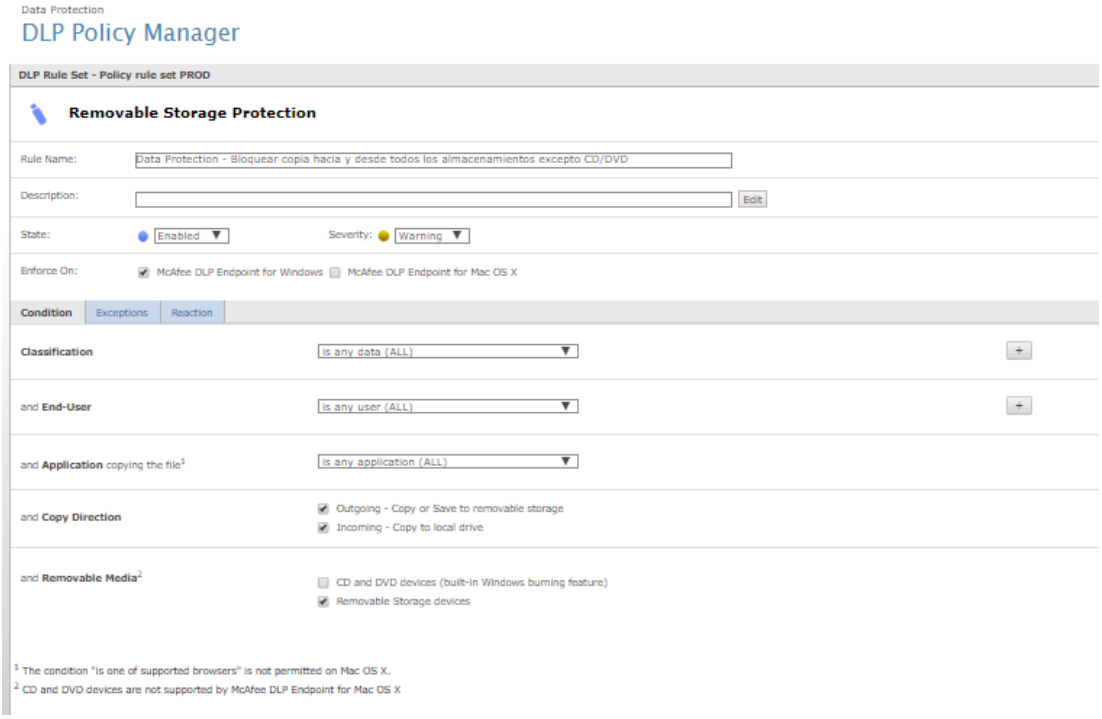

Ilustración 17 Data Protection - Bloquear copia hacia y desde todos los almacenamientos excepto CD/DVD - Condición

La primera de las excepciones hace referencia a la regla definida para el uso de cámaras digitales donde estamos permitiendo el tráfico entrante (Desde el dispositivo a la PC), solo a los miembros del grupo de autorizados para esta acción y que sea ejecutado por el proceso explorer.exe, es decir, no se pueden usar programas para descargar las imágenes. En los dispositivos Celulares o Cámaras Digitales el tráfico es detectado de manera inversa (Ingoing lo toma como Outgoing y viceversa).

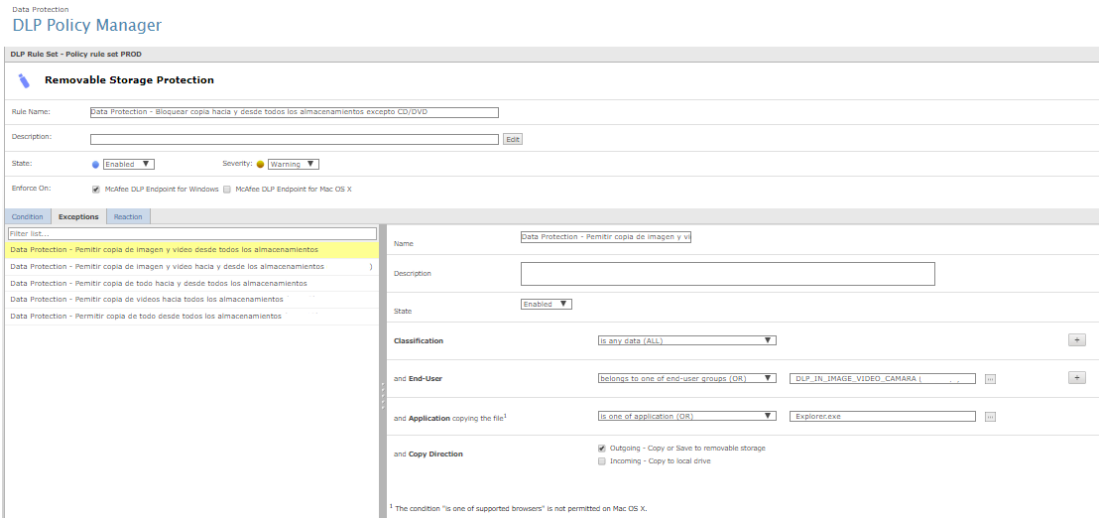

Ilustración 18 Data Protection - Bloquear copia hacia y desde todos los almacenamientos excepto CD/DVD - Primera Excepción

La segunda excepción hace referencia al permiso para descargar archivos de una cámara y al mismo tiempo pasar Imágenes y videos a memorias extraíbles. En el tipo de archivo permitimos solo Imágenes y videos y nuevamente en proceso solo se permite, explorer.exe.

