
**Universidad Autónoma del Estado de México**

Centro Universitario UAEM Valle de Chalco

# IMPLEMENTACIÓN DE SOFTWARE MCAFEE PARA LA SEGURIDAD INFORMÁTICA DE UNA PLANTA AUTOMOTRIZ DE PUEBLA

# MEMORIA DE EXPERIENCIA LABORAL

**QUE PARA OBTENER EL TÍTULO DE**

***INGENIERO EN COMPUTACIÓN***

**P R E S E N T A**

FRANCISCO JAVIER DE LA MORA SANTANDER

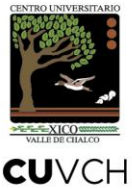
**ASESOR:**

DRA. CRISTINA JUAREZ LANDIN

Revisor: MTRO José Ramon Silverio Garcia Ibarra

Revisor: L.I.A Juan Carlos Cisneros Rasgado

**VALLE DE CHALCO SOLIDARIDAD, MÉXICO FEBRERO 2023.**



# IMPLEMENTACIÓN DE SOFTWARE MCAFEE PARA LA SEGURIDAD INFORMÁTICA DE UNA PLANTA AUTOMOTRIZ DE PUEBLA

# ÍNDICE

# I. RESUMEN

Los negocios hoy en día requieren de una solución en la cual sea posible manejar la seguridad de forma centralizada, además de proveer protección en contra de diversas amenazas y problemas relacionados con la productividad en los negocios.

Dado el aumento del número de cibercriminales que se mueven por intereses lucrativos y la naturaleza sofisticada de las amenazas actuales, gestionar la seguridad y controlar la conectividad de los equipos de escritorio y portátiles en una organización es cada vez más difícil. Los empleados gozan de mayor movilidad, lo que ha aumentado la presión sobre el equipo de TI para garantizar que se conecten con seguridad a la red de la empresa. Además, las empresas necesitan protección de tipo zero-day contra las amenazas, para ganar tiempo que les permita priorizar, probar y desplegar los parches necesarios de manera adecuada.

Las soluciones de **McAfee** hacen visibles las amenazas y protegen frente al malware de forma incomparable, e incluyen protección de endpoints y sistemas, seguridad de redes, seguridad en la nube, seguridad de bases de datos, detección y respuesta en endpoints y protección de datos.

La plataforma **McAfee® ePolicy Orchestrator® (McAfee® ePO™)** permite la administración e implementación de directivas centralizada en endpoints y productos de seguridad empresariales. McAfee ePO supervisa y administra la red para detectar amenazas y proteger a los endpoints frente a ellas.

Con McAfee ePO se pueden llevar a cabo numerosas tareas cliente y de red desde una única consola:

- Administrar e implementar la seguridad de la red y del sistema mediante asignaciones de directivas y tareas cliente.
- Supervisa el mantenimiento de su red.
- Recopilar datos sobre eventos y alertas.
- Crear informes mediante el generador de consultas del sistema, el cual muestra gráficos y tablas configurables de los datos sobre la seguridad de la red.

- Automatizar los despliegues de productos, las instalaciones de parches y las actualizaciones de seguridad el usuario para los sistemas gestionados desde el repositorio principal.

El software McAfee ePO proporciona una administración flexible y automatizada para identificar amenazas y problemas de seguridad, y responder con rapidez ante ellos. La única vista de McAfee ePO permite acceder a los clientes gestionados, las redes, los datos y las soluciones de conformidad para proteger su red La implementación de McAfee ePO fue derivado a la actualización de los componentes de la protección de antimalware que se tenía operando al momento de realizar la planeación, es por ello, que decide realizar la implementación de la consola y los productos de McAfee a la versiones mas recientes y recomendadas por el fabricante.

# II. IMPORTANCIA DE LA TEMATICA

Hoy en día la lucha en contra problemas relacionados con la seguridad de tecnologías de información es más compleja. Día a día nos encontramos con amenazas como son, **Virus, Adware, Troyanos, Spyware**, así como ataques de **Phishing** y **Ransomware**[1]. Manejar diferentes productos de seguridad en diferentes ambientes y mantener los parches para vulnerabilidades de los sistemas, consumen mucho tiempo convirtiéndose en una actividad muy demandante. Los negocios hoy en día requieren de una solución en la cual sea posible manejar la seguridad de forma centralizada, además de proveer protección en contra de diversas amenazas y problemas relacionados con la productividad en los negocios.

**McAfee,** es una empresa reconocida a nivel mundial dedicada a la tecnología de seguridad. **McAfee**, ofrece soluciones, servicios proactivos y comprobados que ayudan a asegurar sistemas y redes en todo el mundo, protege a consumidores y empresas de todos los tamaños frente a todo tipo de amenazas. Las soluciones están diseñadas para trabajar juntas e integrar las funciones de **Antimalware**, **Antispyware** y **Antivirus** con las de una administración de la seguridad que ofrece visibilidad y análisis en tiempo real incomparables. Además, reducen el riesgo, garantizan el cumplimiento de las normativas y ayudan a las empresas a aumentar la eficiencia operativa (McAfee, Guía de instalación de McAfee ePolicy Orchestrator 5.10.0, 2019).

El software **McAfee ePolicy Orchestrator**[2] versión 5.10 proporciona una herramienta escalable para la gestión y aplicación centralizada de directivas de los productos **Endpoint Security**[3] **y Device Control**[4], con los cuales estaremos trabajando en este proyecto. Este a su vez ofrece funciones de generación de informes gráficos y despliegue de productos desde un único punto de control.

---

[1] Tipos de eventos de amenaza que representan un riesgo para los sistemas y la información de las empresas. Actualmente las amenazas más críticas son de tipo Ransomware y las comunes son de tipo Phishing.

[2] Software ampliable y adaptable de administración centralizada de la seguridad más avanzado, facilita y optimiza la administración de los riesgos.

[3] Solución de seguridad que protege servidores, sistemas y todo tipo de dispositivos conectados a la red, contra amenazas conocidas y desconocidas.

[4] Solución integral de DLP que protege a su empresa de la pérdida y el robo de información por medio de la supervisión y el control de la transferencia de datos entre PCs y medios extraíbles.

**McAfee ePO** es líder en la industria para el manejo de sistemas de seguridad, proporcionando seguridad en los sistemas de forma coordinada y proactiva en contra de amenazas y ataques para las organizaciones. Ha sido diseñado para ser una solución escalable; es una herramienta capaz de alertar y notificar el cumplimiento de políticas, así como el monitoreo de las amenazas presentes en la organización. El manejo de políticas que cubran cada capa de la protección a amenazas, desde la frecuencia de actualización hasta los tipos de archivos a analizar, así como las configuraciones para el escaneo Heurístico, todo ello de forma centralizada, siendo aplicada a grupos o individualmente. Todas las políticas son automáticamente forzadas por lo que garantiza una protección sólida. En la figura 1 muestra que McAfee es líder en el cuadrante para Endpoint Protection (Gartner, 2021).

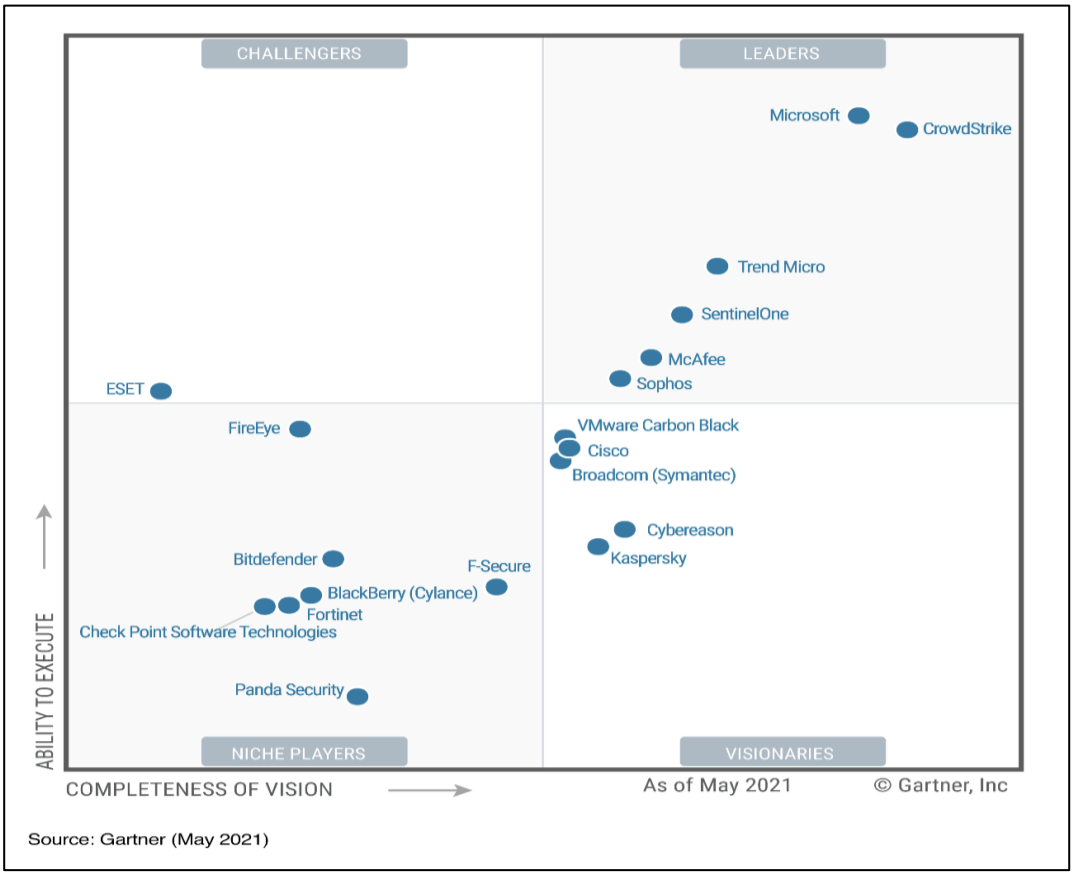



Figura 1:Magic Quadrant for Endpoint Protection Paltform *(Gartner, 2021)*.

También integra servicios de notificación y reportes gráficos proveyendo la información necesaria para el monitoreo de los sistemas de seguridad en un esquema **24x7**[5], ayudando a evaluar el estatus de las políticas de seguridad y ayudando a encontrar los puntos vulnerables dentro de la organización.

Actuando como administrador centralizado puede mitigar riesgos de seguridad. Es capaz de generar exclusiones, así como reglas específicas por nivel de criticidad. Además, es capaz de distribuir software de seguridad a través de paquetes de instalación personalizados.

El software de seguridad de **McAfee ePO y Endpoint Security** colaboran para detener los ataques de malware en sus sistemas y para enviarle notificaciones cuando se producen ataques.

## Qué sucede durante un ataque:

Los componentes y procesos de **McAfee ePO** detienen el ataque, le envían una notificación y registran el incidente en la consola de administración (McAfee, Guía del producto de McAfee ePolicy Orchestrator 5.10.0, 2018).

- El malware ataca un equipo de su red gestionado por **McAfee ePO**.
- El producto de software de **McAfee**, por ejemplo, **McAfee Endpoint Security**, limpia o elimina el archivo de malware.
- **McAfee Agent** notifica el ataque a **McAfee ePO**.
- **McAfee ePO** almacena la información del ataque.
- **McAfee ePO** muestra la notificación del ataque en el panel número de eventos de amenaza y guarda el historial del ataque en el Registro de eventos de amenaza.

En la figura 2 se muestran los procesos que se ejecutan en el **Endpoint** y en la consola **McAfee ePO** durante un evento de amenaza detectado.

[5] El monitoreo de infraestructura es la visión directa, en tiempo real e histórica, de todos los elementos que forman los sistemas informáticos de un negocio.

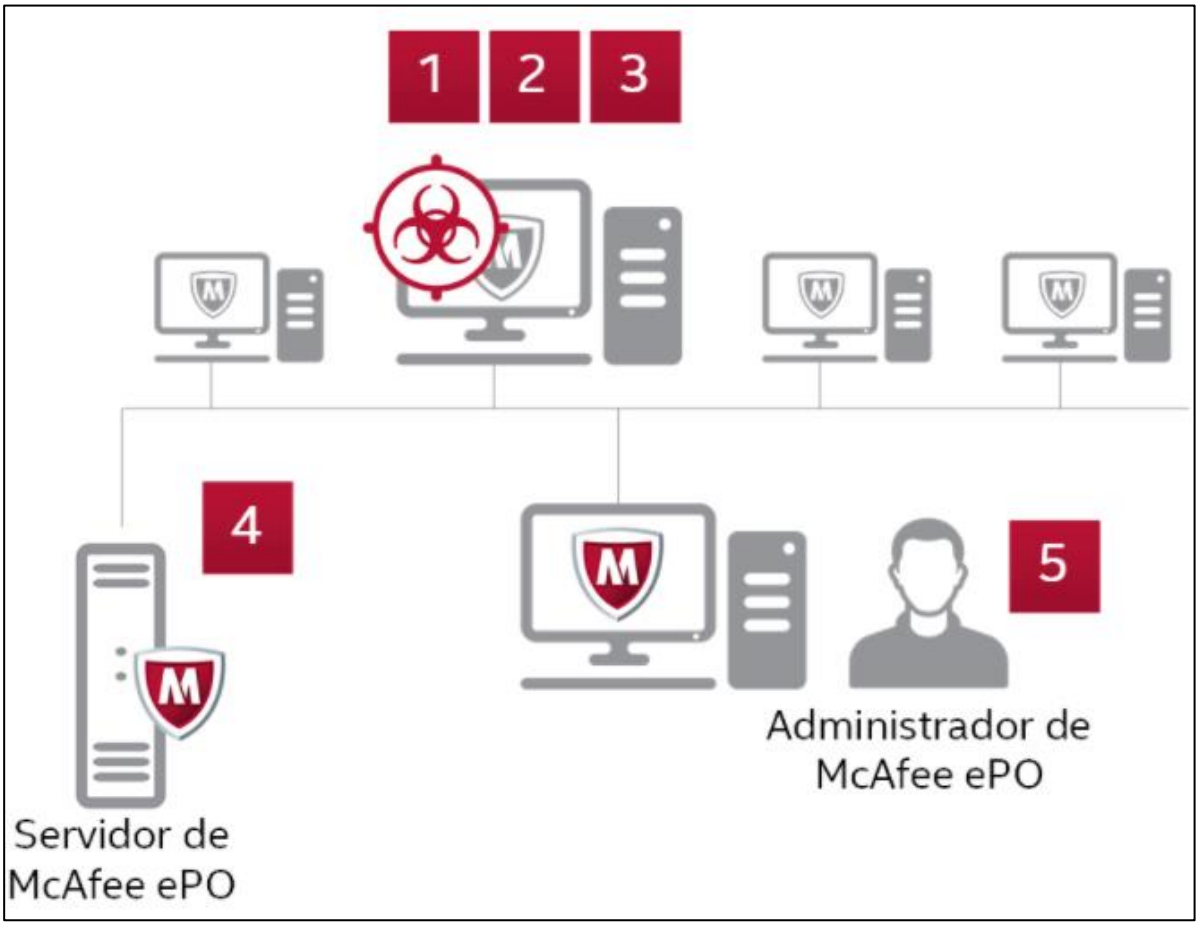



Figura 2: Ejemplo de los procesos que se ejecutan durante un evento de amenaza *(McAfee, Guía del producto de McAfee ePolicy Orchestrator 5.10.0, 2018)*.

# III. DESCRIPCIÓN DEL PUESTO O EMPLEO

Un ingeniero o especialista de seguridad de la información son las personas a las que compete la protección de los datos o la información de las organizaciones, así como hacer frente y dar respuesta a los incidentes de seguridad de la información. La misión consiste en luchar en contra de los cibercriminales, comúnmente conocidos como hackers, ladrones y espías cibernéticos, quienes se sirven de internet y de varios métodos de piratería para robar información confidencial. En la figura 3 se muestra las recomendaciones a seguir durante un incidente de seguridad (Infocyte, 2021).

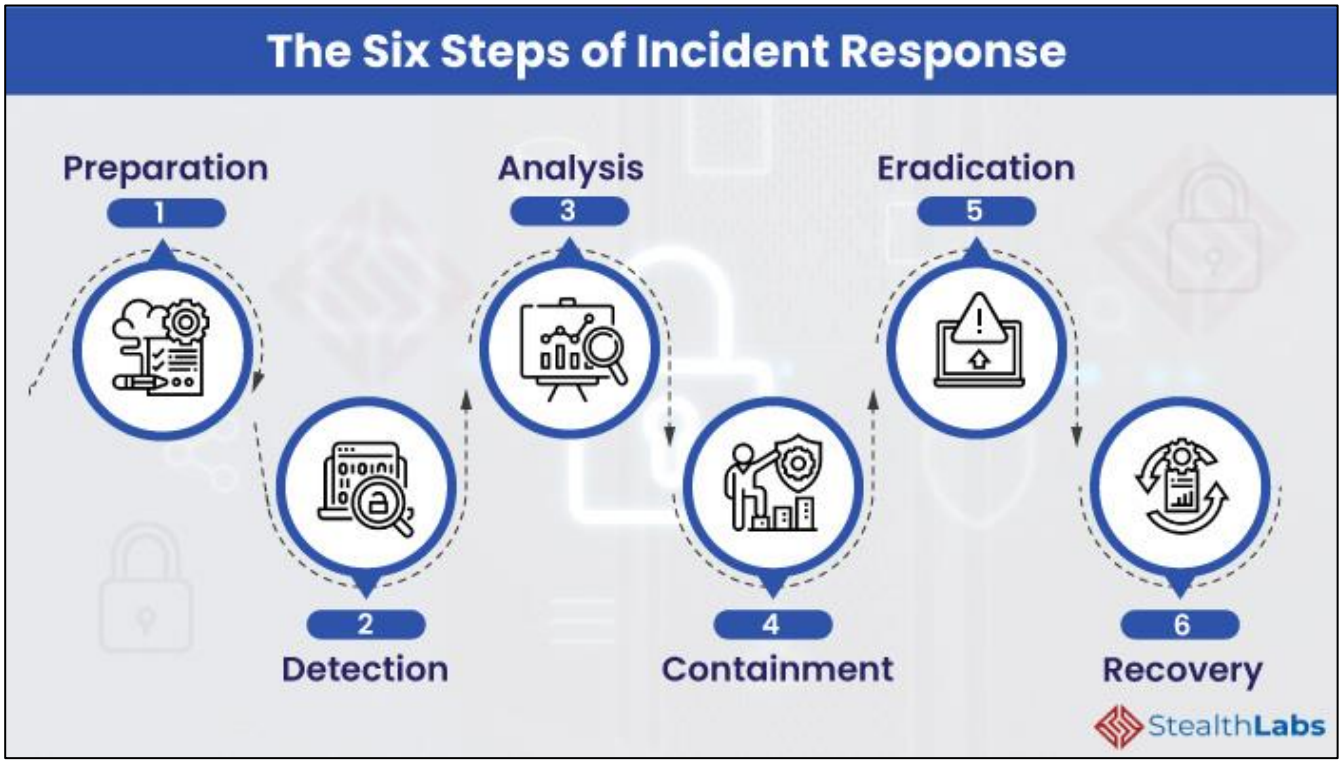



Figura 3: Ciclo de vida completo de una investigación en un incidente de seguridad *(Infocyte, 2021)*.

Las funciones principales del sustentante consisten en diseñar e implementar proyectos, programas y/o herramientas de seguridad que den soporte o automaticen parte de las tareas a realizar. Las tareas que se realiza con regularidad es la implementación de seguridad perimetral, sistemas de monitoreo, gestión de parches de seguridad y antivirus empresariales en Sistemas Operativos **Microsoft, Linux, MacOS, entre otros**.[6]

[6] Principales sistemas operativos con los que se trabaja con regularidad.

De igual manera el sustentante realiza la gestión y administración de las consolas, ***Appliance***[7] y/o softwares implementados, como se comentó anteriormente, se realizan tareas o directivas automatizadas para facilitar la operación diaria de los clientes administrados, así como alertas automatizadas que notifican a través de correo electrónico sobre nuevos eventos detectados, esto con la finalidad de actuar de manera oportuna en dichos eventos que puedan provocar un impacto critico en la infraestructura de los clientes administrados. En la figura 4 se indican las fases para realizar una implementación exitosa (Infogram, 2021).

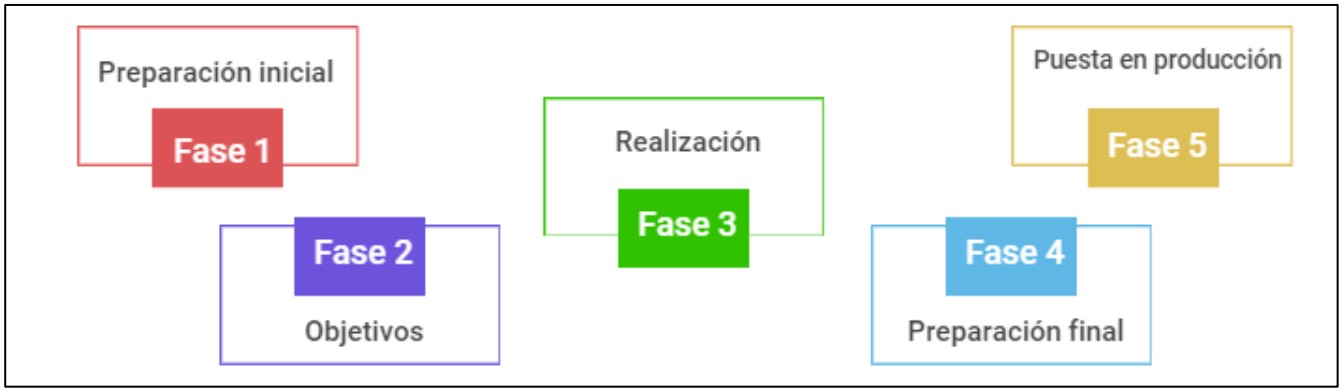



Figura 4: Fases para lograr una implementación exitosa *(Infogram, 2021)*.

[7] Dispositivos de hardware dedicados, encargados de efectuar un número determinado de funciones, habitualmente diseñados para instalarse en un rack, y que operan con software específicamente diseñado para ellos.