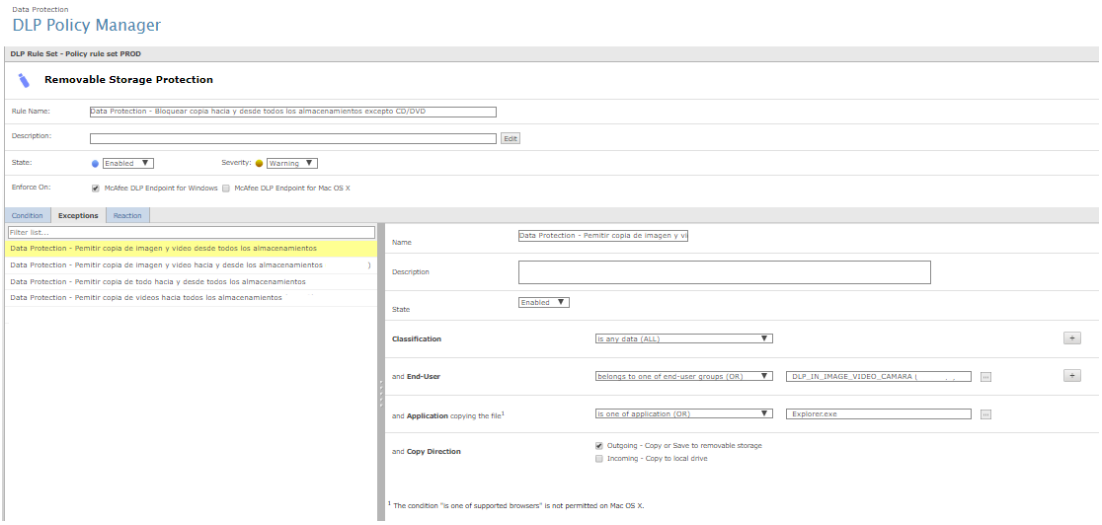

Ilustración 19 Data Protection - Bloquear copia hacia y desde todos los almacenamientos excepto CD/DVD - Segunda Excepción

La tercera excepción hace referencia al grupo que no debe contar con restricciones de transferencia de archivos, solo ejecutables se le restringe, pero por otra regla. Por lo que en tipo de archivo se permiten todos tanto para tráfico entrante como saliente.

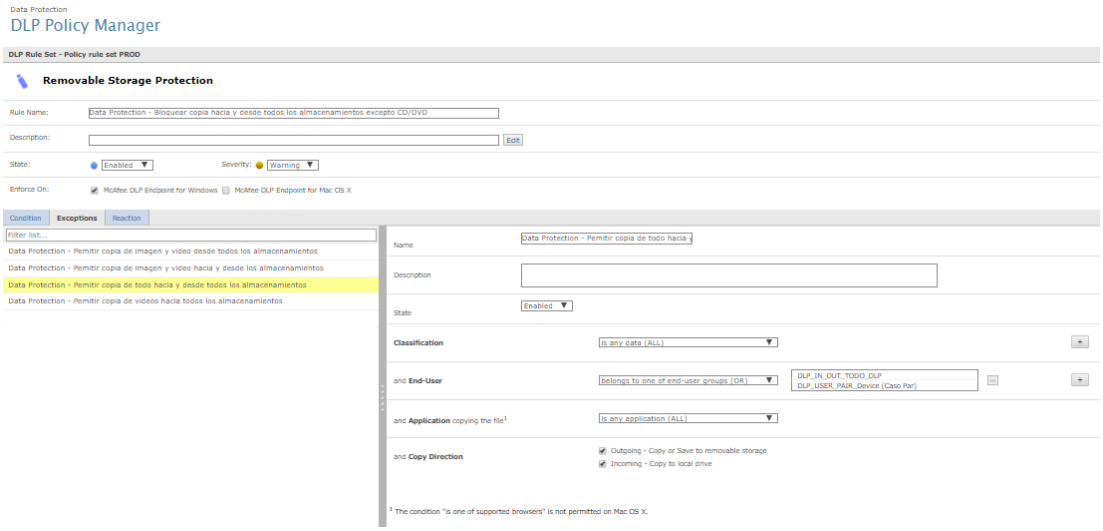

Ilustración 20 Data Protection - Bloquear copia hacia y desde todos los almacenamientos excepto CD/DVD - Tercera Excepción

La cuarta excepción fue definida para el caso de trafico saliente de videos a dispositivos de almacenamiento. Por lo que el tipo de archivo es de video y solo tráfico outgoing.

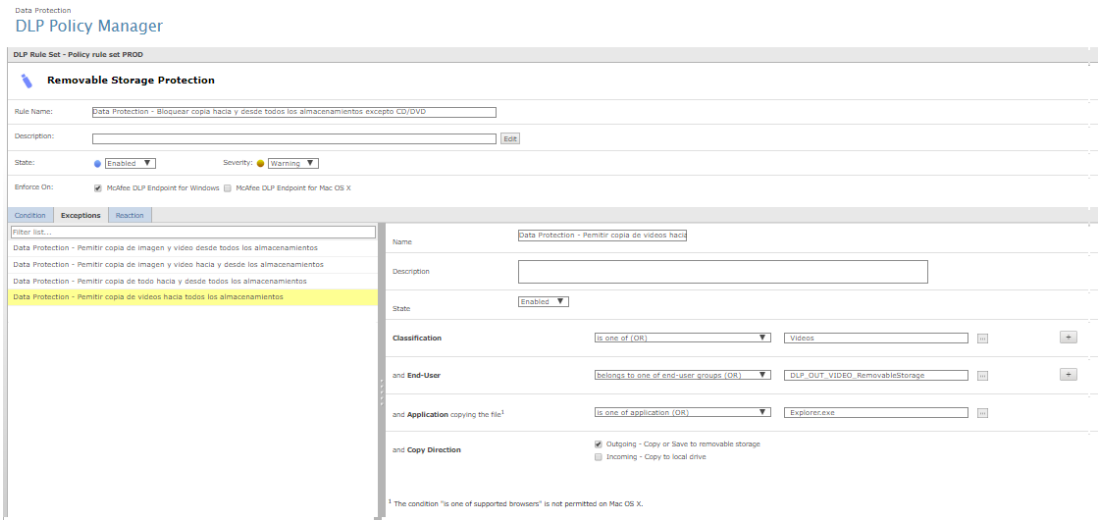

Ilustración 21 Data Protection - Bloquear copia hacia y desde todos los almacenamientos excepto CD/DVD - Cuarta Excepción

5.5.2.2 Data Protection - Bloquear copia hacia y desde todos los CD/DVD

Como segunda regla, se definió una idéntica a la anterior pero solo para CD/DVD. Básicamente esta regla bloquea el tráfico entrante y saliente a CDs/DVDs excepto usuarios miembros del grupo de autorizados.

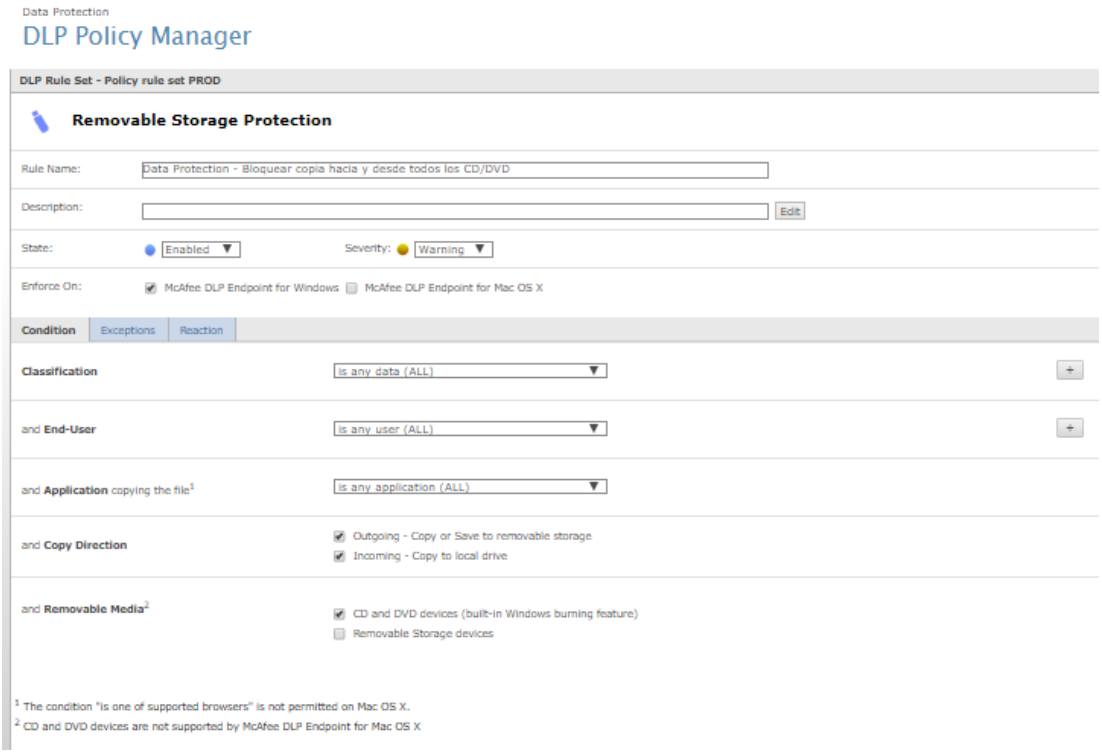

Ilustración 22 Data Protection - Bloquear copia hacia y desde todos los CD/DVD - Condición