# IV. PROBLEMÁTICA IDENTIFICADA

**VolksWagen de México** planta de **Puebla**, contrata a ingenieros en sistemas computacionales o del área afín para para actualizar su consola de administración actual **McAfee ePolicy Orchestrator** versión **5.0.1**, por ende, los agentes de **McAfee** y los agentes de **VirusScan**[8] a las versiones más actuales de **McAfee**, de igual manera solicita implementar la solución de **McAfee Data Loss Prevention** en su módulo de **Device Control**, ya que quieren aplicar el bloqueo de USB´s en sus equipos productivos. En la figura 5 se puede observar la interface grafica de **McAfee ePolicy Orchestrator** en su versión **5.0.1** (McAfee, ePolicy Orchestrator , s.f.)**.**

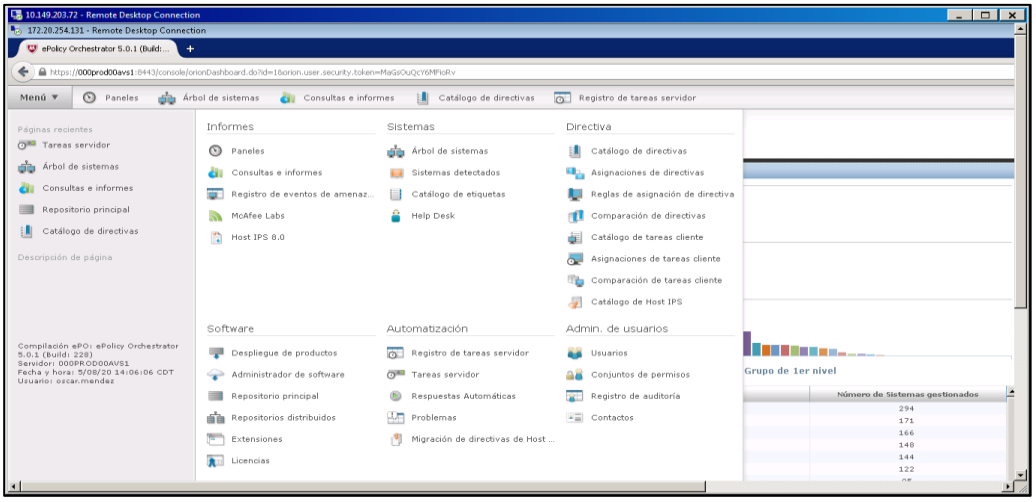



Figura 5: Consola de administración de VolksWagen en Puebla McAfee ePolicy Orchestrator versión 5.0.1 *(McAfee, ePolicy Orchestrator , s.f.)*.

Por parte de un servidor, se realiza el análisis pertinente para iniciar con la actualización de la consola, detectando que la versión que se tienen actualmente implementada en **Volkswagen de México** planta de **Puebla** es una versión demasiada obsoleta, misma que fue liberada en el año de 2013 la cual ya está detectada como ***End of Life*** (EOL)[9]. Así mismo se valida que las versiones que soportan **McAfee Data Loss Prevention** son las versiones de **McAfee ePolicy Orchestrator 5.9.1** en adelante.

[8] Software que protege los sistemas ante amenazas como Virus, Gusanos, Troyanos, Programas y códigos potencialmente no deseados (VirusScan, 2010)**.**

[9] El Fin de vida útil, más conocido por su término inglés End Of Life (EOL), es un término que se refiere a la caducidad de un producto de software. Es decir, es el momento en el cual un software deja de tener mantenimiento y soporte (Techopedia, 2016).

Rutas de ampliación admitidas:

| Amplíe De Versión | Ampliar a la versión de ePO | | | | | | |
|---|---|---|---|---|---|---|---|
| | 5.10 | 5.9.1 | 5.9.0 | 5.3.3 | 5.3.2 | 5.3.1 | 5.3.0 |
| 5.9.1 | Compatible | n/d | n/d | n/d | n/d | n/d | n/d |
| 5.9.0 | Compatible | Compatible | n/d | n/d | n/d | n/d | n/d |
| 5.3.3 | Compatible | Compatible | **Bloqueada** | n/d | n/d | n/d | n/d |
| 5.3.2 | Compatible | Compatible | Compatible | Compatible | n/d | n/d | n/d |
| 5.3.1 | Compatible | Compatible | Compatible | Compatible | Compatible | n/d | n/d |
| 5.3.0 | **Bloqueada** | **Bloqueada** | **Bloqueada** | **Bloqueada** | Compatible | Compatible | n/d |
| 5.1.3 EOL | Compatible | Compatible | Compatible | Compatible | Compatible | Compatible | n/d |
| 5.1.2 EOL | **Bloqueada** | **Bloqueada** | **Bloqueada** | Compatible | Compatible | Compatible | n/d |
| 5.1.1 EOL | **Bloqueada** | **Bloqueada** | **Bloqueada** | Compatible | Compatible | Compatible | Compatible |
| 5.1.0 EOL | **Bloqueada** | **Bloqueada** | **Bloqueada** | Compatible | Compatible | Compatible | Compatible |

n/d: no aplicable
Bloqueado = la ampliación desde esta versión no es compatible.

Figura 6:Tabla de versiones de ampliación permitidas *(McAfee, Plataformas compatibles con ePolicy Orchestrator, 2021)*.

De igual manera se valida que tienen equipos que cuentan con sistema operativo **Windows XP**[10] y servidores productivos con sistema operativo **Windows Server 2003**[11], los cuales solo son soportados por las versiones de **VirusScan 8.8 Patch 7**, esta versión de **VirusScan** solo es soportada por versiones de **McAfee ePolicy Orchestrator 5.3** o anteriores.

Por último, se le informa al cliente que para actualizar la consola actual a la versión más reciente es necesario contar con las credenciales de ***"sa" (cuenta administradora creada***

[10] Microsoft dejó de proporcionar soporte para Windows XP SP3 el 8 de abril de 2014. Para obtener los mejores resultados y un nivel de seguridad óptimo, amplíe su sistema operativo a una versión compatible (XP, 2022)
[11] Microsoft dejó de proporcionar soporte para Windows Server 2003 el 14 de julio de 2015. A partir del final de 2015 (Microsoft, 2022)

***por default al instalar SQL)***[12] de la base de datos y ***Passphrase*** (Recuperación de desastres). Nuestro cliente nos indica que no cuenta con estos datos importantes.

Después de realizar todo el análisis correspondiente en este ambiente, realizar las maquetas simulando el escenario el que se iba a trabajar y por experiencias que se habían tenido anteriormente con actualizaciones se recomendó lo siguiente:

Realizar la implementación de la consola de **McAfee ePolicy Orchestrator 5.10 patch 8**[13] desde cero.

Es necesario contar con dos servidores con los requerimientos mínimos indicamos por **McAfee** para la instalación de la consola y la base de datos. En la figura 7 y 8 se observan los requerimientos mínimos del servidor de **McAfee y SQL** respectivamente.

Hardware recomendado según el número de sistemas gestionados

| | Servidor de McAfee ePO | | |
|---|---|---|---|
| Recuento de nodos | Núcleos de CPU | RAM (GB) | Almacenamiento (GB) |
| < 10 000 | 4 | 8 | 300 |
| 10 000-25 000 | 4 | 8-16 | 500 |
| 25 000-75 000 | 8 | 16-32 | 500 |
| 75 000-150 000 | 12 | 16-64 | 500 |
| Más de 150 000 | 16 | 16-64 | 500 |

Figura 7: Requerimientos mínimos de Hardware para el servidor de McAfee ePO *(McAfee, Guía de instalación de McAfee ePolicy Orchestrator 5.10.0, 2019)*.

[12] Microsoft SQL Server crea una cuenta de administrador por defecto denominada SA. Esta cuenta dispone de privilegios de administrador completos, así como de propiedad de tablas de sistema

[13] Versión más actual de McAfee ePolicy Orchestrator al momento de implementar la solución.

| Recuento de nodos | SQL Server Núcleos de CPU | RAM (GB) | Almacenamiento (TB) | Rendimiento (IOPS) |
|---|---|---|---|---|
| < 10 000 | 4 | 8 - 16 | 0,5-1,0 | |
| 10 000-25 000 | 4 | 8-16 | 0,5-1,5 | |
| 25 000–75 000 | 8 | 16-32 | 1,0-2,0 | >10 000 |
| 75 000-150 000 | 16 | 32-128 | 2,0-3,0 | >30 000 |
| 150 000 o más | +32 | 128-256 | 3,0 | >90 000 |

Figura 8: Requerimientos mínimos de Hardware para el servidor de SQL *(McAfee, Guía de instalación de McAfee ePolicy Orchestrator 5.10.0, 2019)*

Se recomienda migrar de **VirusScan a Endpoint Security** ya que **McAfee Endpoint Security** protegen el entorno automáticamente frente a amenazas *zero-day*[14] como el **Ransomware**, remplaza **McAfee Host IPS a Firewall**[15] y también podemos tener la protección de **McAfee Web Control**[16].

Mantener en operación la consola actual para los equipos y servidores con sistema operativo que no son soportados con las nuevas versiones de **McAfee.**

Nuestro cliente está de acuerdo con las recomendaciones realizadas y nos brinda su Vo. Bo. para iniciar con la implementación de la consola de administración **McAfee ePolicy Orchestrator 5.10 patch 8** desde cero.

Es importante mencionar que, para iniciar con la instalación de la consola, nuestro cliente nos preparó dos servidores con los requerimientos mínimos solicitados por **McAfee,** una instancia de **SQL Server Enterprise**[17] previamente solicitada y la conexión remota a la infraestructura de **Volkswagen.**

[14] una vulnerabilidad de día cero o Zero Day, es un tipo de vulnerabilidad que acaba de ser descubierta y que aún no tiene un parche que la solucione (Trellix, 2022).
[15] Protección contra amenazas conocidas y desconocidas, de tipo zero-day, mediante la combinación de un sistema de prevención de intrusiones basado en firmas y comportamientos (IPS) y un firewall dinámico y con seguimiento de estado.
[16] solución de protección del navegador que supervisa la actividad de navegación y búsquedas web en equipos cliente.
[17] Es un software de servidor de base de datos relacional que ofrece herramientas para el almacenamiento, gestión, análisis e informes de datos (Microsoft S. , 2022)

# V. INFORME DETALLADO DE LAS ACTIVIDADES

## Componentes de la solución

Es importante conocer la arquitectura que nos permite administrar y proteger nuestro entorno correctamente. A continuación, se muestran los componentes que conforman la consola de administración **McAfee ePolicy Orchestrator. En la figura 9 mostramos los componentes de McAfee ePO.**

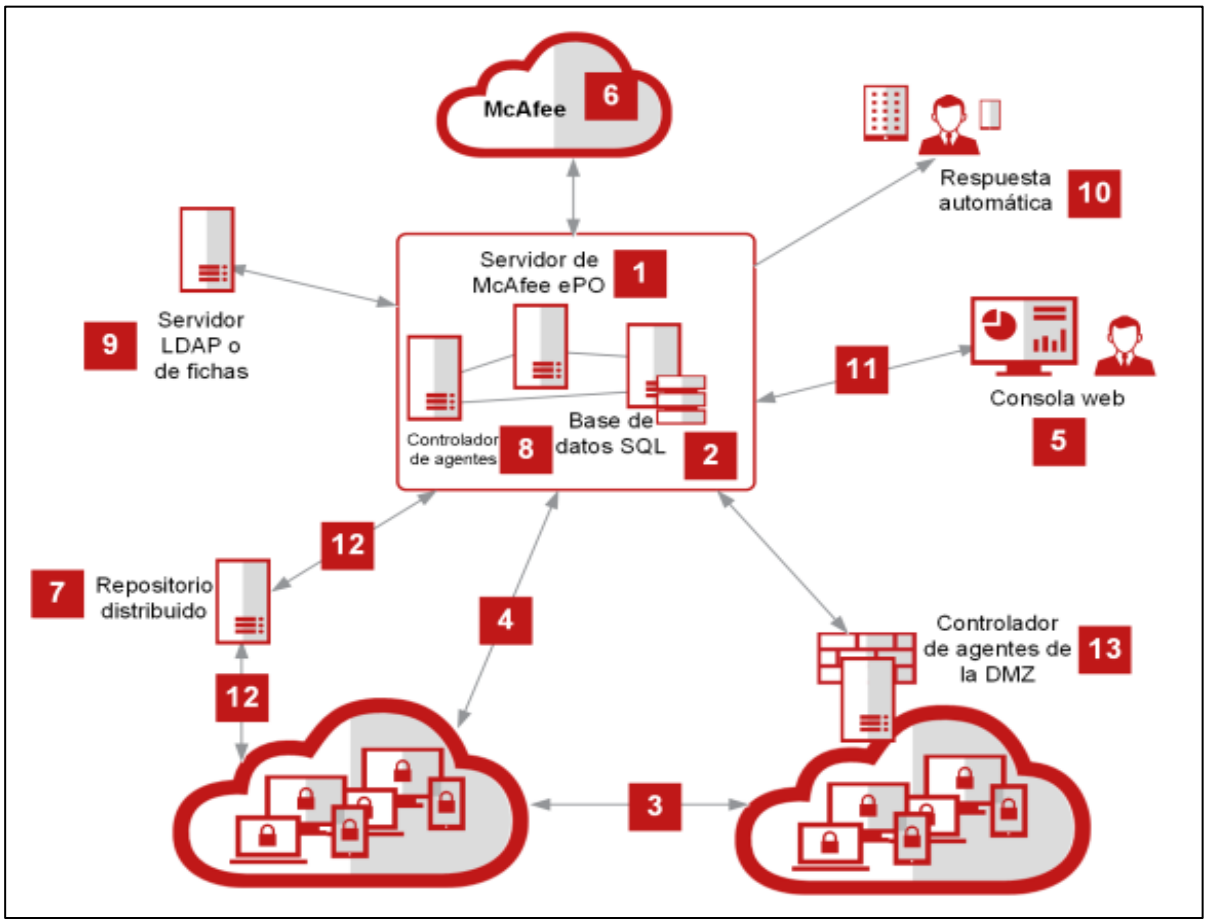



Figura 9: Componentes de McAfee ePO (McAfee, Guía del producto de McAfee ePolicy Orchestrator 5.10.0, 2018)

1. **Servidor de McAfee ePO:** Componente que administra y despliega productos, así como las actualizaciones más recientes, implementa directivas a los equipos finales y recopila eventos de los equipos gestionados.
2. **Base de datos SQL:** Almacena todos los datos de los equipos gestionados por **McAfee ePO.**

3. **McAfee Agent instalado en clientes:** Realiza la comunicación entre **McAfee ePO** y el equipo final para la implementación de directivas, despliegue de productos o actualizaciones.
4. **Conexiones de comunicación agente-servidor segura (ASSC**): Proporcionan comunicaciones a intervalos regulares entre los endpoints y el servidor.
5. **Consola Web:** Permite a los administradores iniciar sesión a la consola McAfee ePO, para realizar tareas, ejecutar consultas y trabajar sobre las directivas de seguridad de los equipos gestionados.
6. **Servidor web de McAfee:** Repositorio en la nube donde se almacena todo el contenido de seguridad, donde el servidor de McAfee ePO consulta para incorporar los paquetes más actuales a su consola. Esto conforme a las tareas automatizadas.
7. **Repositorios distribuidos:** Equipos o servidores incorporados en diferentes zonas que alojan el contenido de seguridad y distribuyen las actualizaciones de manera local en los equipos finales.
8. **Controladores de agentes:** reducen la carga de trabajo del servidor principal al asumir las tareas de procesamiento de eventos y de conectividad de **McAfee Agent.**
9. **LDAP o Directorio Activo:** Permiten la comunicación entre el servidor de McAfee ePO y el servidor **LDAP** o **Directorio Activo**.
10. **Respuestas automáticas:** Tareas configuradas para notificar a los administradores sobre algún evento detectado.
11. **Conexión de consola web:** Permite la conexión HTTPS entre el servidor de McAfee ePO y el navegador web mediante el puerto predeterminado 8443.
12. **Conexiones de repositorio distribuido:** Permite conexiones a los recursos compartidos en repositorios distribuidos en su red. Por ejemplo, conexiones HTTP, FTP o UDP.

## Fases de la implementación

Para realizar la implementación de manera exitosa de **McAfee ePolicy Orchestrator** y la migración de agentes de **McAfee, Endpoint Security y Device Control** se ejecutaron las siguientes fases. En la tabla 1 mostramos las fases para la implementación y migración exitosa.

Tabla 1: Fases para una implementación y migración exitosa.

| FASE | ACTIVIDAD | DESCRIPCIÓN |
|---|---|---|
| 1 | Validación de Prerrequisitos | Validar que los servidores productivos cuenten con los requerimientos mínimos solicitados a **Volkswagen de México** para la implementación de **ePolicy Orchestrator**. |
| 2 | Instalación de la consola **ePolicy Orchestrator** | Realizar la instalación de la consola de administración **ePolicy Orchestrator McAfee ePO, en seguida** se realiza la actualización de **ePolicy Orchestrator** a **Update 8 (2.0.0.929).** |
| 3 | Incorporación de **McAfee Agent, Endpoint Secutity y Device Contro**l la consola **McAfee ePO** | Descargar e incorporar los paquetes y extensiones para **McAfee Agent, Endpoint Secutity y Device Control** en el servidor de McAfee ePO. |
| 4 | Configuración de Directivas | Configuración y migración de políticas y tareas conforme a la configuración se tienen actualmente en la consola denominada como *"consola vieja",* así como definir las políticas y excepciones para aplicar el bloqueo de dispositivos externos, de acuerdo con la operación de **Volkswagen de México** y a las mejores prácticas. |
| 5 | Despliegue de los productos **McAfee Agente, Endpoint Security y Device Control**. | Instalación de los productos **McAfee Agent**, **Endpoint Security** y **Device Control** en cada uno de los equipos cliente proporcionados por **Volkswagen de México**. |
| 6 | Validación de Instalación | Verificación de la instalación adecuada en cada uno de los equipos proporcionados por **Volkswagen de México**. |

## Validación de Prerrequisitos

La primera fase consiste en validar que los servidores que fueron solicitados cuenten con los requerimientos mínimos para poder llevar a cabo la implementación de manera exitosa. En la tabla 2 y tabla 3 se muestran las características del servidor de McAfee ePO y SQL Server respectivamente.

Tabla 2: Tabla de las características del servidor de McAfee.

| CARACTERISTICA | PARAMETRO |
|---|---|
| MODELO: | VIRTUAL |
| HYPERVISOR: | Citrix Workspace |
| PROCESADOR: | Intel Xeon CPU E5-2697 2.30 GHz 8 procesadores |
| MEMORIA RAM: | 20 GB |
| SISTEMA OPERATIVO: | Windows Server 2019 Standard |
| IDIOMA DEL SISTEMA OPERATIVO: | Ingles |
| HOSTNAME: | SRVVWMEPOAPP01 |
| DIRECCION IP: | 172.20.254.101 |

| | |
|---|---|
| VELOCIDAD DE RED: | Auto |
| CAPACIDAD DE DISCO DURO: | 2 particiones: C: (59.4 GB), D: (ePO: 299 GB) |
| FORMATO DE SISTEMA DE ARCHIVOS: | NTFS |
| CONEXIÓN A INTERNET: | Solo a los sitios de McAfee |
| SOFTWARE REQUERIDO: | McAfee ePO |
| DOMINIO: | N/A |

Tabla 3: Tabla de las características del servidor de SQL Server.

| CARACTERISTICA | PARAMETRO |
|---|---|
| MODELO: | VIRTUAL |
| HYPERVISOR: | Citrix Workspace |
| PROCESADOR: | Intel Xeon CPU E5-2697 2.30 GHz 8 procesadores |
| MEMORIA RAM: | 32 GB |
| SISTEMA OPERATIVO: | Windows Server 2019 Standard |
| IDIOMA DEL SISTEMA OPERATIVO: | Ingles |
| HOSTNAME: | SRVVWMEPODB01 |
| DIRECCION IP: | 172.20.254.102 |
| VELOCIDAD DE RED: | Auto |
| CAPACIDAD DE DISCO DURO: | 2 particiones: C: (299 GB), D: (: 499 GB) |
| FORMATO DE SISTEMA DE ARCHIVOS: | NTFS |
| CONEXIÓN A INTERNET: | Solo a los sitios de McAfee |
| SOFTWARE REQUERIDO: | McAfee ePO |
| DOMINIO: | N/A |

Se procede a ingresar por **RDP**[18] al servidor de **McAfee ePO** SRVVWMEPOAPP01 con IP 172.20.254.101 y se valida que se está cumpliendo con los requerimientos solicitados. En la figura 10 se muestran las propiedades del equipo.

[18] Protocolo desarrollado por Microsoft que permite la comunicación entre una terminal y un servidor Windows en la ejecución de aplicaciones (¿Qué es el RDP?, 2021)

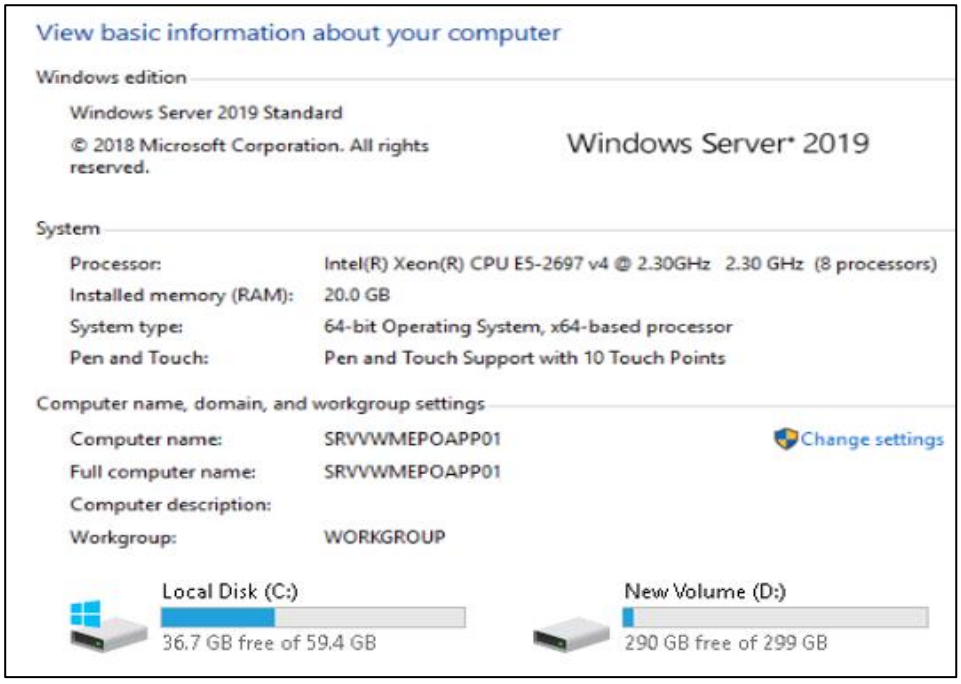


Figura 10: Servidor Windows Server 2019 donde se realizará la instalación de McAfee ePO.

Se procede a ingresar por **RDP** al servidor de la base de datos (**SQL**) proporcionado por **Volkswagen** y se valida que se está cumpliendo con los requerimientos solicitados. En la figura 11 se muestran las propiedades del equipo.

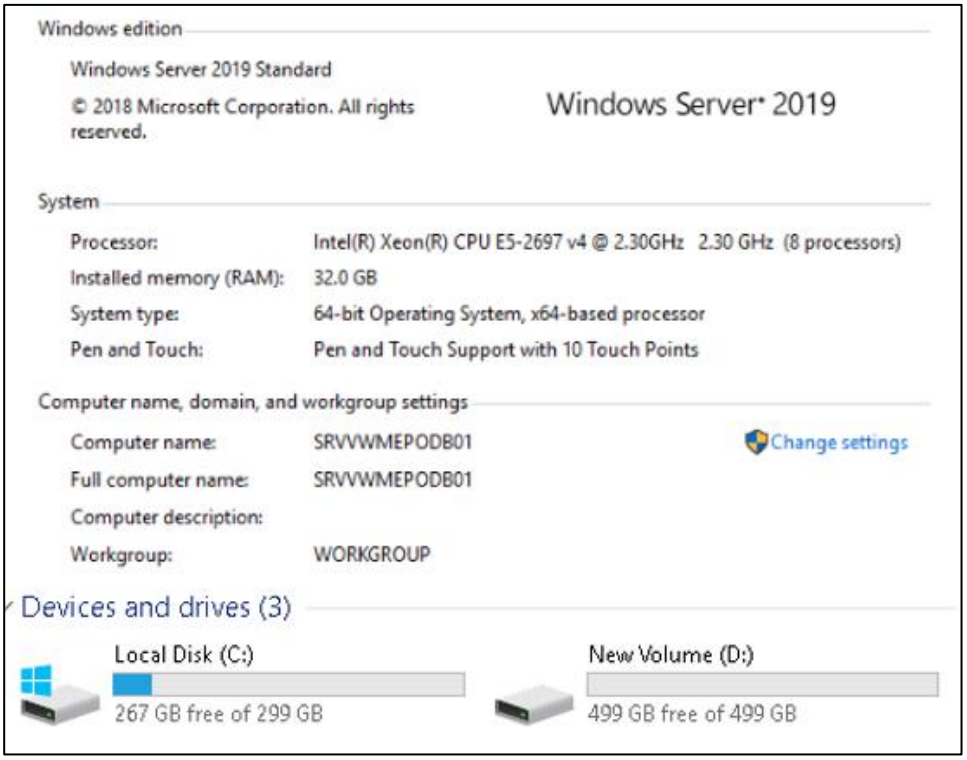


Figura 11: Servidor Windows Server 2019 donde se realizará la instalación de la base de datos SQL.