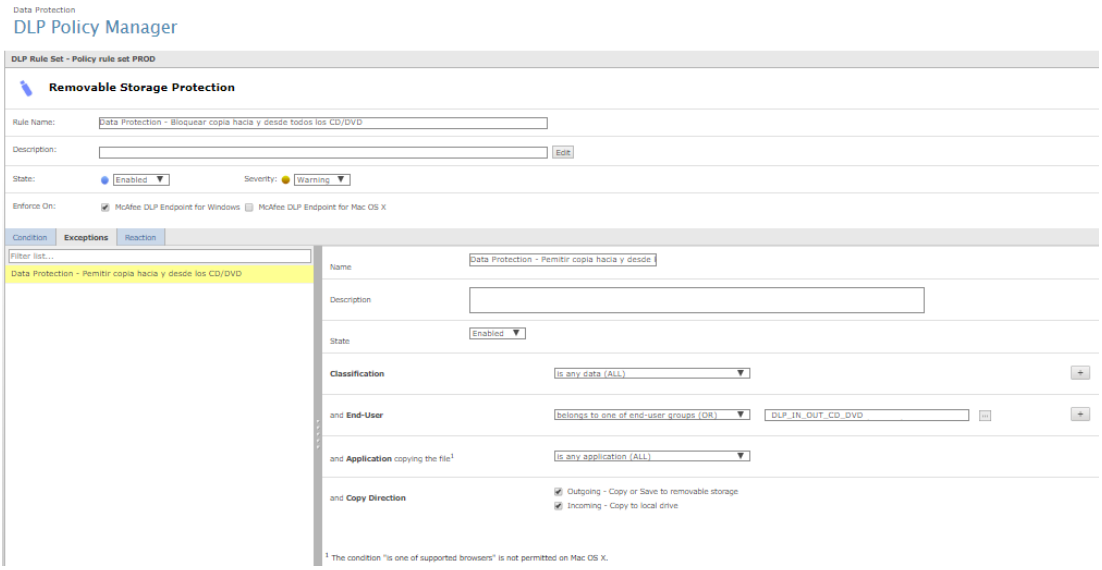

Ilustración 23 Data Protection - Bloquear copia hacia y desde todos los CD/DVD – Excepción

5.5.2.3 Data Protection - Monitorear copia imagen-video desde todos los almacenamientos

Toda excepción cargada para las reglas de bloqueo de Data Protection, debe contar con una regla de monitoreo. Esto se debe a que las excepciones en reglas de bloqueo permiten la transferencia de información, pero no deja registro de lo que se transfiera, es por lo que por cada excepción se crea una regla de monitoreo idéntica a la excepción, pero en vez de bloquear, audita, o como lo llama la herramienta Acción “No Action” y el campo Report Incident habilitado.

En este caso se configuró el monitoreo para los tipos de archivo Imagen y Video para los usuarios que tengan el grupo correspondiente para esta acción.

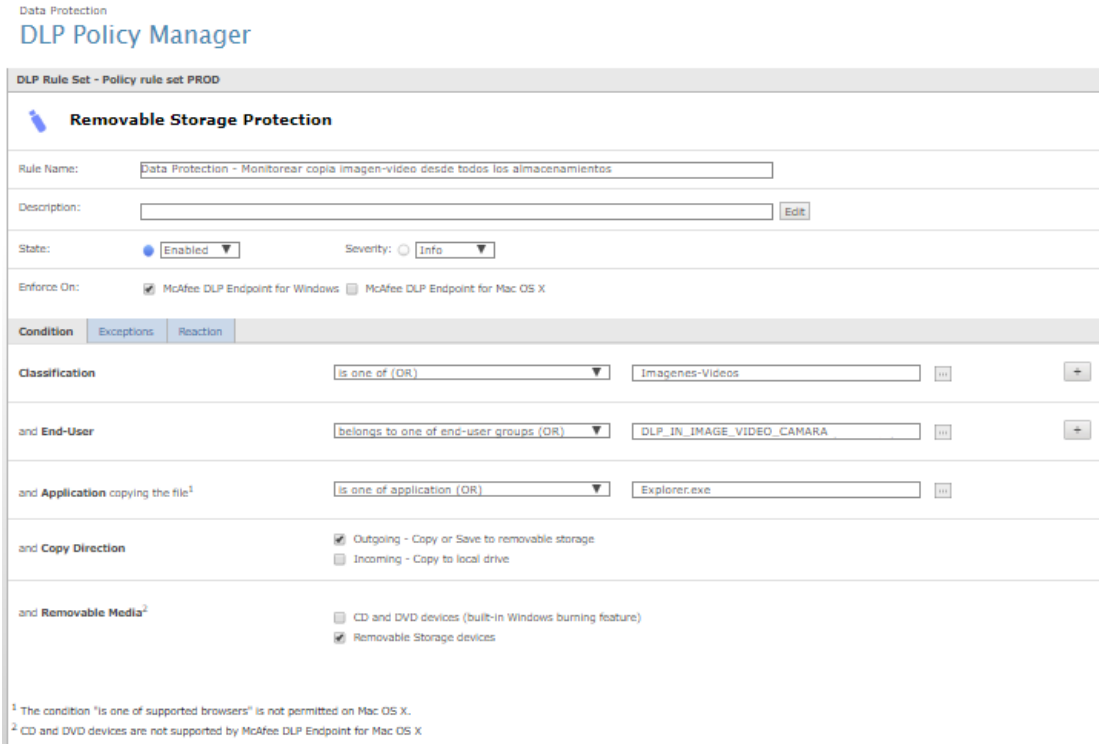

Ilustración 24 Data Protection - Monitorear copia imagen-video desde todos los almacenamientos - Condición

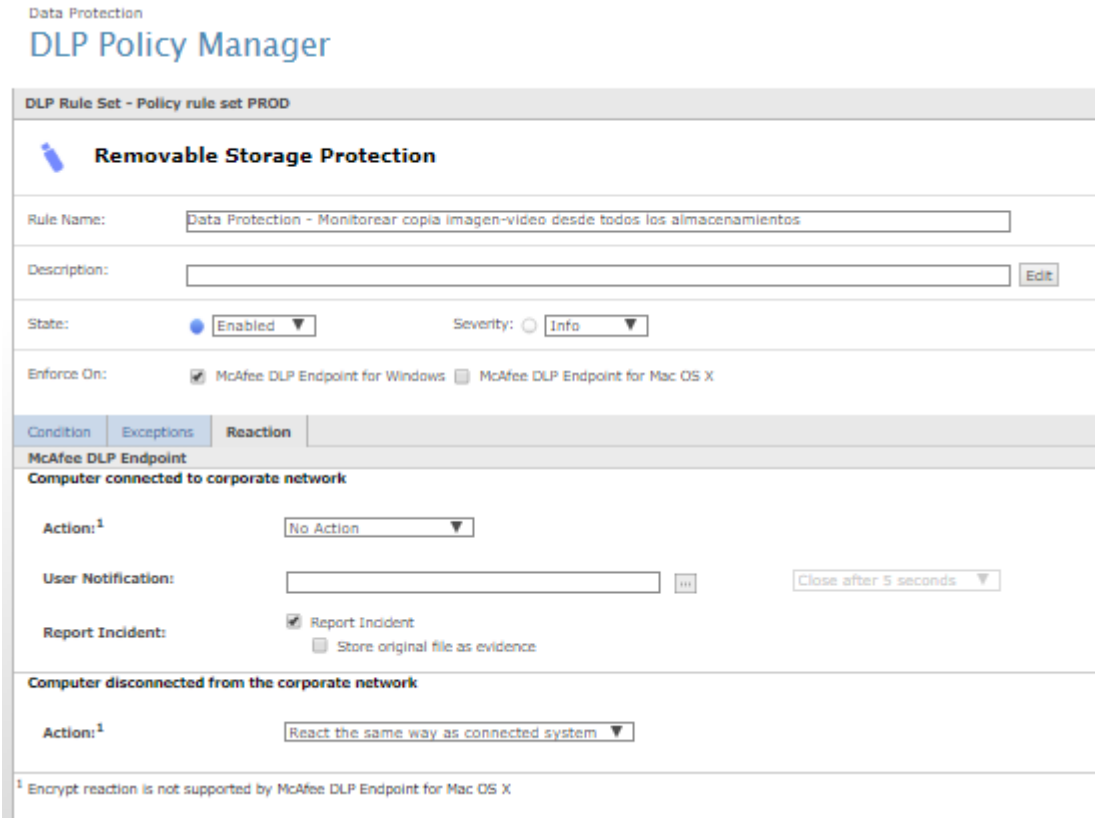

Ilustración 25 Data Protection - Monitorear copia imagen-video desde todos los almacenamientos - Reacción

5.5.2.4 Data Protection - Monitorear copia imagen-video desde todos los almacenamientos

Al igual que la regla anterior, se basa todo en las excepciones de las reglas de bloqueo.

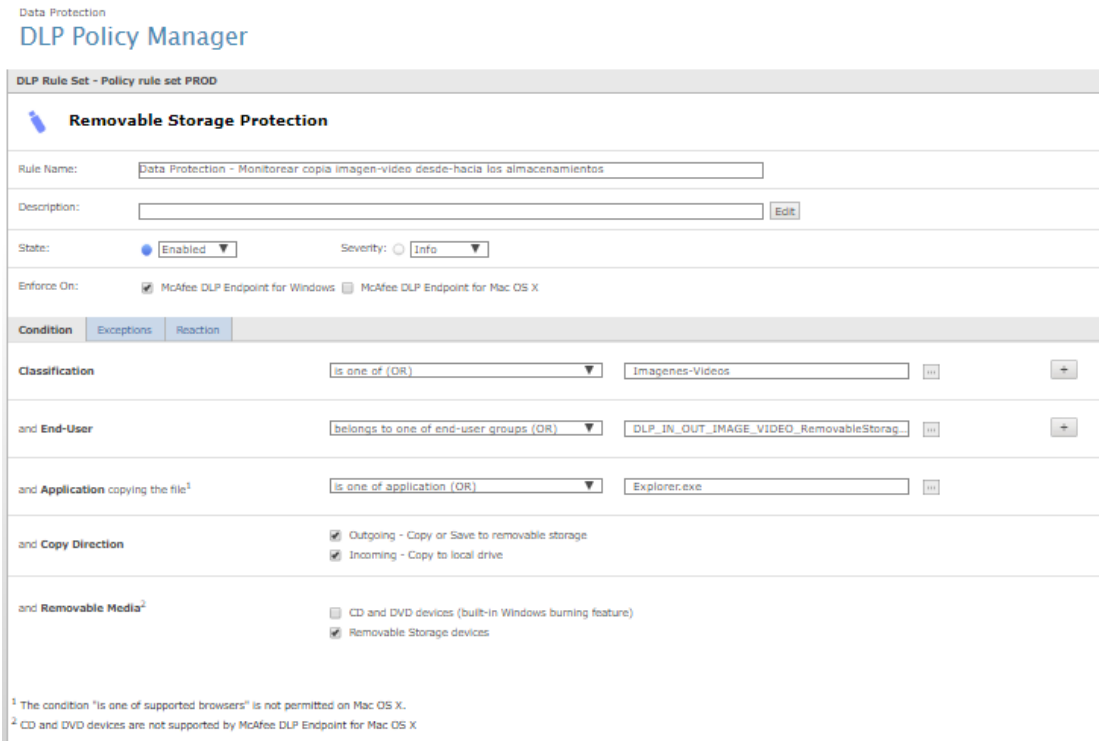

Ilustración 26 Data Protection - Monitorear copia imagen-video desde todos los almacenamientos - Condición

5.5.2.5 Data Protection - Monitorear copia todo desde-hacia todos los almacenamientos

Regla de monitoreo para el grupo de usuarios que puede transferir cualquier tipo de archivos excepto ejecutables y scripts.