Por último, se procede a solicitar los datos de la instancia[19] de la base de datos de **SQL**, ya que esta actividad es responsabilidad del cliente. Se brinda la información solicitada. En la Tabla 4 se muestran las características de la instancia de la base de datos SQL.

Tabla 4: Tabla de las características de la instancia de la base de datos SQL.

| BASE DE DATOS | |
|---|---|
| **PARÁMETRO** | **CONFIGURACIÓN** |
| **Dirección IP** | 172.20.254.102 |
| **Puerto Lógico** | 1433 |
| **Nombre de la BD** | ePO_SRVVWMEPOAPP01 |
| **Tipo de comunicación** | SSL |
| **Nombre de Usuario** | Sa / Autenticación Windows |
| **Contraseña de sa** | ********** |
| **Dominio** | N /A |
| **Tamaño de la BD** | 299 GB |

## Instalación de la consola ePolicy Orchestrator McAfee ePO

En la segunda fase de la implementación, se inicia con la instalación de la consola de **ePolicy Orchestrator McAfee ePO** versión **5.10** en el servidor proporcionado por **Volkswagen de México.** A continuación, se muestra de manera general la instalación de la consola. En la figura 12 se muestra el asistente de instalación de la consola McAfee.

[19] Una instancia de Motor de base de datos es una copia del ejecutable de sqlservr.exe que se ejecuta como un servicio de sistema operativo. Cada instancia administra varias bases de datos del sistema y una o varias bases de datos de usuario. Cada equipo puede ejecutar varias instancias de Motor de base de datos (Server, 2022)

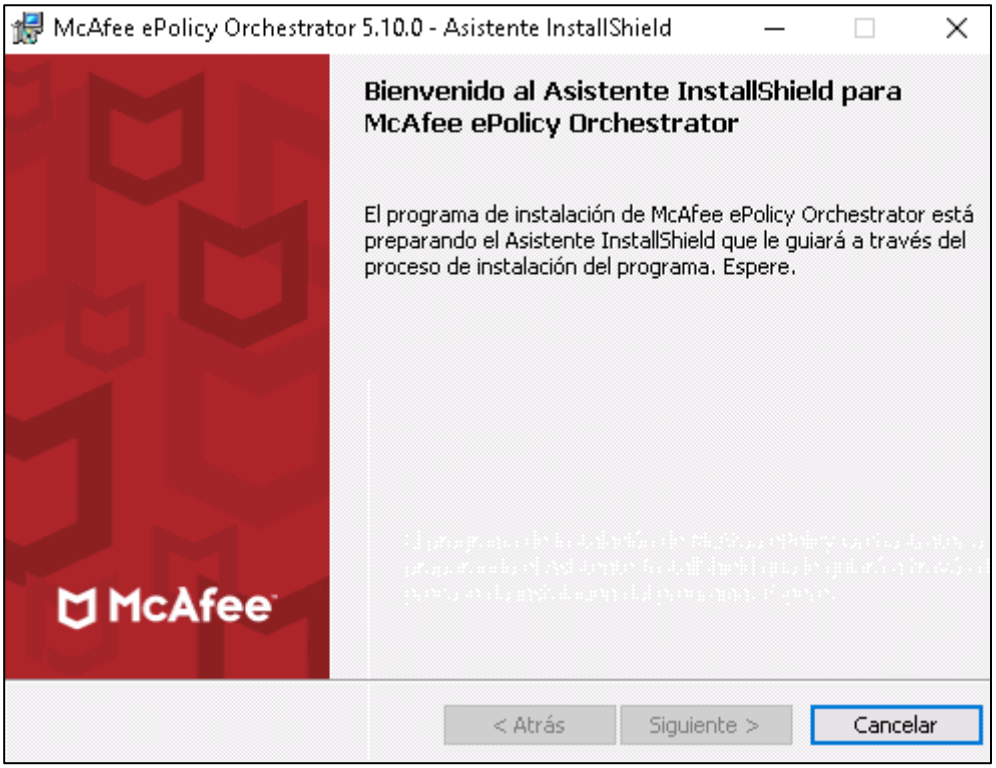



Figura 12: Se muestra el asistente de instalación de la consola de ePolicy Orchestrator McAfee ePO.

En la figura 13 se indica la ruta del sistema operativo donde se va a instalar la consola de **ePolicy Orchestrator McAfee ePO**.

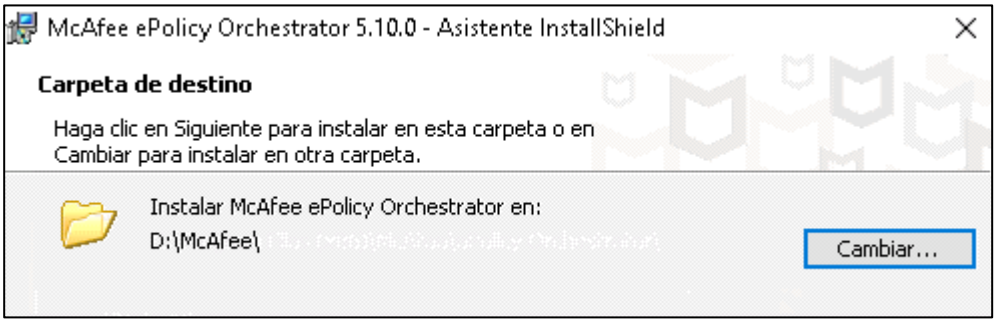



Figura 13: Ruta de instalación de McAfee ePO

Después serán solicitados todos los datos de la base de datos **SQL** que previamente fue creada por **Volkswagen de México**. En la figura 14 se muestran los datos ingresados de **SQL**.

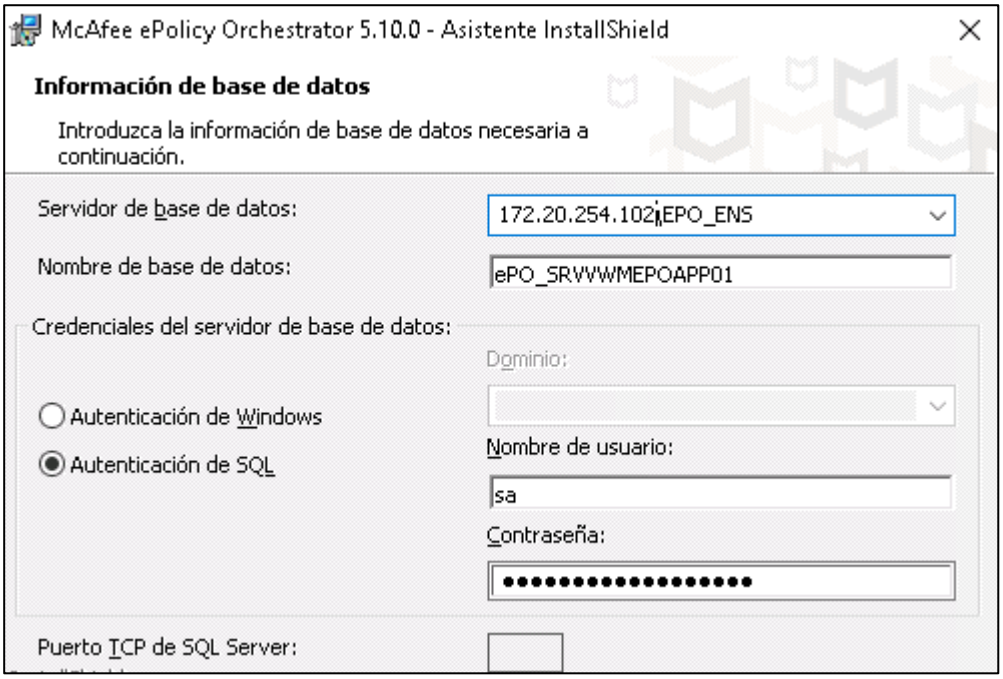


Figura 14: Datos de la base de datos SQL.

En la siguiente configuración se solicitará información de la cuenta de administración, así como la frase de recuperación. En la figura 15 se muestran los datos que son solicitados.

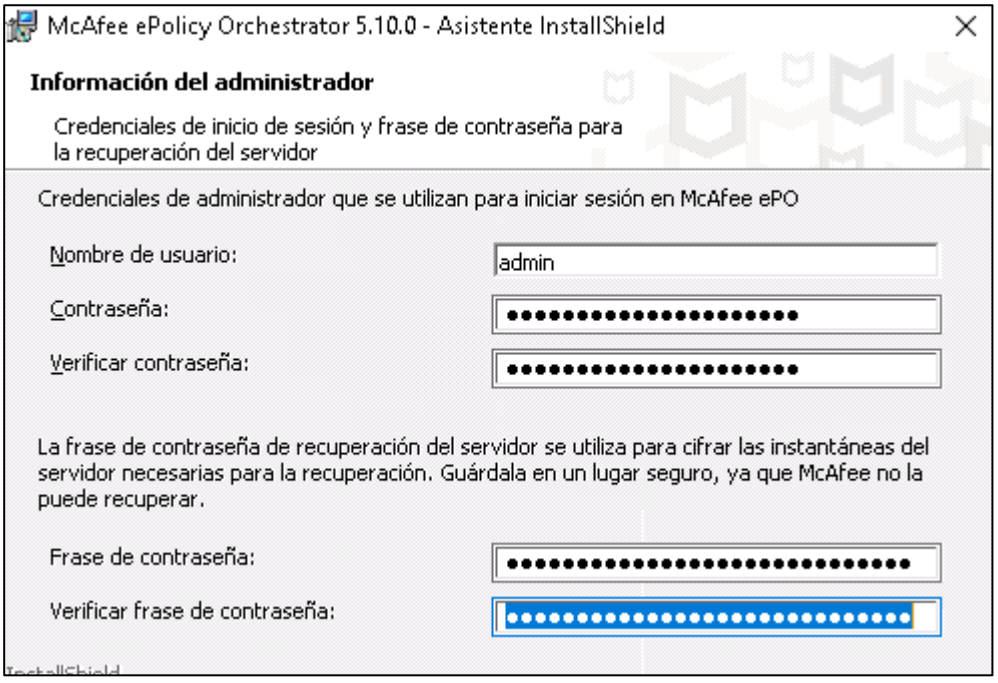


Figura 15: Credenciales para el usuario administrador de la consola y frase de recuperación.

En la siguiente configuración se solicitarán ingresar los puertos de comunicación, estos puertos son necesarios para la comunicación entre agente–servidor, activación de los agentes,

acceso a la consola Web y puerto del servidor de **SQL**. En la figura 16 se muestran los puertos que se definieron para la consola de McAfee ePO.

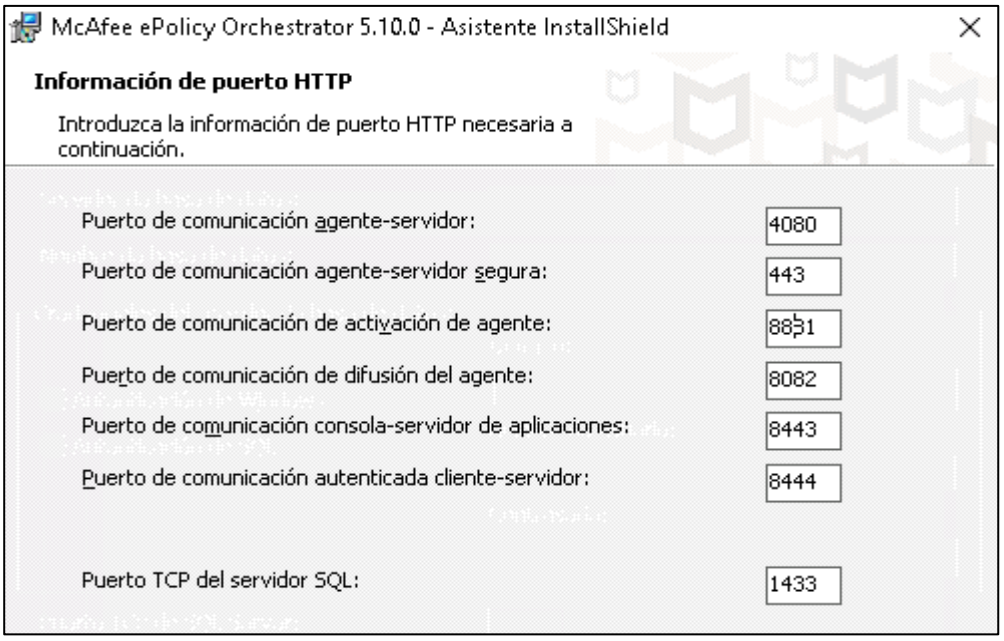



*Figura 16: Puerto de comunicación definidos para la comunicación de McAfee ePO.*

En la siguiente configuración será necesario agregar la clave de licencia de McAfee ePO y se tiene que seleccionar la casilla de “Activar instalación automática de productos” esto con la finalidad de descargar los productos que se tienen disponibles con la licencia contratada, después aceptaremos los términos de licencia. En la figura 17 se muestran la licencia (por temas de confidencialidad fue ocultada) y la aceptación de los términos de licencia.


Figura 17: Clave de licencia y aceptación de términos de licencia.

Después de esto habremos finalizado la instalación de la consola de ePolicy Orchestrator McAfee ePO. En la figura 18 se muestra la instalación correcta de la consola.

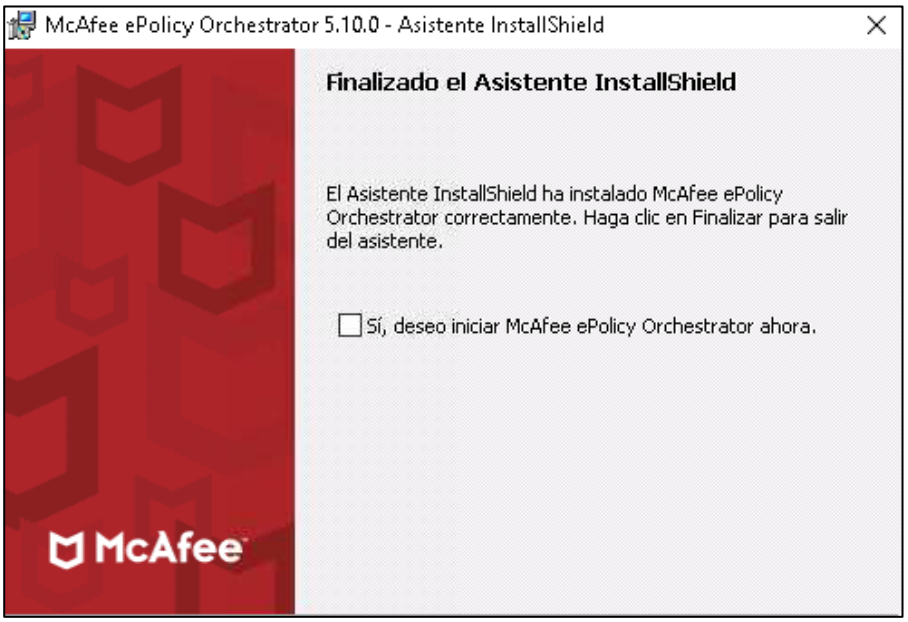



Figura 18: El asistente de configuración indica que la instalación ha concluido correctamente.

Para finalizar, es necesario ingresar a la consola de McAfee ePO, esto con la finalidad de validar la comunicación correcta, el usuario que se creó y la versión instalada. Como buena práctica, se recomienda realizar la instalación de McAfee Agent en un equipo y validar que se registe de manera correcta. En la figura 19 se muestra el acceso a la consola.

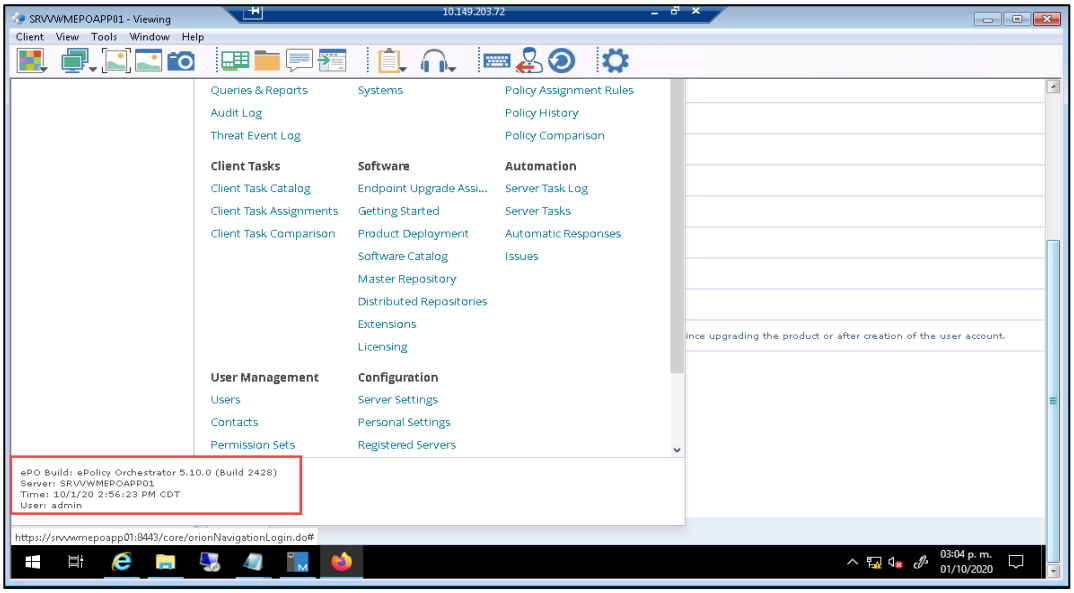



Figura 19: Acceso a la consola de McAfee ePO.

Se ha concluido con la primera parte de la instalación de la consola, ya que ahora es necesario aplicarle la actualización indicada por fabricante para el correcto funcionamiento de la consola y sus componentes. En esta consola se aplicó la actualización de ePolicy Orchestrator al Update 8 (2.0.0.929).

Para realizar esta actualización en necesario contar con los siguientes datos de la base de datos, ya que realiza una validación de sincronización con la consola de McAfee ePO, de lo contrario, no se podrá realizar la actualización. En la figura 20 se muestra el inicio de la actualización del **patch 8.**

- Databases Name
- Datebase Server Name / IP
- Port Number
- User Name (DB)
- Password de DB

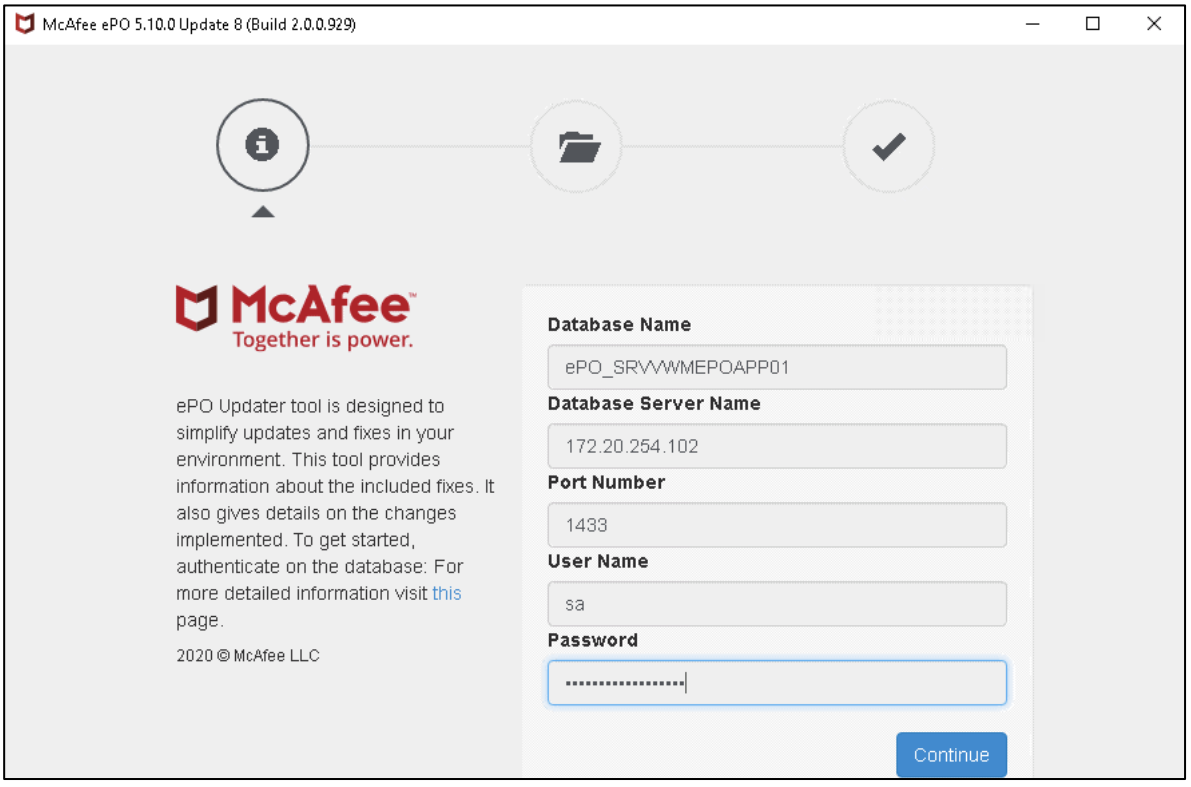


Figura 209 : Se muestra evidencia de que se inicia con la actualización de McAfee ePO al patch 8.

Al concluir de manera satisfactoria con la actualización, se muestra un mensaje indicando que se completó la actualización al 100% y donde se inician los servicios de McAfee ePO[20] que fueron detenidos antes de la actualización. En la imagen 21 se observa que la actualización concluyo de manera exitosa.

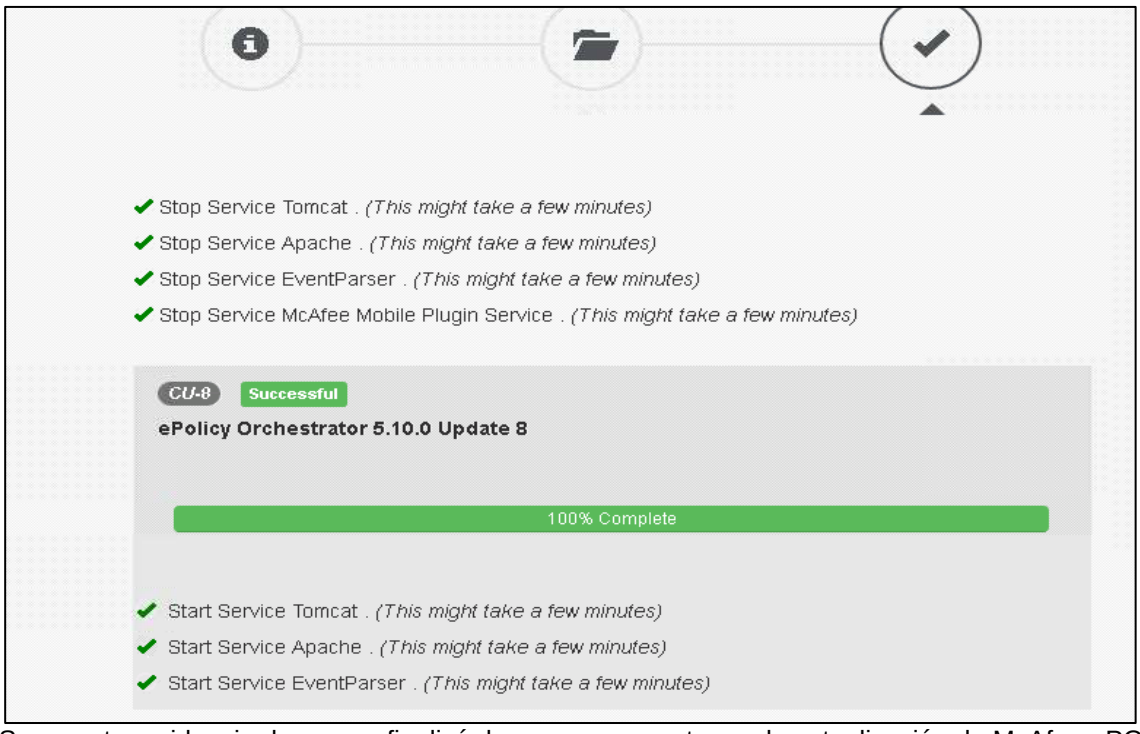



Figura 21: Se muestra evidencia de que se finalizó de manera correcta con la actualización de McAfee ePO al patch 8.

Para comprobar que la actualización se aplicó de manera correcta, ingresamos nuevamente a la consola de administración McAfee ePO y validamos las versiones que tiene instalada. En la figura 22 se observan las versiones instalas.

[20] Los servicios de McAfee ePO son indispensables para el correcto funcionamiento de la consola, el servicio de aplicación proporciona una página Web para la configuración en general, el servicio de analizador de eventos se encarga de almacenar los eventos en la base de datos para trasmitirla a nivel consola y el servicio de Apache administra la comunicación Agente – Servidor.

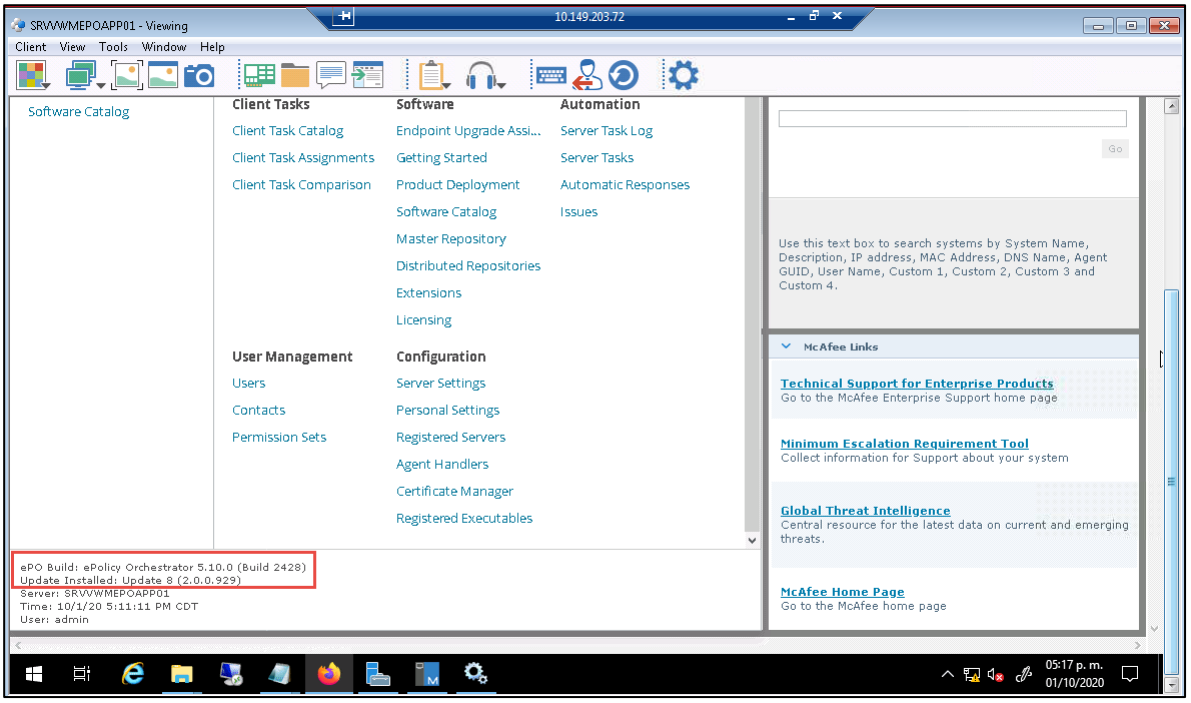


Figura 22: Se validan las versiones instaladas para la consola de McAfee ePO.

## Configuración inicial de McAfee ePolicy Orchestrator

Una vez que se haya concluido con las actualizaciones necesarias para la consola de McAfee ePO es necesario aplicar algunas configuraciones iniciales adicionales para la correcta administración de la consola. A continuación, se muestran las configuraciones aplicadas.

Se realiza la configuración del servidor Proxy,[21] ya que esto es necesario para que la consola de McAfee ePO pueda consultar los sitios de McAfee para la descarga de actualizaciones de productos y motores de antimalware. En la Figura 23 podemos observar el proxy aplicado.

[21] Proxy: Servidor que funciona como intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los paquetes entre ambos, para poder acceder a servicios que tienen bloqueado su contenido en un determinado (Proxy, 2022)

| | |
|---|---|
| **Tipo:** | Utilizar distintos servidores proxy para los protocolos HTTP y FTP |
| **Configuración de servidor proxy:** | Servidor proxy: 104.129.202.15<br>Puerto: 80<br>Servidor FTP: 104.129.202.15<br>Puerto: 80 |
| **Autenticación de proxy:** | Usar autenticación de proxy HTTP<br>Nombre de usuario: na\DZM9CBR<br>Usar autenticación de proxy FTP<br>Nombre de usuario: na\DZM9CBR |

Figura 23: Se muestra la configuración de Proxy.

Ahora vamos a validar la información del servidor de McAfee ePO y la base de datos, donde vamos a observar Nombre del servidor, IP´s asignadas de los servidores, parche instalado, unidad donde se instalado, espacio en disco, versión del sistema operativo y nombre de la instancia de la base de datos, así como las versiones de Java y Tomcat. En la Figura 24 se observa esta información.

| | |
|---|---|
| **Información de base de datos:** | Servidor: 172.20.254.102:1433<br>Versión: Microsoft SQL Server 2019 (RTM-GDR) (KB4517790) - 15.0.2070.41 (X64) Oct 28 2019 19:56:59 Copyright (C) 2019 Microsoft Corporation Standard Edition (64-bit) on Windows Server 2019 Standard 10.0 (Build 17763: ) (Hypervisor)<br>Nombre de la base de datos: ePO_SRVVWMEPOAPP01 |
| **Información del servidor de McAfee ePO y la base de datos** | |
| **Información del servidor:** | Nombre: SRVVWMEPOAPP01<br>Nombre DNS: SRVVWMEPOAPP01<br>Dirección IP: 172.20.254.101<br>Versión: 5.10.0.2428<br>Actualización instalada: Update 8 (2.0.0.929)<br>Unidad: D:\<br>Espacio libre en disco: 296531 MB |
| **Información del controlador de agentes:** | |
| **Versión de Java:** | 1.8.0_241 |
| **Versión de Tomcat:** | 7.0.103 |
| **Versión de Apache:** | |
| **Versión de OpenSSL:** | 1.0.2t-fips |

Figura 24: Información del servidor McAfee ePO y la base de datos.

Después vamos a validar los puertos que se configuraron al momento de realizar la instalación de la consola de McAfee ePO, esto para la correcta comunicación entre los agentes y el servidor. En la figura 25 se observan los puertos configurados.

| | |
|---|---|
| **Puerto de comunicación agente-servidor:** | 4080 |
| **Puerto de comunicación agente-servidor segura:** | Activado en puerto 443 |
| **Puerto de comunicación de activación de agente:** | 8881 |
| **Puerto de comunicación de difusión de agente:** | 8082 |
| **Puerto de comunicación consola-servidor de aplicaciones:** | 8443 |
| **Puerto de comunicación cliente-servidor autenticada:** | 8444 |

Figura 25: Puertos de comunicación entre agentes-servidor.

Por último, vamos a realizar la configuración del servidor de SMTP[22], esto es indispensable para recibir por medio de correo electrónico notificaciones de la consola de McAfee ePO (Amenazas, reportes, eventos de auditoria). En la figura 26 vamos a observar la configuración aplicada.

| | |
|---|---|
| **Nombre del servidor SMTP:** | 10.148.9.103 |
| **Puerto del servidor SMTP:** | 25 |
| **Nombre de usuario:** | |
| **Dirección del remitente:** | epo_industrial@vw.com |

Figura 26: Configuración del servicio de SMTP.

[22] SMTP: Protocolo simple de transferencia de correo electrónico, es un protocolo TCP/IP que se utiliza para enviar y recibir correo electrónico. Normalmente se utiliza con POP3 o con el protocolo de acceso a mensajes de Internet (IMAP) para guardar mensajes en un buzón del servidor y descargarlos periódicamente del servidor para el usuario.

**Nota: Es importante mencionar que algunas configuraciones fueron aplicadas durante la instalación de la consola y solo se tiene que ingresar a validar que se hayan aplicado de manera correcta**

## Incorporación de McAfee Agent, Endpoint Secutity y Device Control la consola McAfee ePO

En este apartado vamos a mostrar la incorporación los paquetes y extensiones para McAfee Agent, Endpoint Secutity y Device Control en el servidor de McAfee ePO.

El proceso de incorporación de paquetes y extensiones consola a la ePolicy Orchestrator consta de las siguientes fases:

- Validar la incorporación de extensiones sobre la consola McAfee ePO.
- Validar la incorporación de productos sobre la consola McAfee ePO

### Validación de extensiones para ePolicy Orchestrator

A continuación, se muestran las extensiones que fueron incorporadas para McAfee ePolicy Orchestrator. Es importante mencionar que estas licencias son indispensables para el correcto funcionamiento de la consola McAfee ePO. En la figura 27 se observan las extensiones incorporadas para McAfee ePolicy Orchestrator.

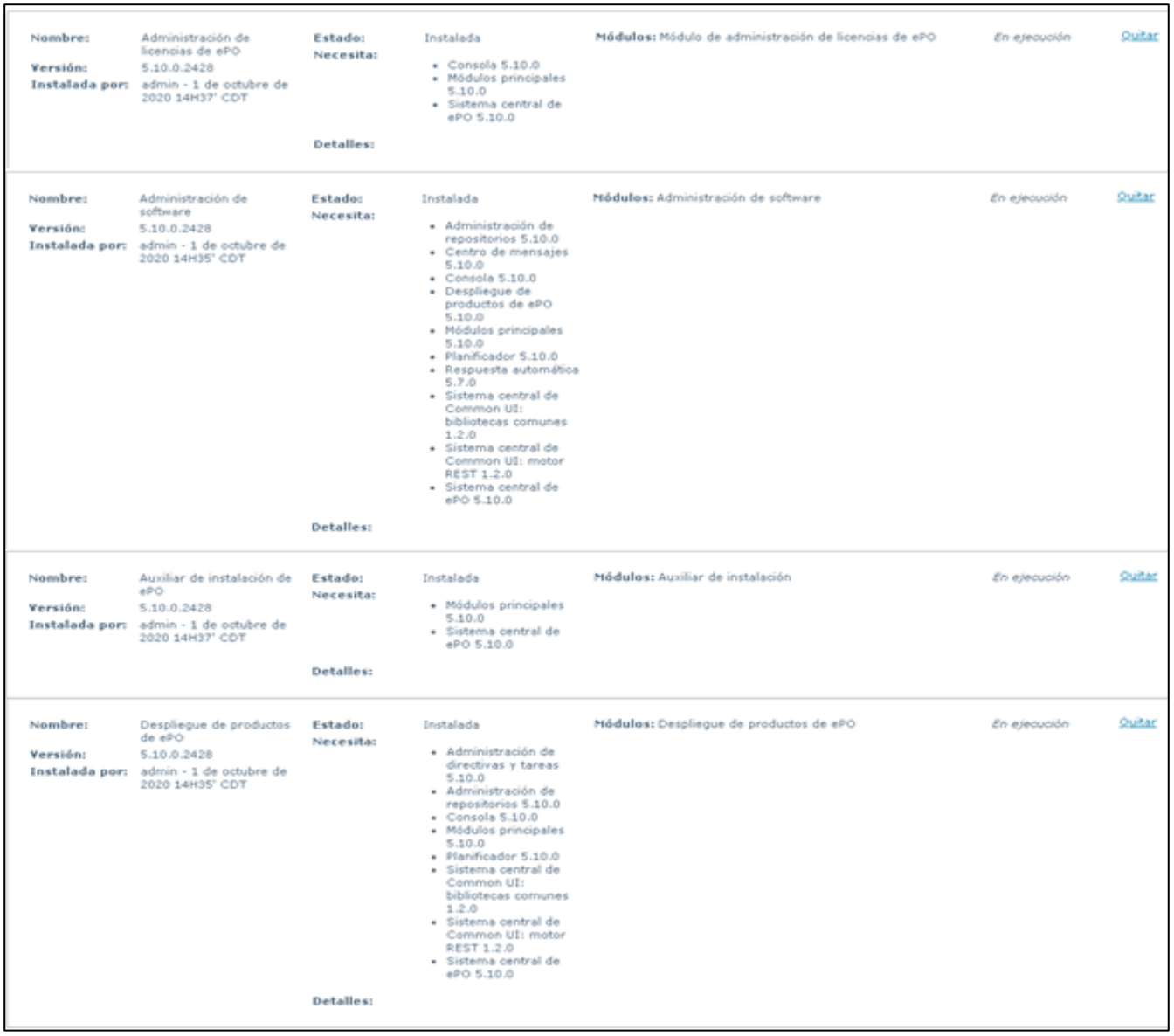



Figura 27: Extensiones incorporadas para McAfee ePolicy Orchestrator.

## Validación de extensiones para McAfee Agent

A continuación, se muestran las extensiones que fueron incorporadas para McAfee Agent. Es importante mencionar que estas licencias son indispensables para el correcto funcionamiento de agentes administrados. En la figura 28 se observan las extensiones incorporadas para McAfee Agent.

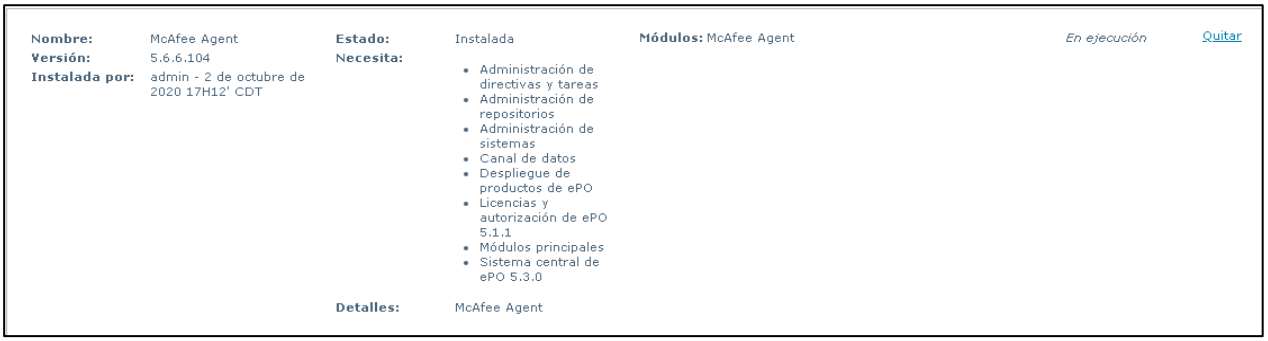
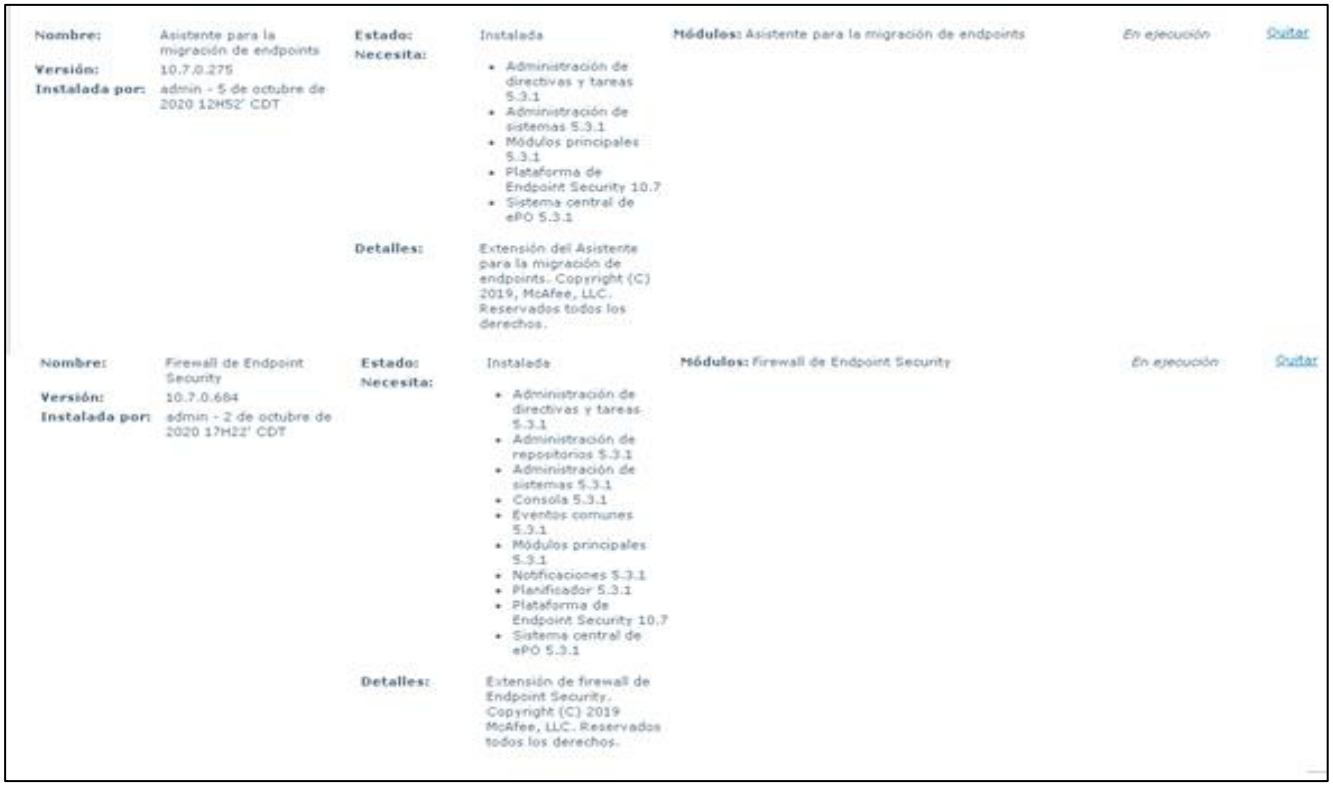



Figura 28: Extensiones incorporadas para McAfee Agent.

## Validación de extensiones para McAfee Endpoint Security

A continuación, se muestran las extensiones que fueron incorporadas para McAfee Endpoint Security. Es importante mencionar que estas licencias son indispensables para el correcto funcionamiento de los productos de Firewall, Plataforma y Prevención de Amenazas. En la figura 29 se observan las extensiones incorporadas para McAfee Endpoint Security.



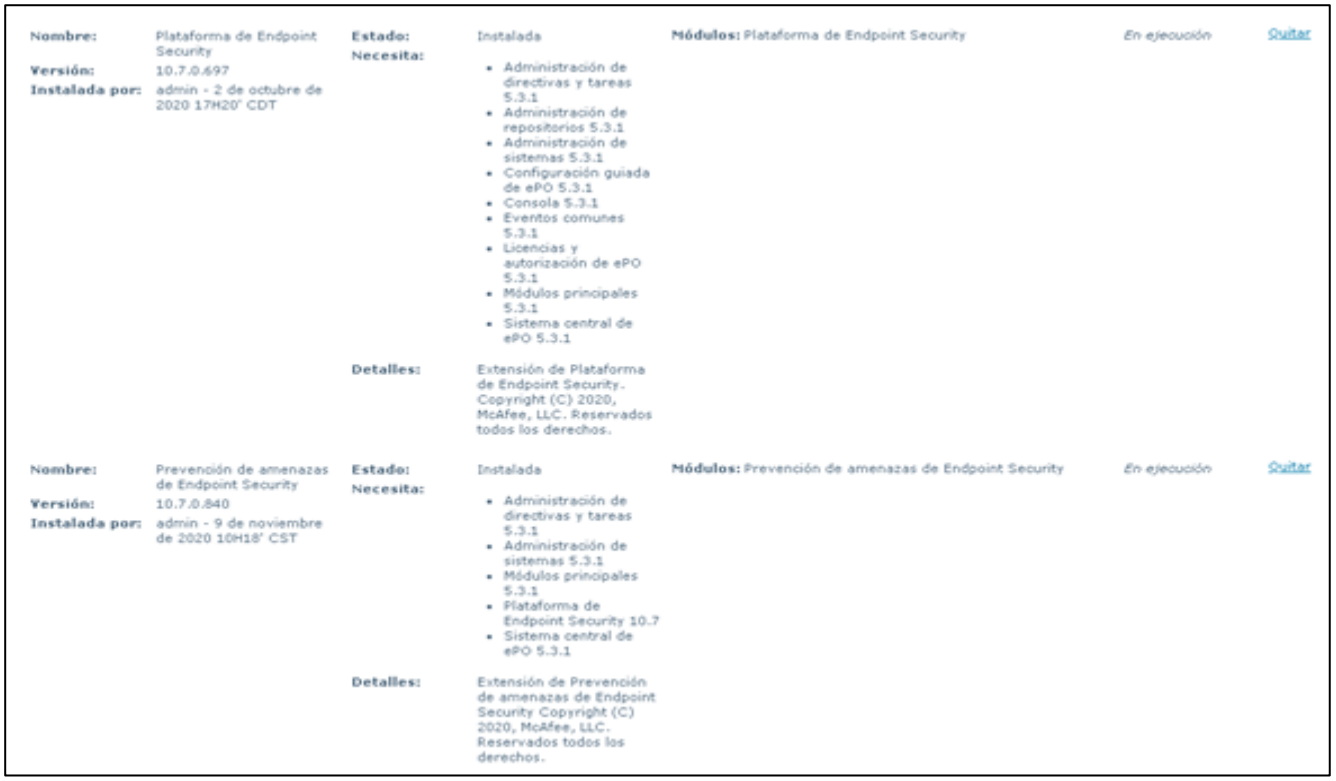



Figura 29: Extensiones incorporadas para McAfee Endpoint Security.