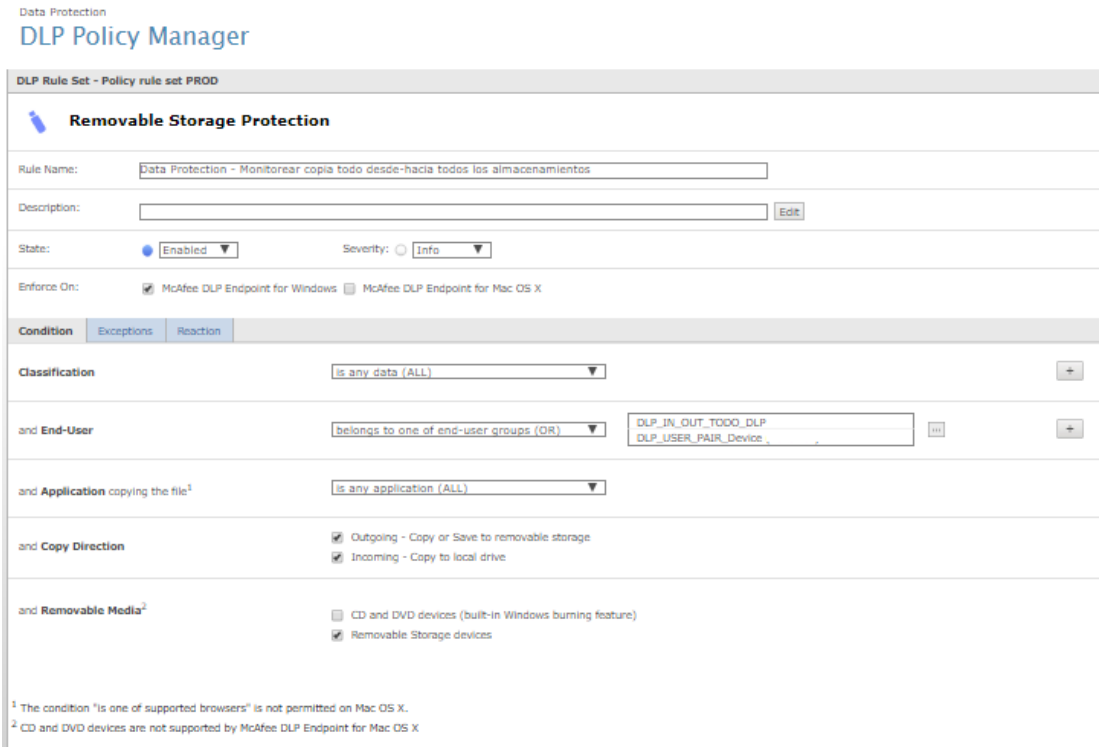

Ilustración 27 Data Protection - Monitorear copia todo desde-hacia todos los almacenamientos - Condición

5.5.2.6 Data Protection - Monitorear copia todo desde-hacia todos los CD/DVD

Regla de monitoreo de todo el trafico entrante y saliente en los medios de almacenamiento del tipo CD/DVD.