## Validación de extensiones para McAfee Data Loss Prevention

A continuación, se muestran las extensiones que fueron incorporadas para McAfee Data Loss Prevention. Es importante mencionar que estas licencias son indispensables para el correcto funcionamiento del bloqueo de dispositivos externos. En la figura 30 se observan las extensiones incorporadas McAfee Data Loss Prevention.

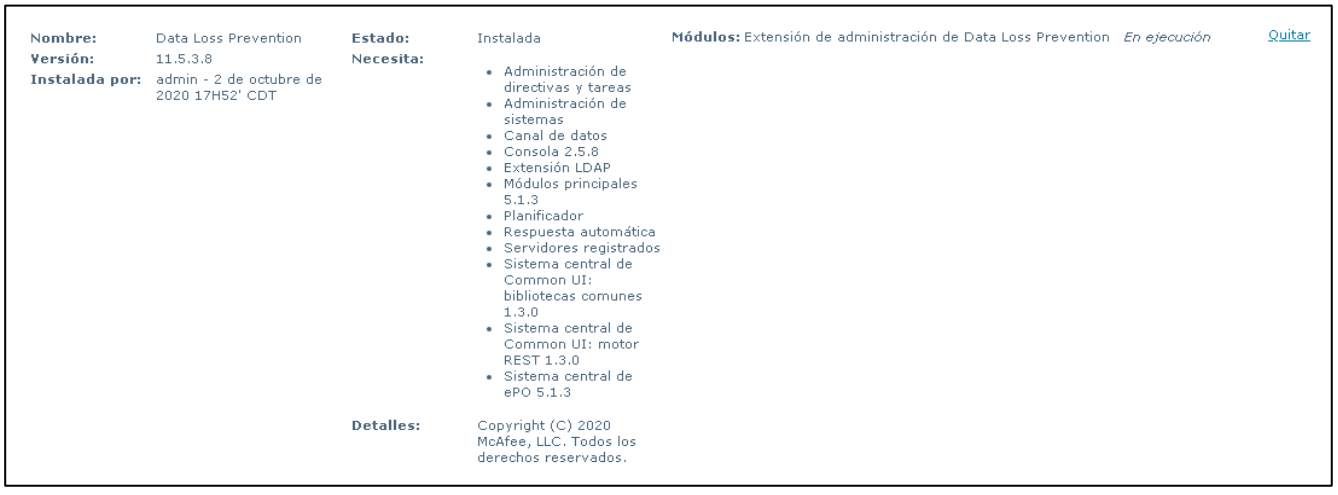



Figura 30: Extensiones incorporadas para McAfee Data Loss Prevention.

**Validación de paquetes de software para McAfee Agent**

Una vez que se haya validado la incorporación de extensiones para los productos de McAfee ePO, es necesario realizar la validación de paquetes de software para los productos de McAfee.

Es importante mencionar que, si los paquetes no fueron incorporados al momento de la implementación de la consola McAfee ePO, los paquetes tendrán que ser descargados del sitio oficial de McAfee (es necesario contar con el Grant Number[23]) e incorporarlos de manera manual a la consola.

A continuación, se muestran los paquetes que fueron incorporadas para McAfee Agent y sus versiones. Es importante mencionar que estos paquetes son necesarios para realizar el despliegue de productos de forma remota desde la consola. En la consola se realizan tareas de instalación o en su defecto crear tareas programas para enviar el despliegue. En la figura 31 se observan los paquetes incorporados para McAfee Agent.

- **McAfee Agent for Windows**
- **McAfee Agent for MAC**
- **McAfee Agent for LINUX**

| | | | |
|---|---|---|---|
| McAfee Agent for Windows | Instalación | 5.6.6 | 232 |
| McAfee Agent for MAC | Instalación | 5.5.1 | 342 |
| McAfee Agent for LINUX | Instalación | 5.6.6 | 232 |

Figura 31: Paquetes incorporados para McAfee Agent.

**Validación de paquetes de software para McAfee Endpoint Security**

A continuación, se muestran los paquetes que fueron incorporadas para McAfee Endpoint Security y sus versiones. Es importante mencionar que estos paquetes son necesarios para realizar el despliegue de productos de forma remota desde la consola. En la

[23] Grant Number: Numero de concesión único otorgado por McAfee que confirma los derechos de póliza de soporte de la empresa contratante, así como el derecho de descarga de productos de McAfee ligados al licenciamiento contratado. Este número es confidencial y no divulgarse a terceros o a usuarios finales (Number, 2018)

consola se realizan tareas de instalación o en su defecto crear tareas programas para enviar el despliegue. En la figura 32 se observan los paquetes incorporados para McAfee Endpoint Security.

- **Endpoint Security Platform**
- **Endpoint Security Threat Prevention**
- **Endpoint Security Firewall**
- **Endpoint Upgrade Assistant**

| | | | | |
|---|---|---|---|---|
| ☐ | Endpoint Security Firewall | Instalación | 10.7.0 | 1433 |
| ☐ | Endpoint Security Platform | Instalación | 10.7.0 | 2000 |
| ☐ | Endpoint Security Threat Prevention | Instalación | 10.7.0 | 2067 |
| ☐ | Endpoint Upgrade Assistant | Instalación | 2.1.0 | 53 |

Figura 32: Paquetes incorporados para McAfee Endpoint Security.

### Validación de paquetes de software para McAfee Data Loss Prevention

A continuación, se muestran los paquetes que fueron incorporadas para McAfee Data Loss Prevention y sus versiones. Es importante mencionar que estos paquetes son necesarios para realizar el despliegue de productos de forma remota desde la consola. En la consola se realizan tareas de instalación o en su defecto crear tareas programas para enviar el despliegue. En la figura 33 se observan los paquetes incorporados para McAfee Data Loss Prevention.

- **McAfee Data Loss Prevention**

| | Nombre | Tipo | Versión | Versión secundaria |
|---|---|---|---|---|
| ☐ | McAfee Data Loss Prevention | Instalación | 11.5.0 | 602 |

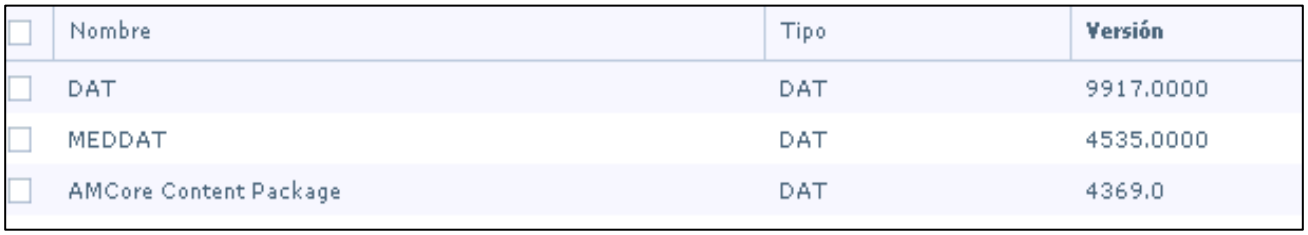
Figura 33: Paquetes incorporados para McAfee Data Loss Prevention.

### Validación de firmas de seguridad DAT y AMCore

Por último, vamos a validar que los motores de actualizaciones estén incorporados de manera correcta, es importante mencionar que la función de estos componentes es consultar

de manera diaria las actualizaciones o firmas de seguridad liberadas por McAfee y mediante tareas programadas, dichas actualizaciones son instaladas en los equipos finales que están administrados por la consola de McAfee ePO. En la figura 34 se observan las firmas de seguridad liberadas por McAfee.

- **DAT**
- **MEDDAT**
- **AMCore Content Package**



| Nombre | Tipo | Versión |
|---|---|---|
| DAT | DAT | 9917.0000 |
| MEDDAT | DAT | 4535.0000 |
| AMCore Content Package | DAT | 4369.0 |

Figura 34: Firmas de seguridad liberadas para McAfee ePO.

**Nota: Al momento de realizar la instalación ePolicy Orchestrator tenemos la opción de activar la instalación automática de productos. La descarga de productos se realiza conforme al licencia que se tienen contratada actualmente.**

## Configuración de directivas

Una directiva es un conjunto de parámetros de configuración que se crean, se configuran y, posteriormente, se implementan.

McAfee ePO organiza sus directivas por productos y, después, por las categorías de cada producto. Por ejemplo, el producto McAfee Agent incluye las categorías General, Repositorio y Solución de problemas (McAfee, Acerca de Politicas, 2019).

En este apartado vamos a mostrar a detalle la configuración de cada una de las directivas (políticas) que se crearon en la consola de McAfee ePO, donde estaremos validando de manera puntual los siguientes productos:

- **Configuración de directivas para McAfee Agent**
- **Configuración de directivas para Endpoint Security Common.**
- **Configuración de directivas para Endpoint Security Threat Prevention.**
- **Configuración de directivas para Endpoint Security Firewall**
- **Configuración de directivas para Data Loss Prevention.**

## Configuración de directivas para McAfee Agent

En el siguiente apartado vamos a mostrar las directivas que se tienen configuradas para el producto de McAfee Agent, para este producto vamos a observa las categorías de General y Repositorio.

Es importante mencionar que la directiva utilizada para todo Volkswagen de México es VMPuebla, el resto de las directivas son predefinidas al momento de incorporar los paquetes de instalación a ePolicy Orchestrator.

## General

A continuación, vamos a observar las configuraciones generales de McAfee Agent, en esta categoría podemos realizar configuraciones como la visibilidad del agente, permitir activación del agente, opciones de reinicio tras despliegue y el intervalo para la comunicación entre agente-servidor. En la Figura 35 se observan las configuraciones aplicadas para McAfee Agent.

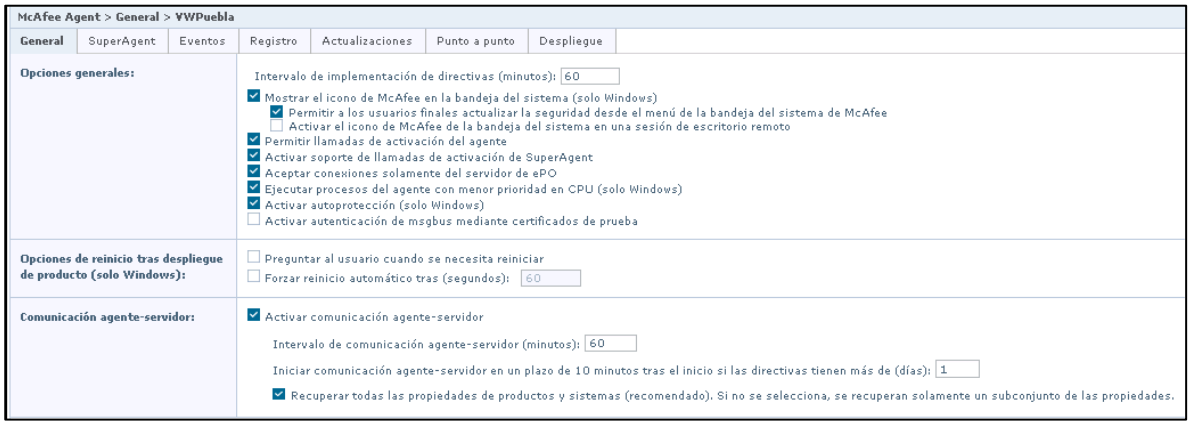



Figura 35: Configuración aplicada para el producto de McAfee Agent.

En la pestaña de Super Agent se activa por si existe la necesidad de que algún equipo cumpla con la función de un Relay, para esta política no se tiene habilitada esta opción. En la Figura 36 se observan las opciones deshabilitadas.

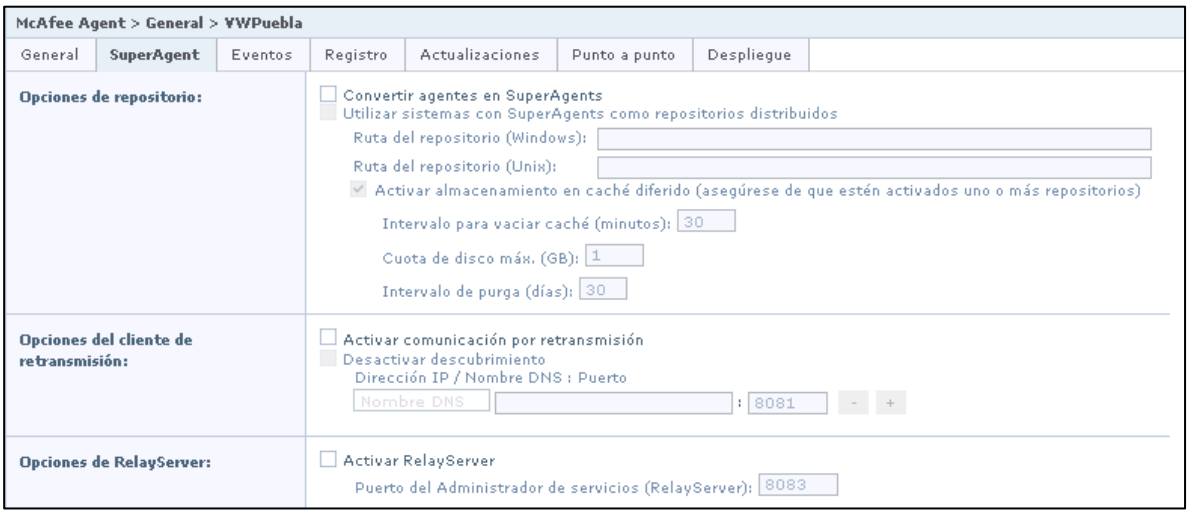


Figura 36: Opciones de SuperAgent deshabilitadas para McAfee Agent.

En la pestaña de Eventos, se realiza la activación de reenvío de eventos según la prioridad, donde vamos a seleccionar la prioridad Grave y los intervalos entre número de eventos y tiempo. En la figura 37 se observa el reenvío de eventos habilitada.

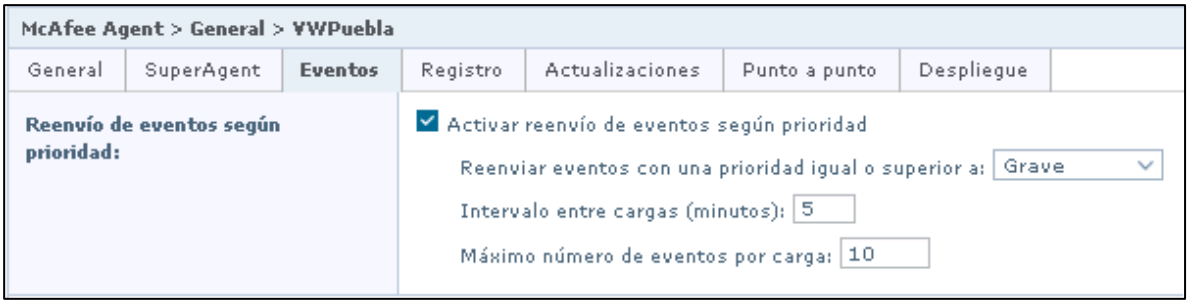


Figura 37: Reenvió de eventos por prioridad habilitada.

En la pestaña de Registro, se habilitaron las opciones de Registro de aplicación que permite a McAfee Agent registrar sus actividades en archivos de registro y Registro remoto, que permite que el registro de actividad del agente se muestre en la consola del servidor de McAfee ePO. En la figura 38 se observan las opciones habilitadas.


Figura 38: Registro de aplicaciones y registro remoto habilitados para McAfee Agent.

En la pestaña de Actualizaciones, vamos a indicar las firmas o motores de seguridad a actualizar cuando se ejecuten tareas de actualización, como Actualizar ahora, Ejecutar tarea cliente ahora o Actualización planificada desde McAfee ePO, solo se tienen en cuenta los paquetes seleccionados en este apartado. En la Figura 39 se observan las firmas y motores de seguridad que se estarán actualizando.

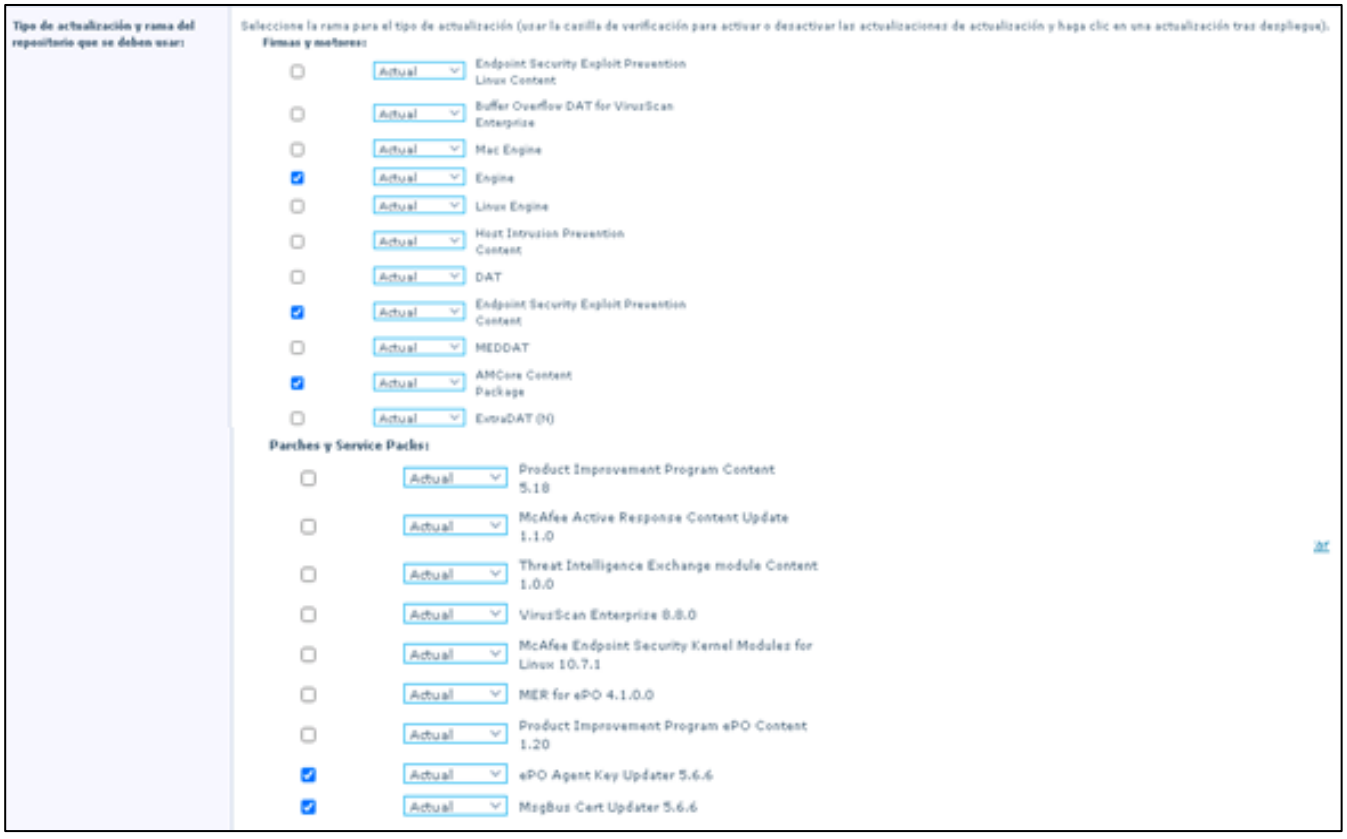



Figura 39: Firmas y motores de seguridad a actualizar para los equipos con McAfee Agent.

En la pestaña de Punto a Punto vamos a habilitar la opción de Activar la comunicación y Servicio de Punto a Punto ya que esto Permite al agente descargar actualizaciones de agentes del mismo nivel en la misma subred. En la figura 40 se observan las opciones de punto a punto habilitadas.

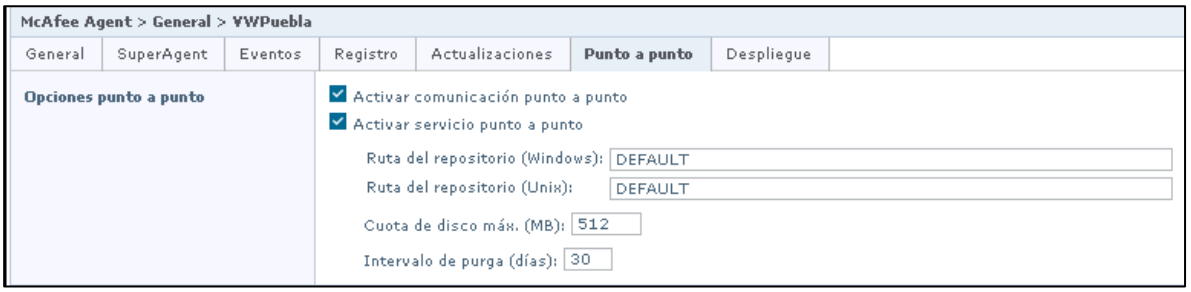



Figura 40: Opciones de Punto a Punto habilitadas para McAfee Agent.

## Repositorio

A continuación, vamos a observar los repositorios que fueron configurados para McAfee Agent, en esta categoría de manera predeterminada, la lista de repositorios disponibles gestionados por el servidor de McAfee ePO incluye los repositorios principales, de origen y de respaldo, y cualquier otro repositorio distribuido que haya configurado. También podemos agregar repositorios para indicarle a los equipos finales a donde se tiene que comunicar para la descarga de actualizaciones y productos.

El primer contacto es directamente al repositorio de la consola de McAfee ePO y el segundo a los sitios oficiales de McAfee, de igual manera se podrá configurar un proxy en caso de ser necesario. la Figura 41 se observan la lista de repositorios configurados para McAfee Agent.

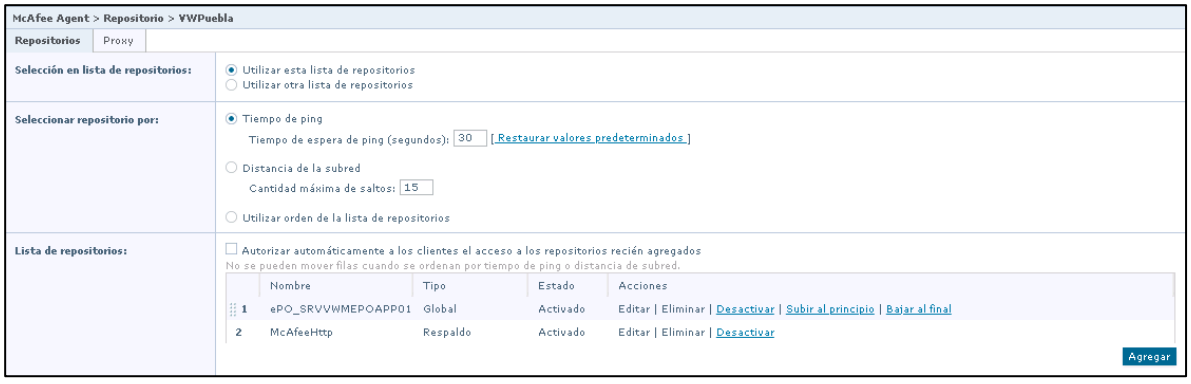



Figura 41: Lista de repositorios configurados para McAfee Agent.

## Configuración de directivas para McAfee Endpoint Security Common

En el siguiente apartado vamos a mostrar las directivas que se tienen configuradas para el producto de McAfee Endpoint Security Common, para este producto solo vamos a observa las categorías de Opciones.

Es importante mencionar que la directiva utilizada para todo Volkswagen de México es VMPuebla, el resto de las directivas son predefinidas al momento de incorporar los paquetes de instalación a ePolicy Orchestrator.

## Opciones

A continuación, vamos a observar las configuraciones generales de la interfaz de usuario de Endpoint Security, en esta categoría podemos realizar configuraciones como el acceso a la interfaz gráfica, contraseña para desinstalación del cliente, idioma, exclusiones, registro de eventos, actualizaciones del cliente. En la Figura 42 se observan las configuraciones de Interfaz del cliente, contraseña de desinstalación e idioma para McAfee Endpoint Security Common.

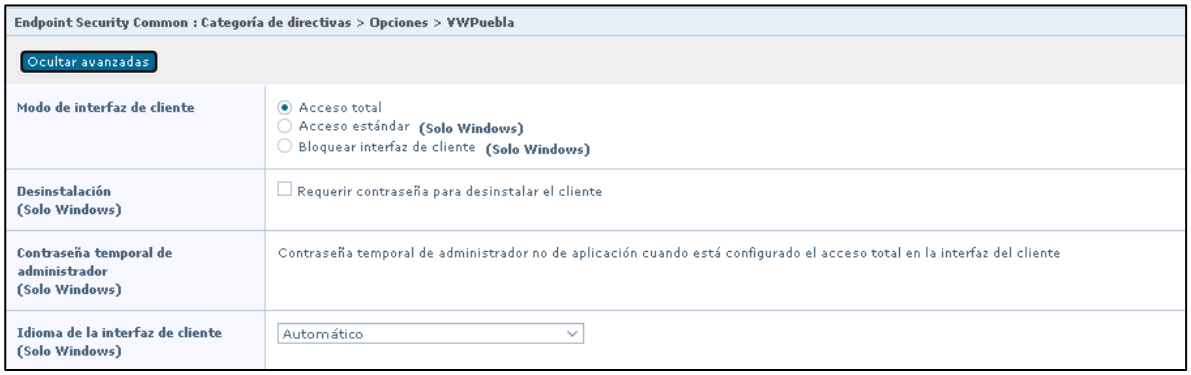



Figura 42: Modo de interfaz de cliente, contraseña de desinstalación e idioma para McAfee Endpoint Security Common.

En la opción de Autoproteccion vamos a seleccionar las acciones que se realizaran para archivos y carpetas, registros y procesos. En la figura 43 de observan las configuraciones aplicadas para Autoproteccion.

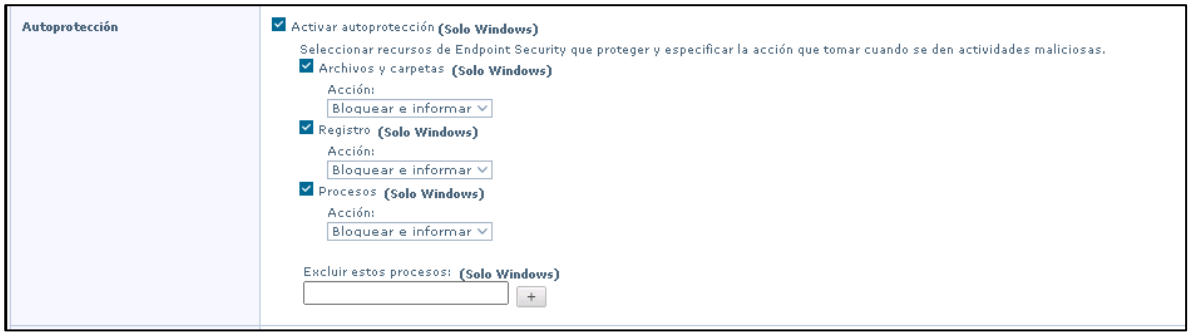



Figura 43: Opciones configuradas en Autoproteccion para McAfee Endpoint Security Common.

En la opción de Registro de eventos vamos a seleccionar él envió de eventos a la consola de administración McAfee ePO, aquí vamos a seleccionar la severidad de evento a reportar por cada categoría, en las que encontramos el producto de Prevención de amenazas (Protección de acceso, Prevencion de exploit, análisis en tiempo real y análisis bajo demanda) y Firewall. En la figura 44 se observan las configuraciones aplicadas para Registros de eventos.

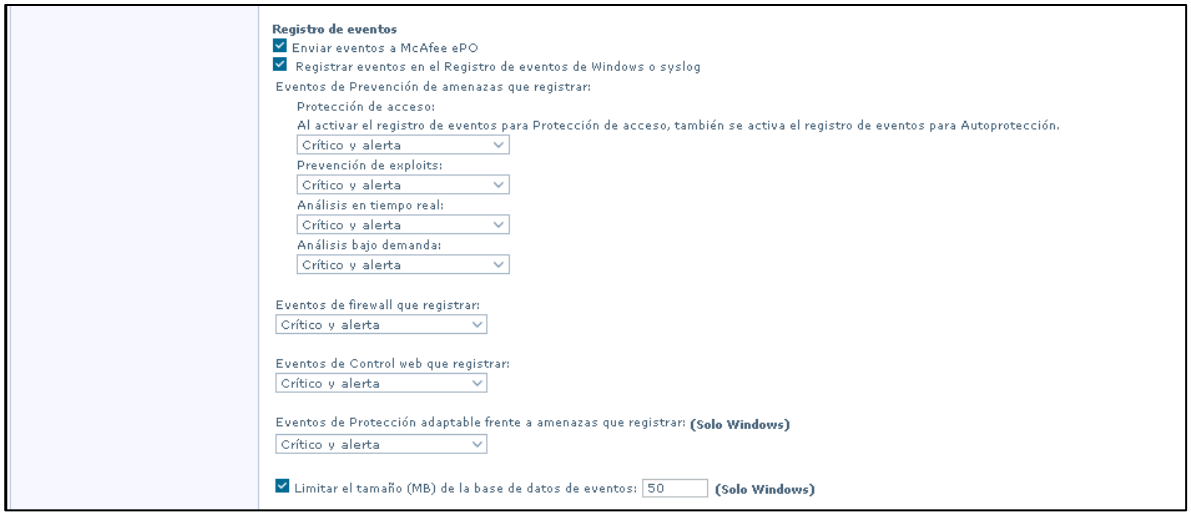



Figura 44: Opciones configuradas en Registro de eventos para McAfee Endpoint Security Common.

En la opción de proxy vamos a indicar que no se tiene un servidor proxy, para las actualizaciones del cliente vamos a habilitar el botón de Actualizar ahora y Planificación de tareas de actualización, después seleccionamos para que se actualicen todo el contenido de seguridad. En la figura 45 se observan las configuraciones aplicadas para proxy y actualizaciones predeterminadas.

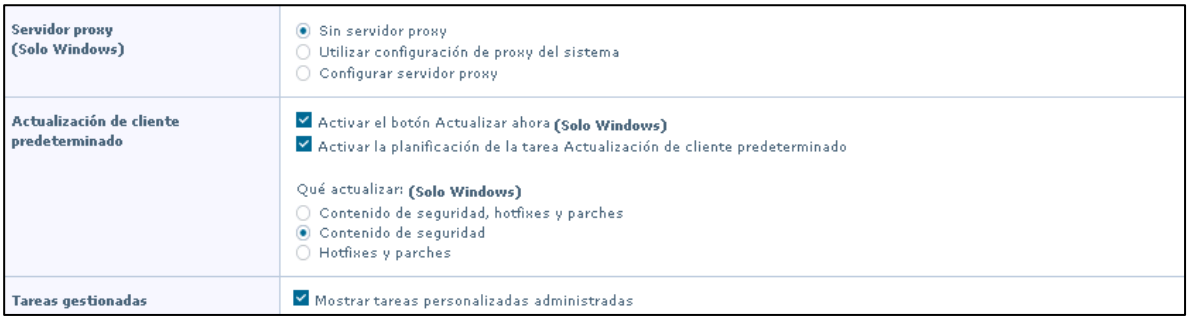



Figura 45: Opciones configuradas en Proxy y configuraciones predeterminadas para McAfee Endpoint Security Common.

## Configuración de directivas para McAfee Endpoint Security Threat Prevention

En el siguiente apartado vamos a mostrar las directivas que se tienen configuradas para el producto de McAfee Endpoint Security Threat Prevention, para este producto vamos a observa las categorías de Análisis en tiempo real, Análisis bajo demanda, Opciones, Protección de Acceso y Prevencion de exploit. Para cada categoría vamos a explicar las opciones que se tienen configuradas. Las directivas que se tienen para este módulo son:

- **VWPuebla – Asignada a toda la organización**
- **VWPuebla_Servidores – Asignada solo a servidores**
- **VWPuebla_ENS_Down – Creada para deshabilitar la protección en los equipos**

A continuación, mostramos las configuraciones que se tienen en la directiva de VWPuebla para la categoría de análisis en tiempo real.

### Análisis en tiempo real

El análisis en tiempo real examina todos los archivos del equipo a medida que el usuario accede a ellos, y proporciona una detección continua y en tiempo real de las amenazas y analiza los archivos en la ubicación por donde entran al sistema por primera vez. Cuando se producen detecciones, el analizador en tiempo real envía notificaciones a la interfaz del servicio (RealTime, 2019).

En la categoría de análisis en tiempo real vamos a habilitar la directiva, de igual manera vamos a indicar si para que analice al iniciar el sistema, el máximo de segundos para el análisis de los archivos, analizar los sectores de arranque, analizar la copia de archivos a medios compartidos o externos y los archivos de correo electrónico adjuntos.

La opción de GTI [24] la vamos a habilitar con un nivel de sensibilidad Alto. Activaremos el modo de AMSI[25] y mostrar mensaje a los usuarios cuando se detecte una amenaza. En la figura 46 mostramos las configuraciones aplicadas para análisis bajo en tiempo real.

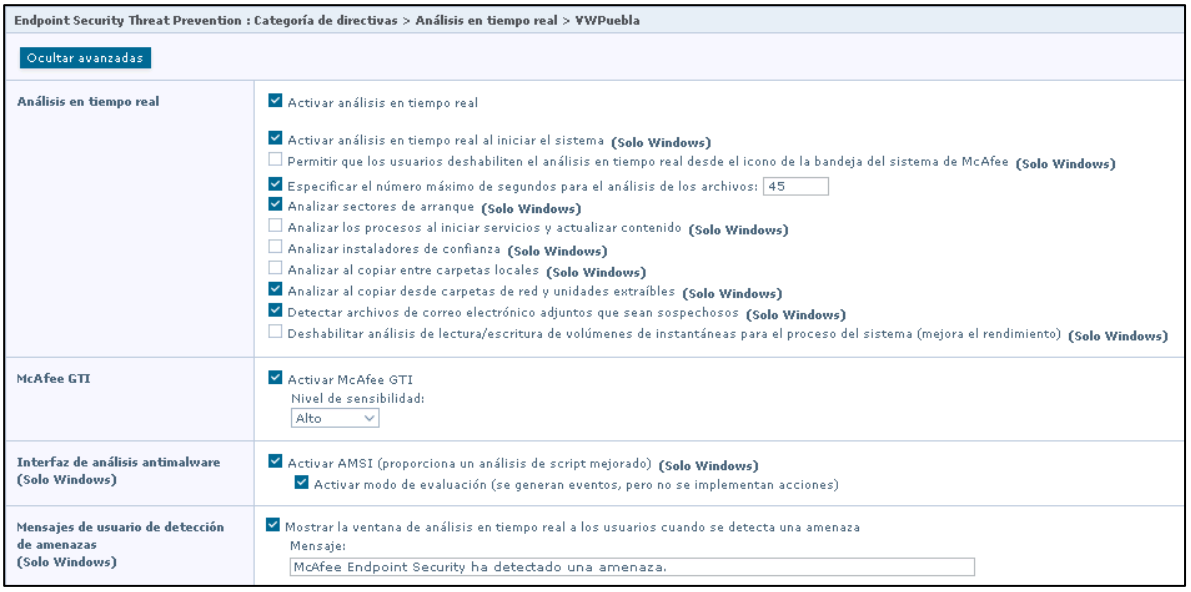



Figura 46: Opciones configuradas para análisis en tiempo real.

Para el análisis en tipos de procesos vamos a seleccionar la opción estándar, donde indicaremos cuando analizar, que analizar y las opciones de análisis adicionales. En la figura 47 vamos a observar las configuraciones aplicadas para los tipos de análisis en tiempo real.

[24] McAfee GTI utiliza heurística o reputación de archivos para buscar archivos sospechosos mediante el análisis en tiempo real y el análisis bajo demanda. Envía huellas digitales de muestras, o hashes, a un servidor de base de datos central alojado por McAfee Labs a fin de determinar si son malware. Al enviar hashes, la detección podría estar disponible antes que la próxima actualización de archivos de contenido, cuando McAfee Labs publique la actualización (McAfeeGTI, 2018)

[25] AMSI proporcionar protección frente a scripts que no están basados en un navegador, tales como PowerShell, JavaScript y VBScript.

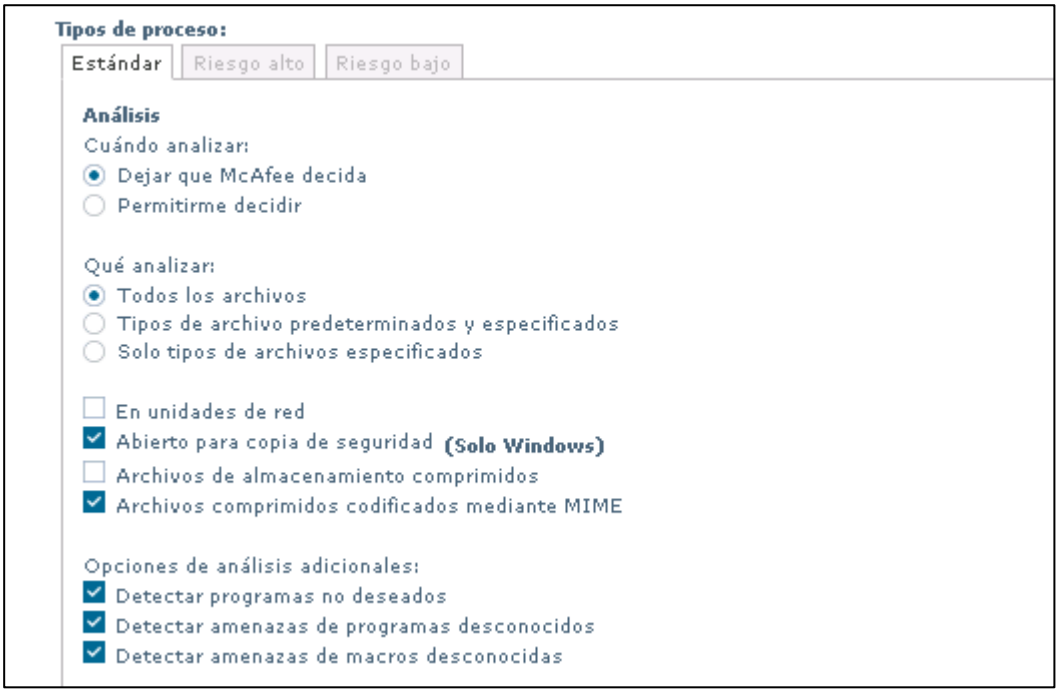



Figura 47: Tipos de procesos para la opción de análisis en tiempo real.

En la siguiente opción vamos a configurar las acciones que se van a realizar al momento de detectar una amenaza o un programa no deseado, así como indicar la segunda acción en caso de que la primera acción falle. Por el momento no es necesario configurar para ambientes Linux. En la figura 48 se observan las configuraciones aplicadas para las acciones al momento de detectar una amenaza.

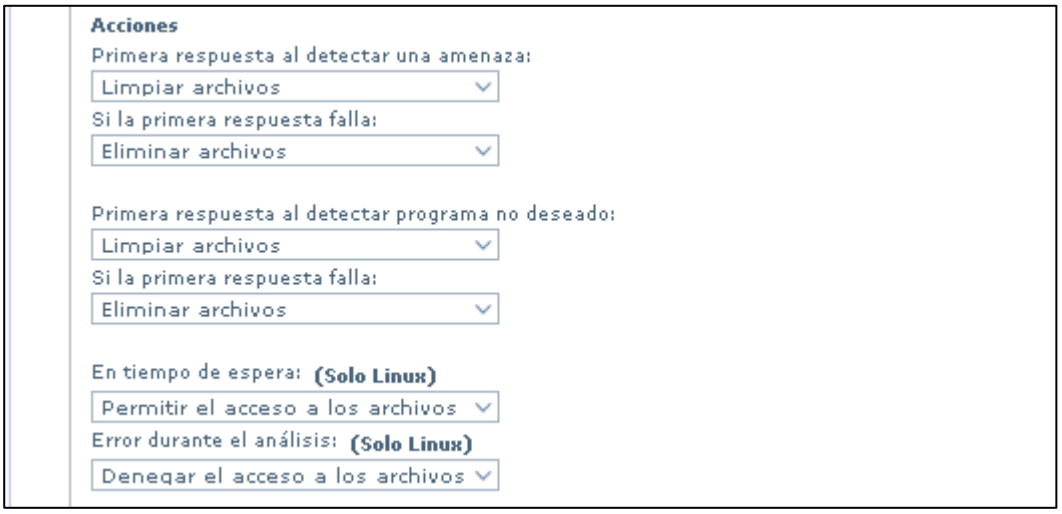



Figura 48: Acciones a realizar al detectar una amenaza en el análisis en tiempo real.

En la opción de Exclusiones, vamos a indicar las rutas o programas que no queremos que se analicen por la categoría de tiempo real, esto es derivado a que las aplicaciones son confiables y/o conocidas y por buenas prácticas, se recomienda excluirlas para no afectar su funcionamiento, de igual manera habilitamos ScriptScan[26]. En la Figura 49 se observan las exclusiones aplicadas para análisis en tiempo real.

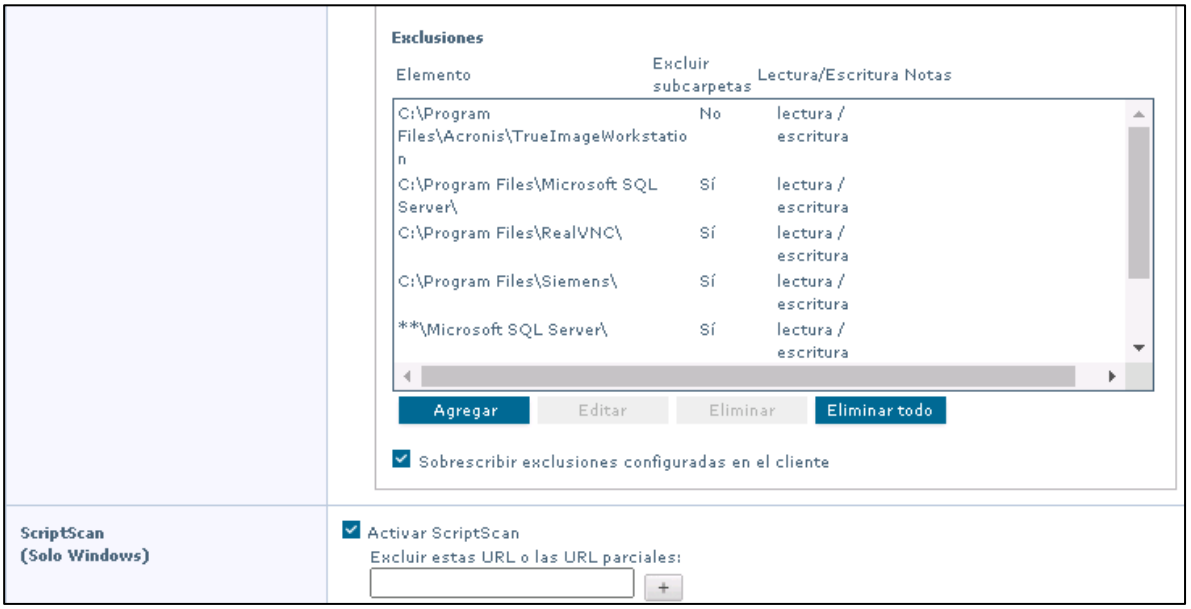



Figura 49: Exclusiones aplicadas para el análisis en tiempo real.

A continuación, mostramos las configuraciones que se tienen en la directiva de VWPuebla_Servidores. Es importante mencionar que los servidores tienen funciones y aplicaciones diferentes a los equipos de usuarios finales, es por ello por lo que se creó una directiva específica para servidores.

En la opción de análisis en tiempo real vamos a habilitar la directiva, de igual manera vamos a indicar si para que analice al iniciar el sistema, el máximo de segundos para el análisis de los archivos, analizar los sectores de arranque, analizar la copia de archivos a medios compartidos o externos y los archivos de correo electrónico adjuntos.

[26] ScriptScan es un objeto auxiliar de explorador que examina código de JavaScript y VBScript en busca de scripts maliciosos antes de que se ejecuten. Si el script está limpio, lo pasa a JavaScript o VBScript para su procesamiento. Si ScriptScan detecta un script malicioso, lo bloquea para que no se ejecute.

La opción de GTI la vamos a habilitar con un nivel de sensibilidad Alto. Activaremos el modo de AMSI y mostrar mensaje a los usuarios cuando se detecte una amenaza. En la figura 50 mostramos las configuraciones aplicadas para análisis bajo en tiempo real para servidores.

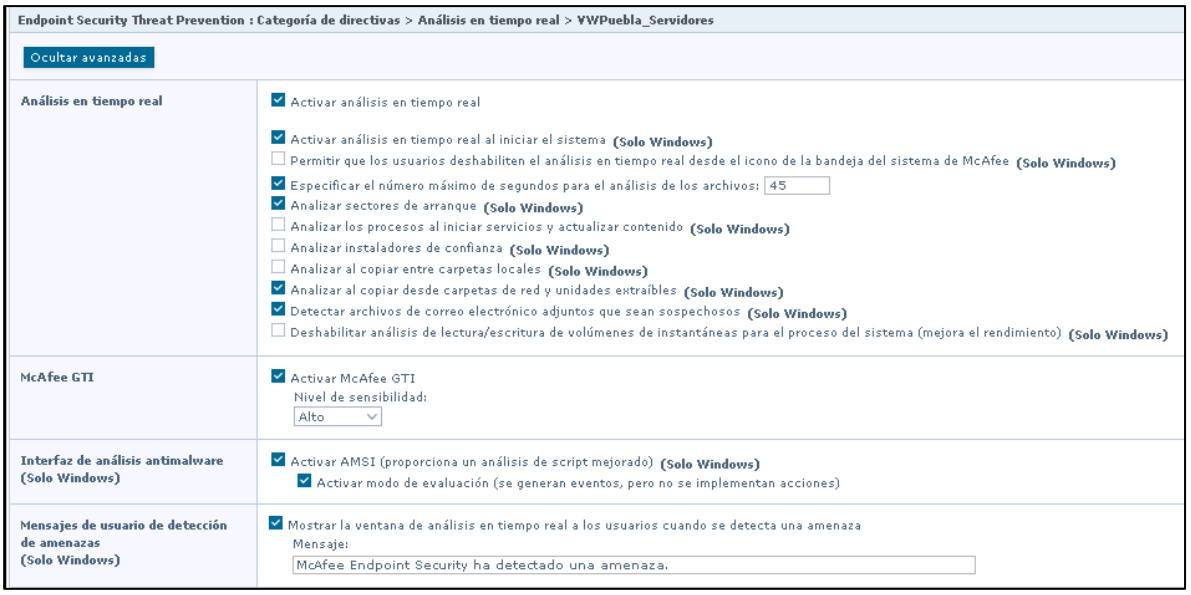



Figura 50: Opciones configuradas para análisis en tiempo real en servidores

Para el análisis en tipos de procesos vamos a seleccionar la opción estándar, donde indicaremos cuando analizar, que analizar y las opciones de análisis adicionales, así como las acciones que se van a realizar al momento de detectar una amenaza o un programa no deseado. En la figura 51 vamos a observar las configuraciones aplicadas para los tipos de análisis en tiempo real para servidores.