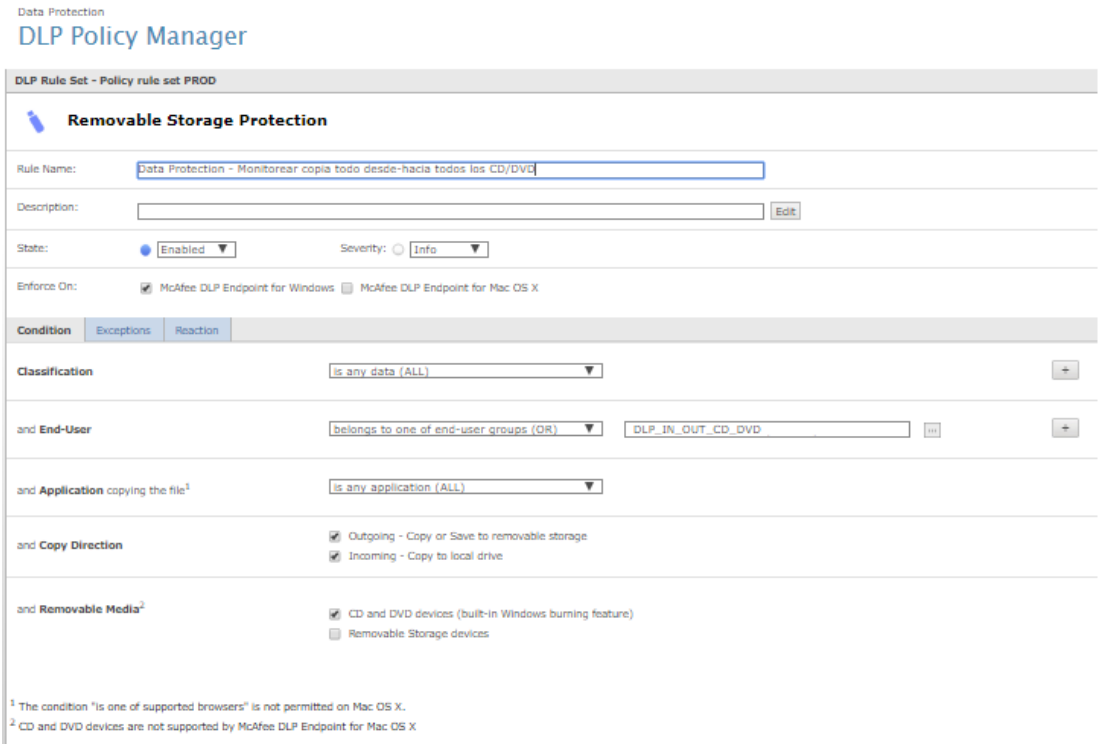

Ilustración 28 Data Protection - Monitorear copia todo desde-hacia todos los CD/DVD - Condición

5.5.2.7 Data Protection - Monitorear copia video hacia todos los almacenamientos

Por último, se configuró la regla asociada a la ultima excepción de bloqueo, que monitorea el trafico de los miembros del grupo de autorizados a extraer archivos del tipo videos.

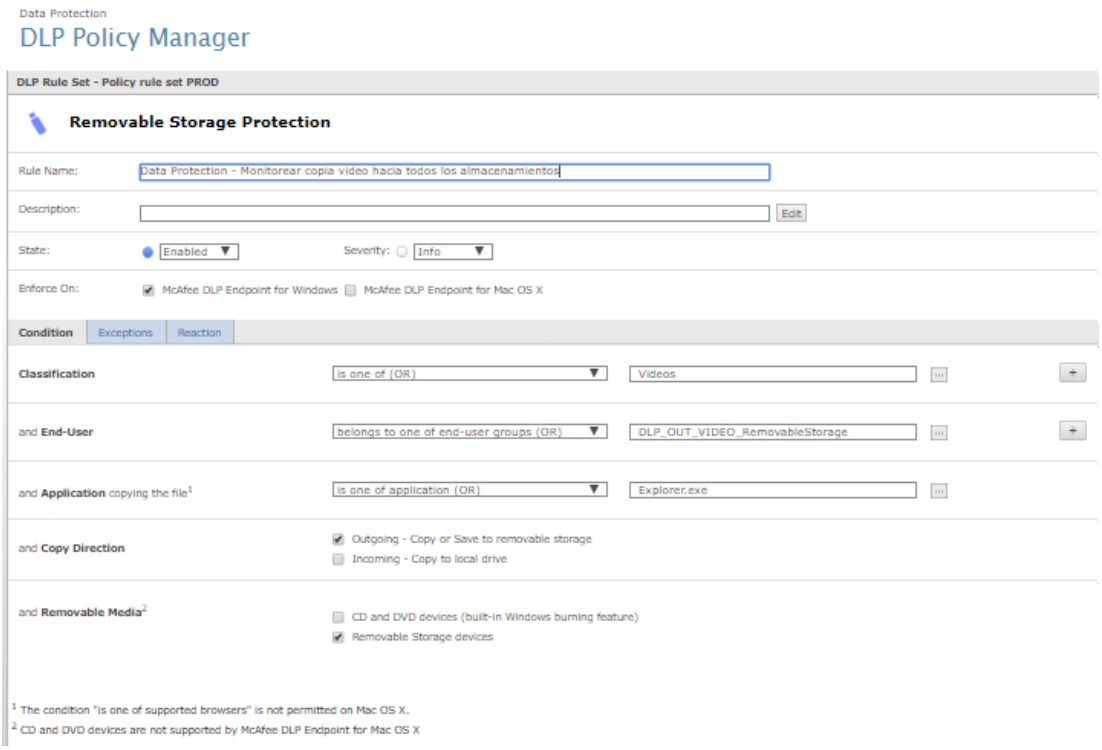

Ilustración 29 Data Protection - Monitorear copia video hacia todos los almacenamientos - Condición

5.7 Etapa de implementación

Una vez configuradas todas estas reglas, se procedió a hacer una precarga de usuarios, a los grupos de permisos para áreas críticas que se conoce que cuentan con la necesidad diaria de utilizar de alguna u otra manera los puertos USB.

El lanzamiento fue acompañado por una serie de videos para poder concientizar a los usuarios acerca de los riesgos que se corren al no implementar este proyecto.

Las primeras dos semanas del lanzamiento de la nueva política de permisos, se contó con un soporte dedicado, para dar respuesta a todos los pedidos que puedan surgir.

6 Logros, Contratiempos y Mejoras Futuras

6.1 Logros

Como resultado de este proyecto se obtuvieron varios cambios positivos que redujeron considerablemente el impacto y la probabilidad de ciertos riesgos.

Por un lado, no se encuentra habilitada la ejecución o manipulación de archivos ejecutables o de scripting desde dispositivos USB. Esto implica que los malwares que vengan embebidos en ejecutables o bien en su ejecución intente llamar a este tipo de archivos, no podrá hacerlo. Si bien estos tipos de archivos puede ser transportados de manera comprimida (.zip), una vez que se pasen a la PC, ya otra herramienta de control va a actuar. La idea de esto fue solo limitar la ejecución desde el dispositivo.