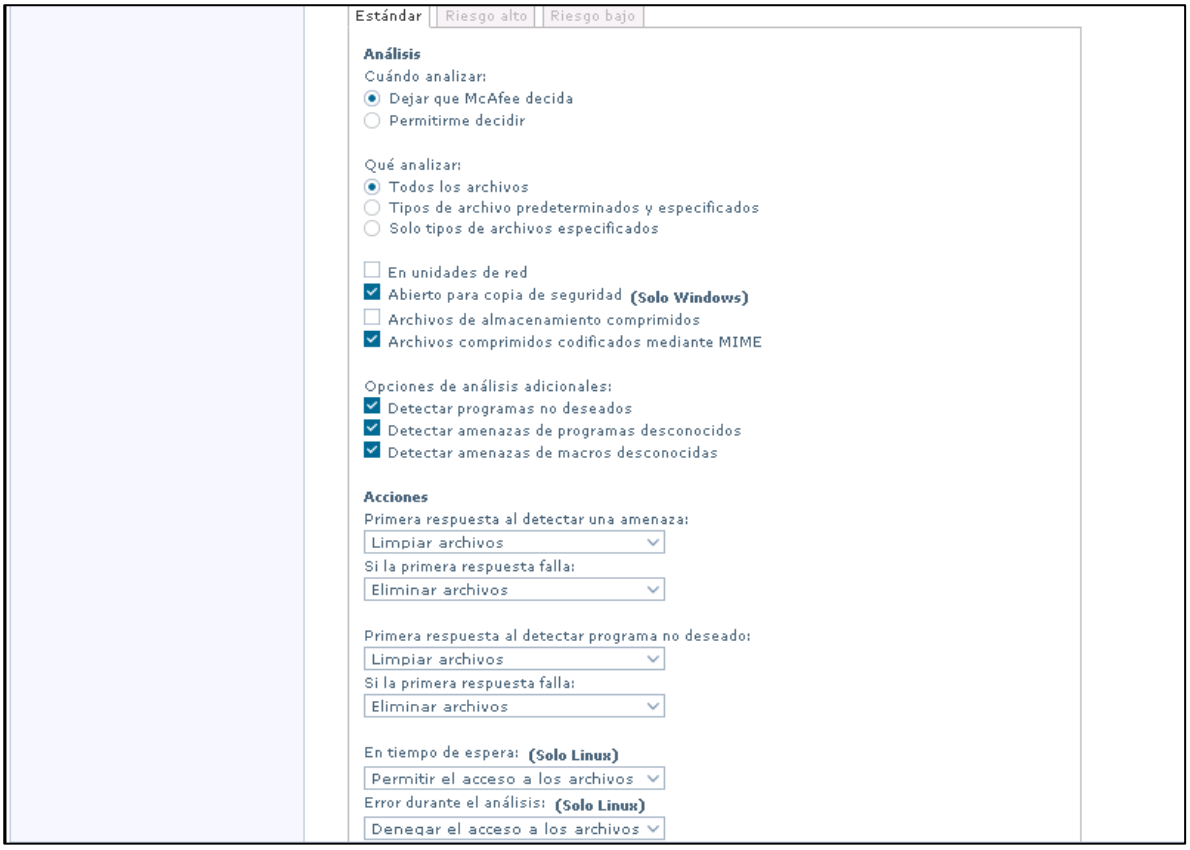



Figura 51: Tipos de procesos y acciones para la opción de análisis en tiempo real en servidores

En la opción de Exclusiones, vamos a indicar las rutas o programas que no queremos que se analicen por la categoría de tiempo real, esto es derivado a que las aplicaciones son confiables y/o conocidas y por buenas prácticas, se recomienda excluirlas para no afectar su funcionamiento, de igual manera habilitamos ScriptScan. En la Figura 52 se observan las exclusiones aplicadas para análisis en tiempo real.

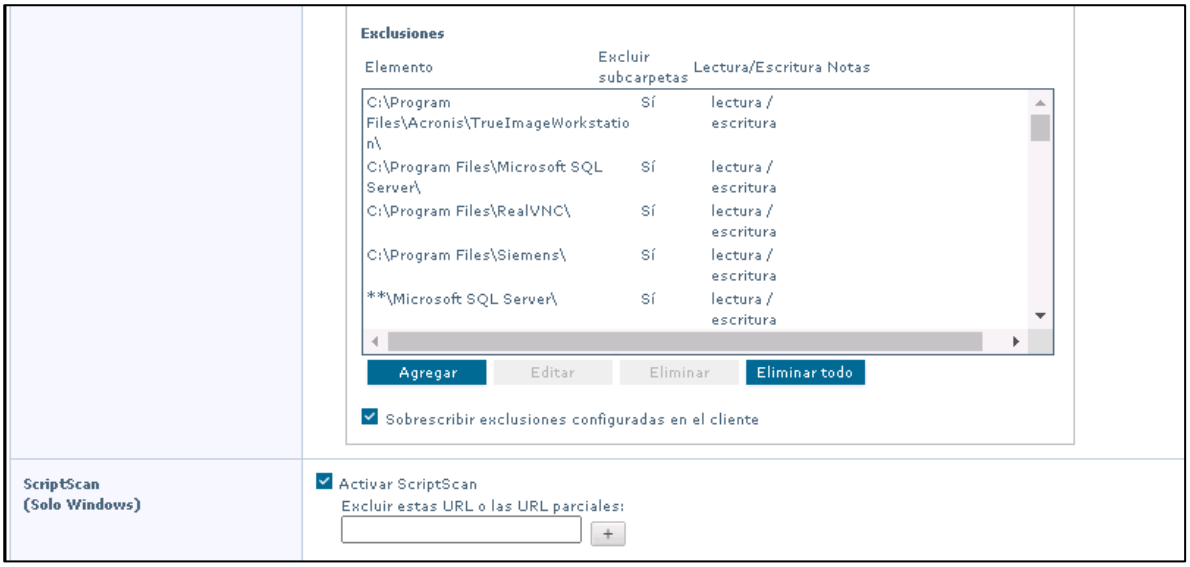



Figura 52: Exclusiones aplicadas para el análisis en tiempo real en servidores.

A continuación, mostramos las configuraciones que se tienen en la directiva de VWPuebla_ENS_Down. Es importante mencionar que esta directiva es creada con la finalidad de deshabilitar la protección en los equipos o servidores.

La casilla de Activar análisis en tiempo real no se encuentra seleccionada, por lo que esta directiva se encuentra deshabilitada. En la figura 53 se observa la directiva deshabilitada.

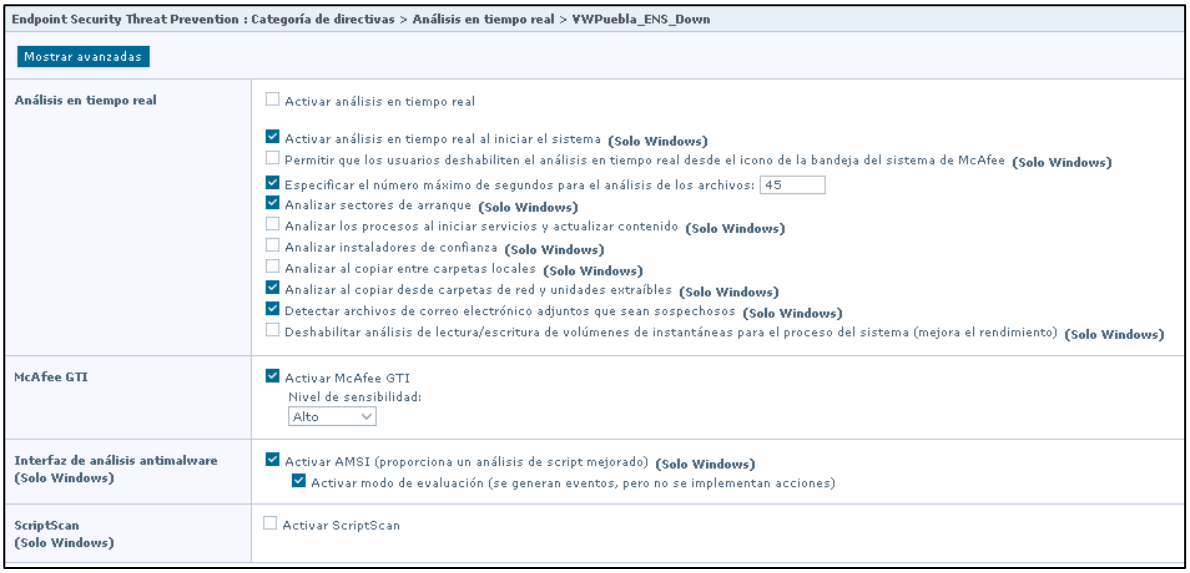



Figura 53: El análisis en tiempo real se encuentra deshabilitado.

**Análisis bajo demanda**

El analizador bajo demanda analiza los archivos, las carpetas, la memoria y el registro en busca de malware que pueda haber infectado el equipo. Puede decidir cuándo y con qué frecuencia se realizan los análisis bajo demanda. Es posible analizar los sistemas manualmente, en un momento planificado o durante el inicio.

En la categoría de análisis bajo demanda vamos a observar los tipos de análisis que se pueden ejecutar, así como las ruta, procesos o tipos de archivos que se requieren analizar, también podemos planificar estos análisis e indicar las acciones a realizar.

A continuación, mostramos las configuraciones que se tienen en la directiva de VWPuebla para la categoría de análisis bajo demanda.

En la pestaña de Análisis completo se configuro los sectores de arranque y archivos comprimidos que se requieren analizar, en análisis adicionales se analizara los programas no deseados, programas desconocidos y macros, de igual manera indicamos las ubicaciones a analizar. En la figura 54 se observa que analizar, opciones adicionales y ubicaciones.

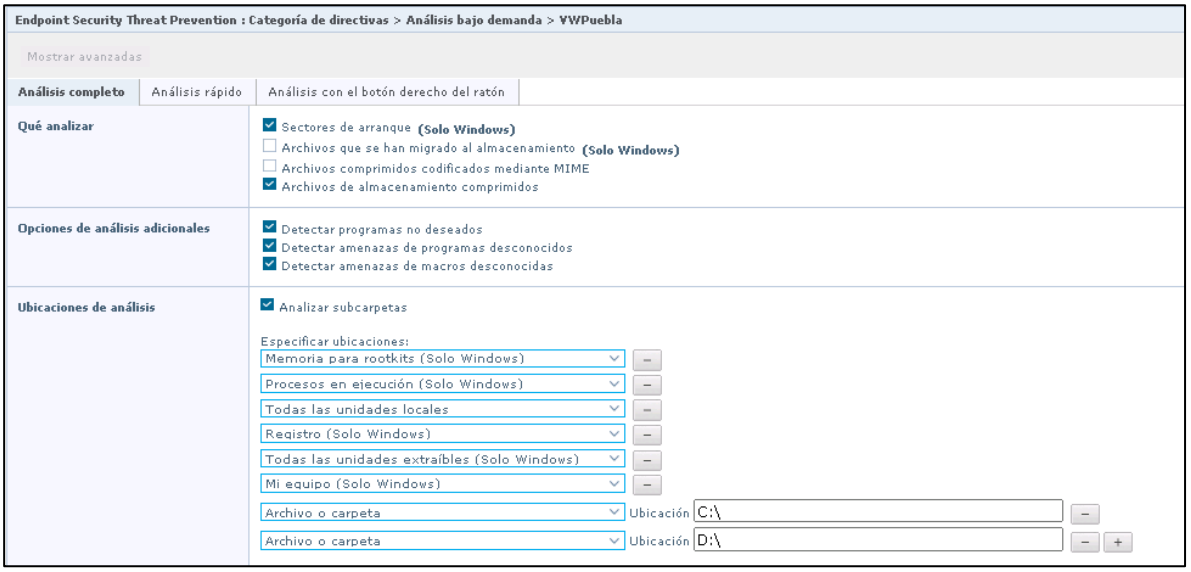



Figura 54: Se configura que analizar, opciones adicionales y ubicaciones para análisis bajo demanda.

En la siguiente opción se configuraron las acciones que se van a realizar al detectar una amenaza, así como la planificación del análisis y el rendimiento del equipo al momento de

analizar. En la figura 55 se observan las configuraciones para acciones, análisis planificado y rendimiento.

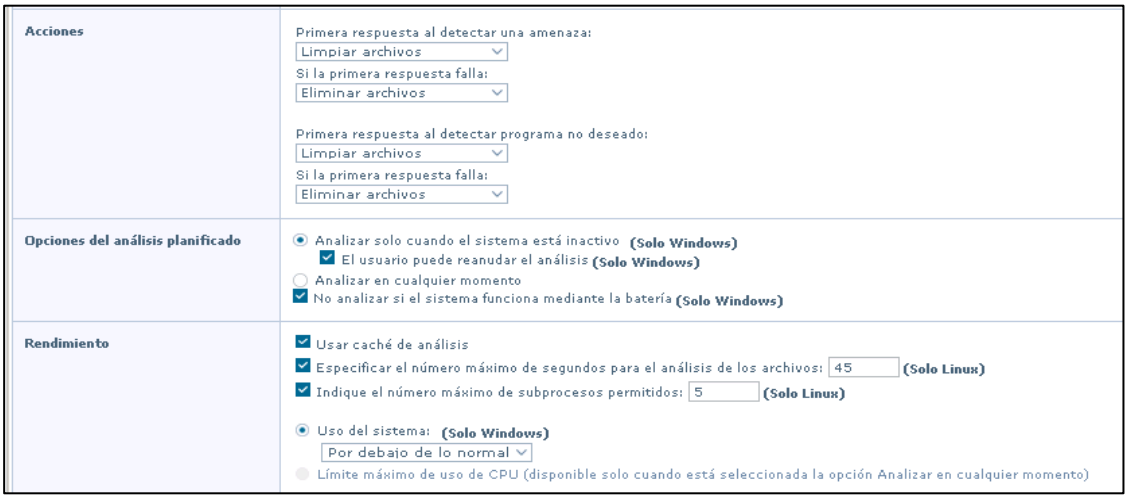



Figura 55: Se configura accionar a realizar, planificación y rendimiento para análisis bajo demanda.

En la pestaña de análisis rápido de igual manera se configuro los sectores de arranque y archivos comprimidos que se requieren analizar, en análisis adicionales se analizara los programas no deseados, programas desconocidos y macros, de igual manera indicamos las ubicaciones y los tipos de archivos a analizar. En la figura 56 se observa que analizar, opciones adicionales, ubicaciones y tipos de archivos.

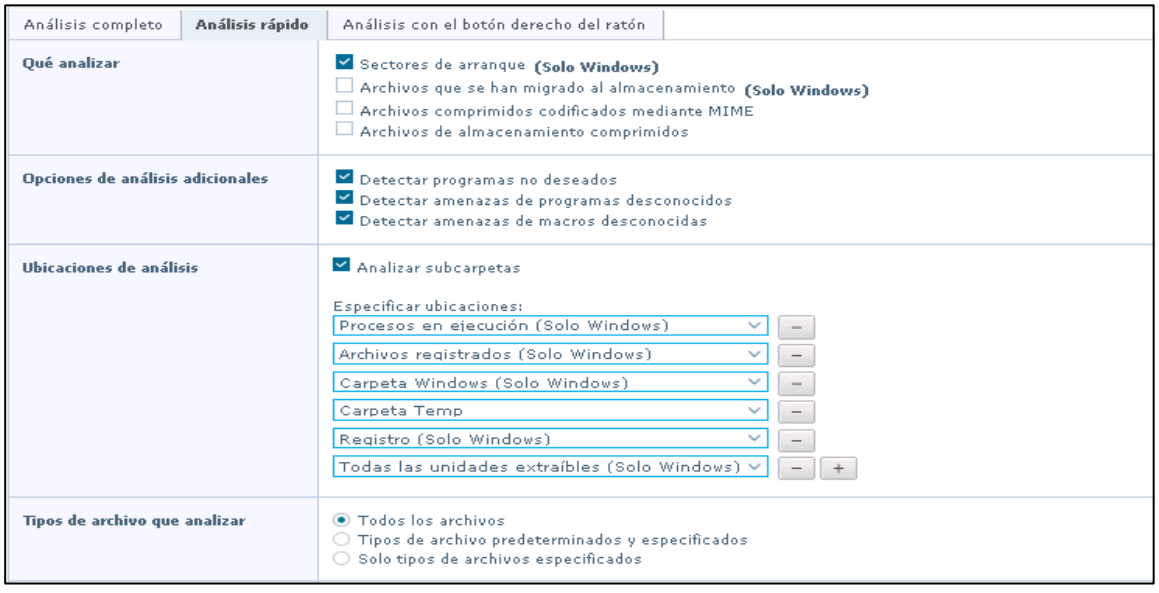



Figura 56: Se configura que analizar, opciones adicionales ubicación y tipo de archivos para análisis bajo demanda.

De igual manera en la siguiente opción se configuraron las acciones que se van a realizar al detectar una amenaza, así como la planificación del análisis y el rendimiento del equipo al momento de analizar. En la figura 57 se observan las configuraciones para acciones, análisis planificado y rendimiento.


Figura 57: Se configura accionar a realizar, planificación y rendimiento para análisis bajo demanda.

Por último, en la pestaña de análisis con el botón derecho del ratón se configuro analizar los archivos comprimidos y subcarpetas, así como programas de deseados, programas desconocidos y macros, y todos los archivos. En la figura 58 se observa que analizar, opciones adicionales y tipos de archivos.

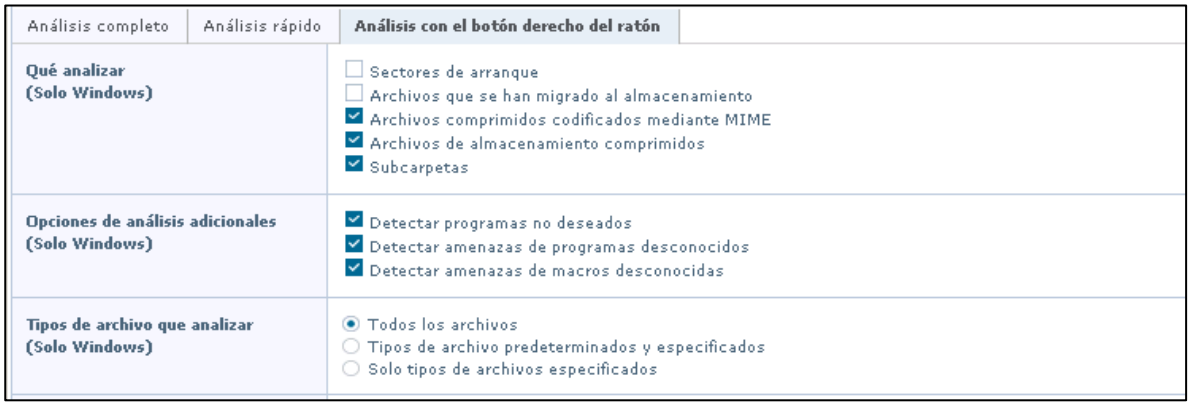



Figura 58: Se configura que analizar, opciones adicionales y tipo de archivos para análisis con el botón derecho del ratón.

En la siguiente opción se configuraron las acciones que se van a realizar al detectar una amenaza y el rendimiento del equipo al momento de analizar. En la figura 59 se observan las configuraciones para acciones y rendimiento.

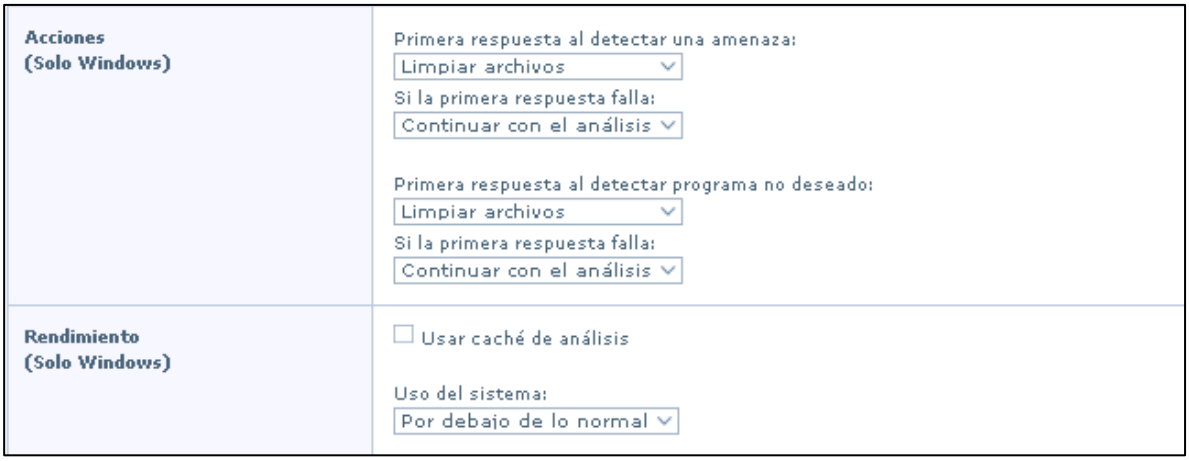



Figura 59: Se configura acciones a realizar y rendimiento para análisis con el botón derecho del ratón.

A continuación, mostramos las configuraciones que se tienen en la directiva de VWPuebla_Servidores para de análisis bajo demanda.

En la pestaña de Análisis completo se configuro los sectores de arranque y archivos comprimidos que se requieren analizar, en análisis adicionales se analizara los programas no deseados, programas desconocidos y macros, de igual manera indicamos las ubicaciones a analizar y los tipos de archivos. En la figura 60 se observa que analizar, opciones adicionales, ubicaciones y tipos de archivos para servidores.