Por otro lado, se logró concentrar el trafico de información a medios en la nube como ser OneDrive y Sharepoint, ya sea para usuarios internos como externos a la compañía. Esto nos permite tener una trazabilidad de la información que se comparte, para que en caso de que ocurra un incidente, pueda contarse con una auditoria de dicho archivo.

Por último, se logró concientizar a los usuarios que realizaban backup de información histórica, y en muchos casos, de suma importancia, en medios de almacenamiento USB, sin contar con seguridad alguna o alta disponibilidad de los mismos. En estos casos se les ofreció nuevamente utilizar las herramientas de Office365, OneDrive y sitios de Sharepoint.

6.2 Contratiempos

Si bien no hubo un gran contratiempo que haya llevado a demorar el lanzamiento del proyecto, se detectaron casos de uso de dispositivos USB o lectoras de CD/DVD sobre la fecha de lanzamiento o hasta pasada la misma, que no habían sido detectados en las fases de relevamiento. En algunos casos se hicieron excepciones por haber limitantes legales, ya que el 100% de los casos correspondía a compartir información con entes del gobierno o entes regulatorios que solicitan que la información sea enviada en el formato que ellos indican.

6.3 Mejoras Futuras

Para un futuro se propone por cada grupo de permisos, buscar alternativas para poder realizar las acciones sin tener que contar con permisos USB y dispositivos de este tipo.

Para el caso de la copia de archivos de videos para compartir en las TVs corporativas o de planta, se propone implementar un sistema centralizado que, por medio de una consola central, se pueda compartir el contenido que se desee en cada TV de la compañía.

Para los casos de descarga de información de CCTV, se propone armar una VLAN separada de la red productiva en la cual se conecten todos los controladores de CCTV o DVRs y que los encargados de controlar o extraer información de los mismos, pueda conectarse a los mismos por este medio.

Por último, se propone reforzar las capacitaciones sobre el uso de las herramientas en la nube para compartir información. Mas que nada en los altos niveles jerárquicos que en varias ocasiones solicitan excepciones a las reglas por el nivel que tienen, porque necesitan extraer una presentación. Cuando podrían presentar desde su dispositivo móvil o desde su misma notebook.

7 Conclusión

El hecho de contar con una política de uso de dispositivos de almacenamiento extraíble ya no debería ser una opción. Para poder reducir los riesgos de ataques a nuestros sistemas, debemos reducir los vectores de ataques por los cuales los diferentes atacantes pueden llegar a ingresar o afectar a nuestros sistemas, y los dispositivos de almacenamiento como pendrives, son unos de los vectores más riesgosos para nuestra organización.

Tomar la decisión de segurizar, de manera efectiva, el uso de los dispositivos de almacenamiento extraíble, en un ambiente corporativo, me llevó a reducir en un 100% la entrada de malware por este medio, ya que se encuentra bloqueado todo tipo de interacción con archivos ejecutables, y el archivo infectado no es ejecutable, al copiarse a la PC, sería detectado en la misma PC por el antivirus. Como otro punto a destacar, se logró que los usuarios no manejen información de la empresa en medios de almacenamiento que puede extraviarse y/o caer en manos equivocadas. Cabe aclarar que este proyecto fue acompañado de la implementación de soluciones en la nube que ayudaron a cubrir las distintas necesidades que previo a este proyecto, eran cubiertas por dispositivos de almacenamiento extraíbles. Otro de los valores destacables es que el numero de usuarios habilitados a utilizar algún tipo de dispositivo de almacenamiento, bajo en un 80%, y dentro de ese 20%, los permisos con los que se cuenta son limitados y controlados por el agente de Data Loss Prevention (DLP). Por último, si por alguna razón llegará a pasar algún tipo de incidente, ya sea fuga de información o bien algún tipo de infección, todo quedaría registrado en el sistema de DLP.

Ejecutar una configuración de este tipo implica realizar un gran análisis para reducir el impacto en los usuarios finales, pudiéndoles brindar alternativas para poder seguir trabajando de manera correcta. Si bien, la reacción de los usuarios durante todo el proyecto no fue positiva, con el pasar del tiempo se van dando cuenta de la mejora que traen las alternativas brindadas, ya que además de que buscan evitar el uso de dispositivos de almacenamiento extraíble, buscan implementar soluciones modernas,

generalmente basadas en tecnología en la nube y con mecanismo de Segurización acorde al momento y la situación a nivel mundial.

En resumen, no hay que tomar este cambio como un simple proyecto de bloqueo de puertos USB, sino como un cambio en la cultura de los usuarios para llevarlos al uso de herramientas mas seguras y con tecnología mas moderna como ser las soluciones en la nube de Office365 para compartir o distintas herramientas de otras marcas. Si no se considera esto, los usuarios buscarán otras maneras de seguir intercambiando información corporativa por medios no seguros.

8 Bibliografía

[1] Device Control. Control and monitor access rights for USB, FireWire, Thunderbolt, etc. and protect data against loss or theft. (Consultada 25/09/2018)

https://www.endpointprotector.com/solutions/usb-lockdown-for-mac

[2] USB monitoring by DLP. (Consultada 26/09/2018)

https://www.symantec.com/connect/forums/usb-monitoring-dlp

[3] Removable device protection and USB data security “Prevent unauthorized use of removable media”. (Consultada 26/09/2018)

https://www.mcafee.com/enterprise/en-in/products/device-control.html

[4] What can I protect? (Consultada 26/09/2018)

https://www.websense.com/content/support/library/data/v84/help/protection_options.aspx