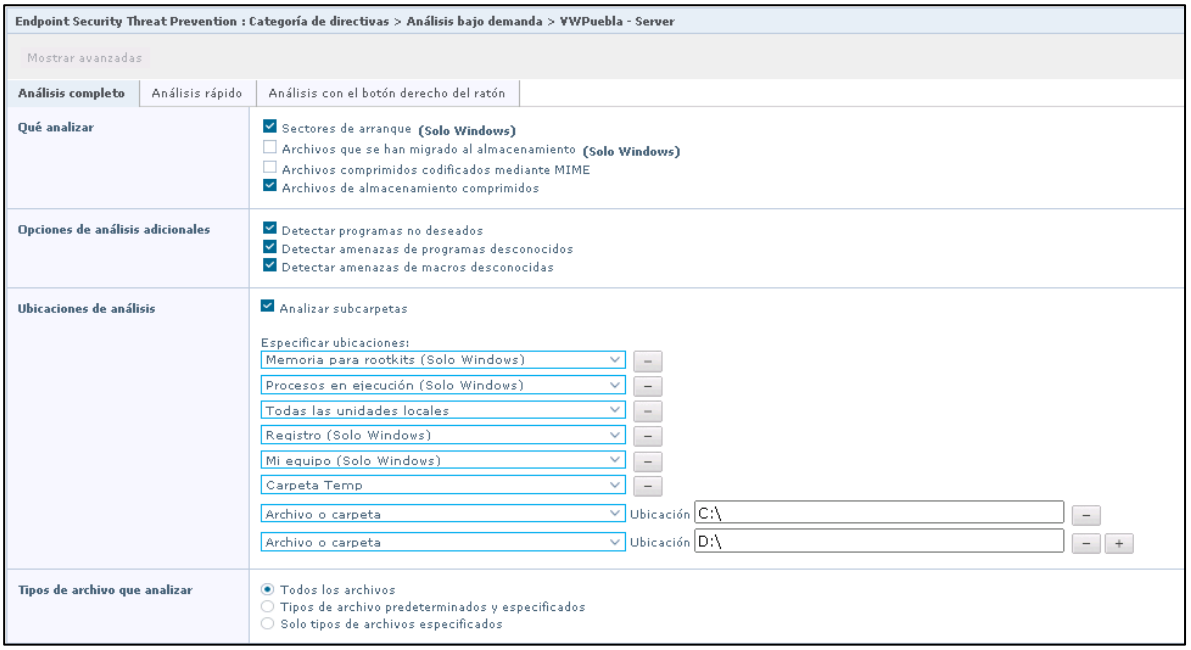



Figura 60: Se configura que analizar, opciones adicionales, ubicaciones y tipos de archivos para análisis bajo demanda para servidores.

En la siguiente opción se configuraron las acciones que se van a realizar al detectar una amenaza, así como la planificación del análisis y el rendimiento del equipo al momento de analizar. En la figura 61 se observan las configuraciones para acciones, análisis planificado y rendimiento.

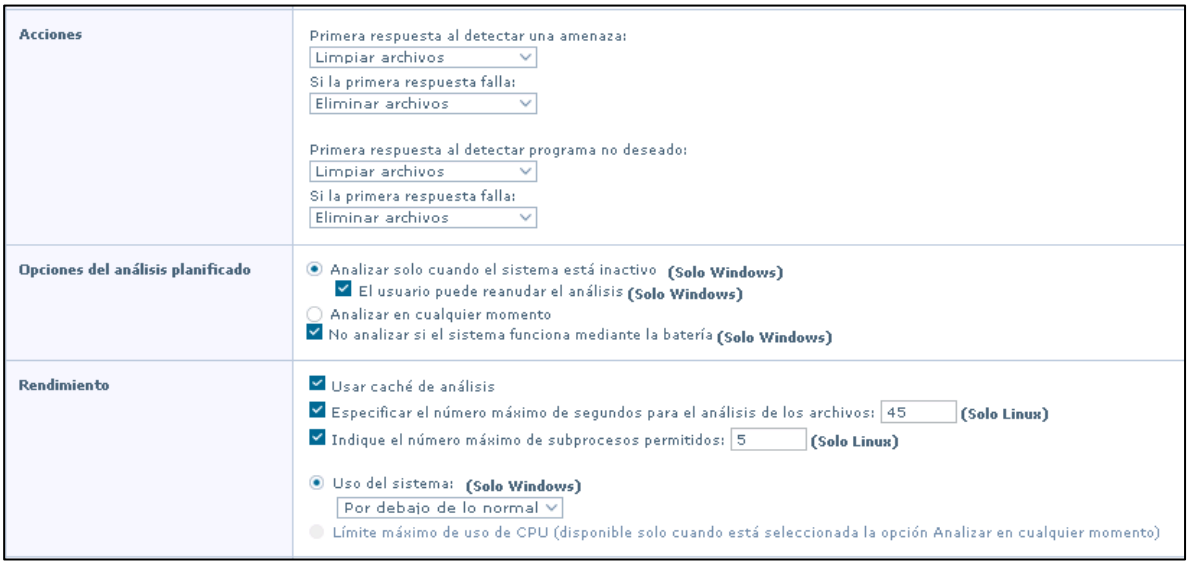



Figura 61: Se configura accionar a realizar, planificación y rendimiento para análisis bajo demanda para servidores.

En la pestaña de análisis rápido se configuro los sectores de arranque, en análisis adicionales se analizará los programas no deseados, programas desconocidos y macros, indicamos las ubicaciones y los tipos de archivos a analizar. En la figura 62 se observa que analizar, opciones adicionales, ubicaciones y tipos de archivos.

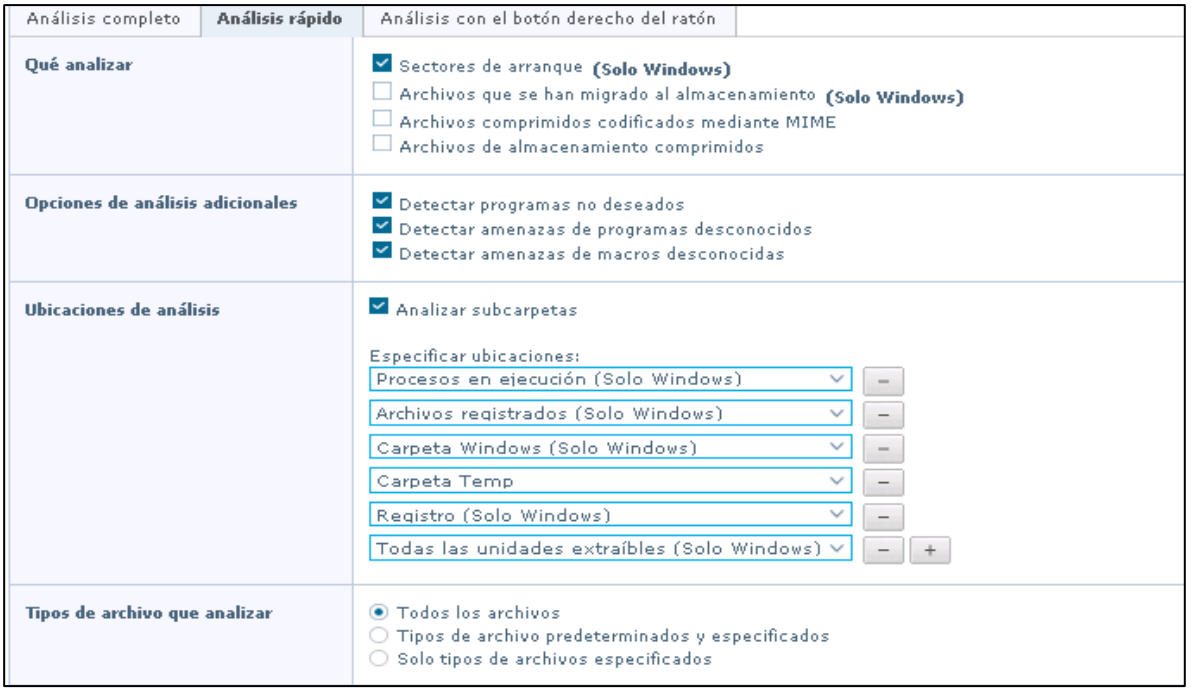



Figura 62: Se configura que analizar, opciones adicionales ubicación y tipo de archivos para análisis bajo demanda en servidores.

En la siguiente opción se configuraron las acciones que se van a realizar al detectar una amenaza, así como la planificación del análisis y el rendimiento del equipo al momento de analizar. En la figura 63 se observan las configuraciones para acciones, análisis planificado y rendimiento.

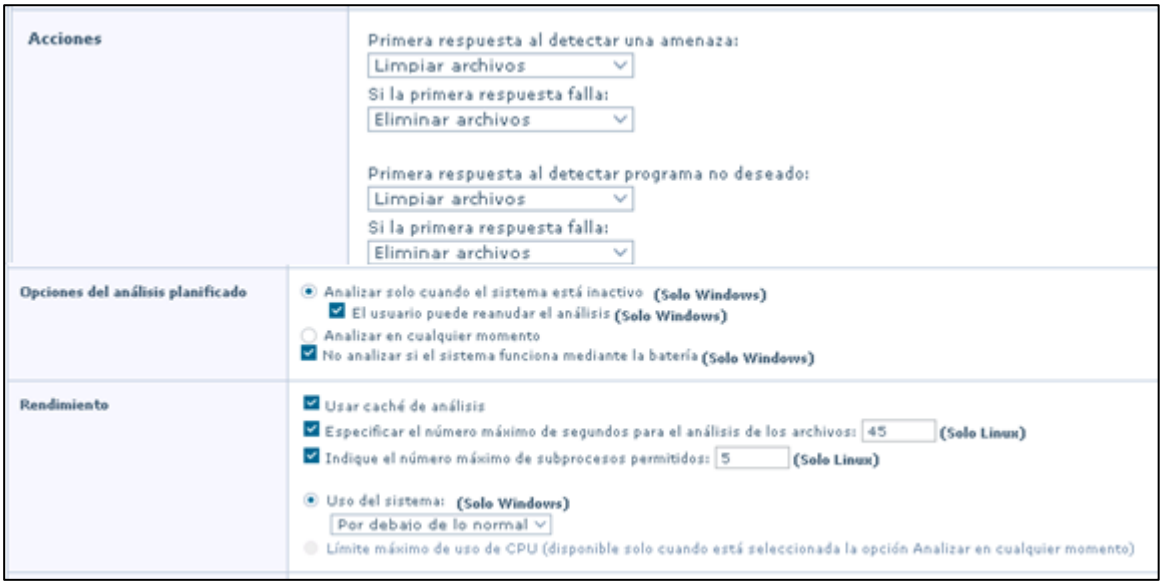



Figura 63: Se configura acción a realizar, planificación y rendimiento para análisis bajo demanda.

Por último, en la pestaña de análisis con el botón derecho del ratón se configuro analizar los archivos comprimidos y subcarpetas, así como programas de deseados, programas desconocidos y macros, y todos los archivos. En la figura 64 se observa que analizar, opciones adicionales y tipos de archivos.

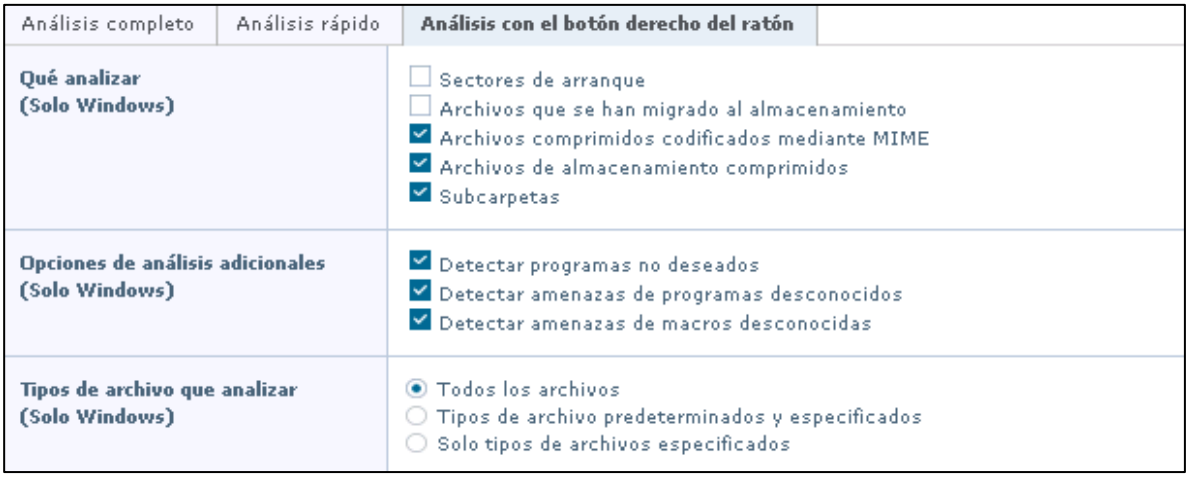



Figura 64: Se configura que analizar, opciones adicionales y tipo de archivos para análisis con el botón derecho del ratón para servidores.

En la siguiente opción se configuraron las acciones que se van a realizar al detectar una amenaza y el rendimiento del equipo al momento de analizar. En la figura 65 se observan las configuraciones para acciones y rendimiento.

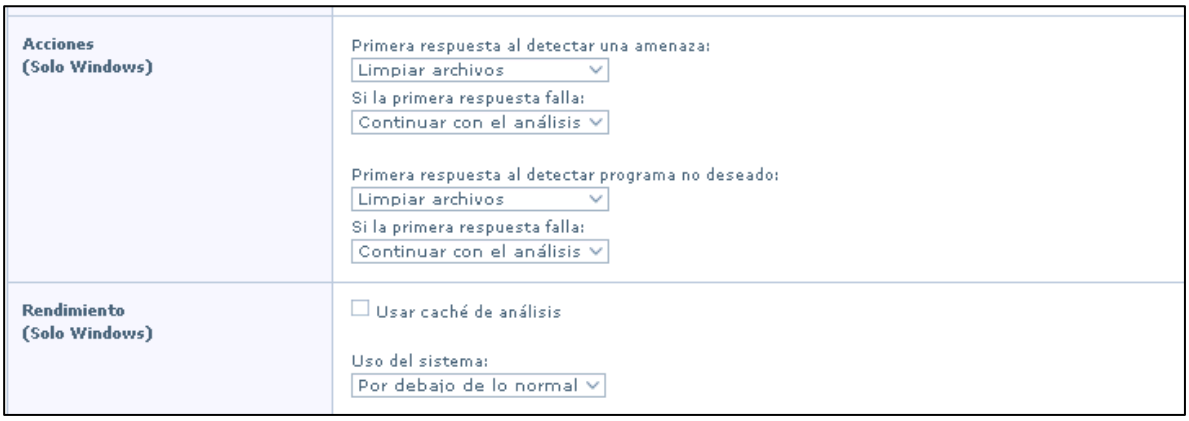



Figura 65: Se configura acciones a realizar y rendimiento para análisis con el botón derecho del ratón para servidores.

**Opciones (Prevención de amenazas)**

En la siguiente categoría se configuro la ubicación para almacenar los archivos en cuarentena, exclusiones por nombre de amenaza, detección de programas potencialmente no deseados por categorías y el análisis proactivo de datos.

A continuación, mostramos las configuraciones que se tienen en la directiva de VWPuebla para la categoría de Opciones.

En la opción de administrador de cuarentena se configuro la ubicación donde se van a almacenar todas aquellas amenazas detectadas y enviadas a cuarentena, así como los días que se guardaran los archivos en la carpeta de cuarentena. Por el momento no se configuraron exclusiones por nombres de detección. En la figura 66 se muestran la ruta de almacenamiento de cuarentena y los días en que se guardaran estas muestras.

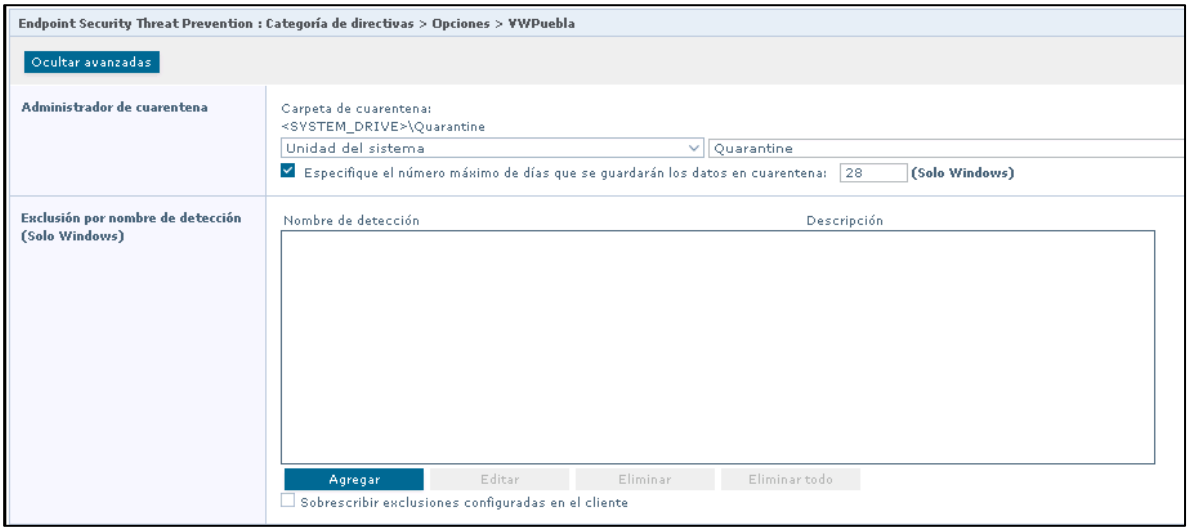



Figura 66: Ubicación y días de almacenamiento para los archivos en cuarentena.

En la siguiente opción se configuraron las categorías de los programas potencialmente no deseados y el análisis proactivo de datos. En la figura 67 se muestra la detección de programas potencialmente no deseado y el análisis proactivo de datos.

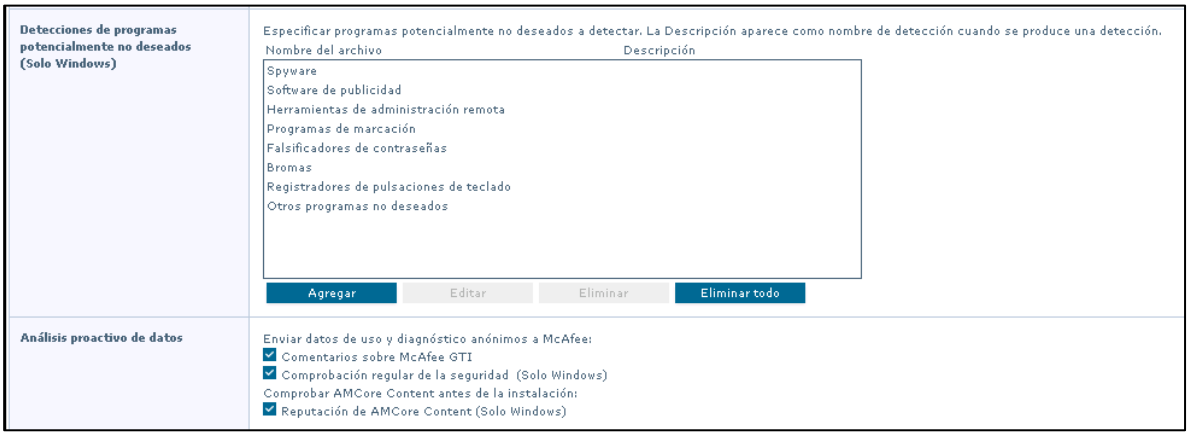



Figura 67: Detección de programamos potencialmente no deseados y análisis proactivo de datos.

A continuación, mostramos las configuraciones que se tienen en la directiva de Exclusiones_Servidores_Perceptron para la categoría de Opciones. Para esta categoría se realizó una directiva para servidores de Perceptron.

En la opción de administrador de cuarentena se configuro la ubicación donde se van a almacenar todas aquellas amenazas detectadas y enviadas a cuarentena, así como los días que se guardaran los archivos en la carpeta de cuarentena. También se aplicaron exclusiones

de aplicaciones utilizadas por estos servidores. En la figura 68 se muestran las configuraciones aplicadas para los servidores de Perceptron.

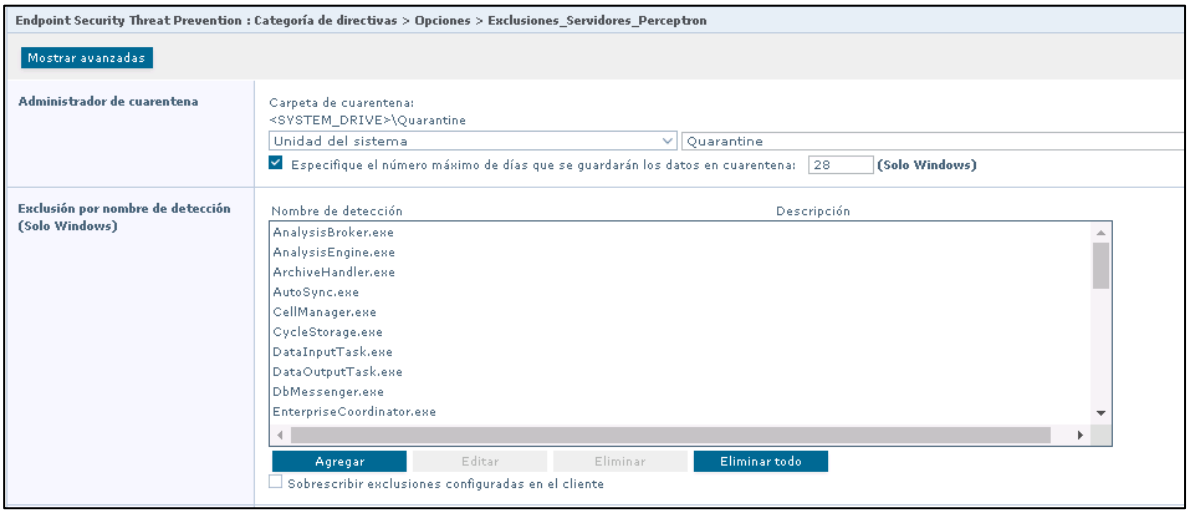



Figura 68: Ubicación y días de almacenamiento para los archivos en cuarentena para los servidores de Perceptron.

En la siguiente opción se configuraron las categorías de los programas potencialmente no deseados y el análisis proactivo de datos. En la figura 69 se muestra la detección de programas potencialmente no deseado y el análisis proactivo de datos para los servidores de Perceptron.

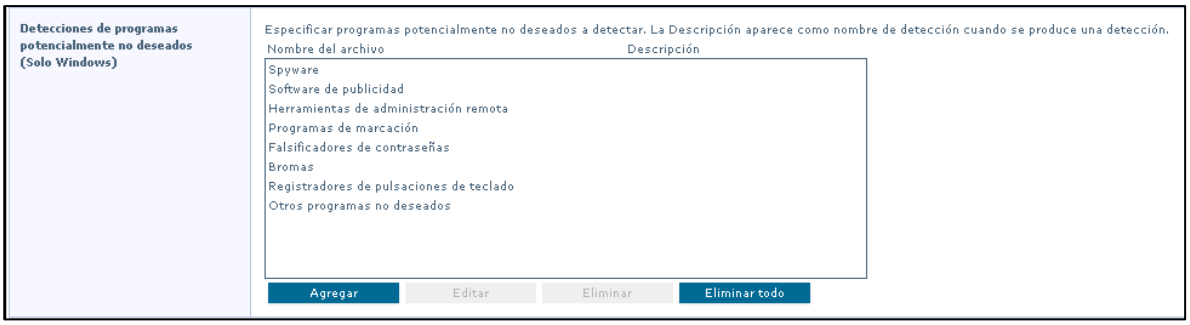



Figura 69: Ubicación y días de almacenamiento para los archivos en cuarentena para los servidores de Perceptron.

## Protección de acceso

Proteja los puntos de acceso de su sistema de acuerdo con las reglas configuradas. La protección de acceso compara una acción solicitada con una lista de reglas configuradas y actúa según la regla.

En la categoría de protección de acceso vamos a observar las exclusiones que se aplicaron y las que se aplicara, así como las reglas que se aplicaron y validar si las reglas se encuentran para bloquear, informar o ambas.

A continuación, mostramos las configuraciones que se tienen en la directiva de VWPuebla para la categoría de protección de acceso.

En la opción de protección de acceso se indicó que la política va a estar habilitada y se agregaron las exclusiones correspondientes de aplicaciones utilizadas por los usuarios finales. En la figura 70 se observan las configuraciones aplicadas.

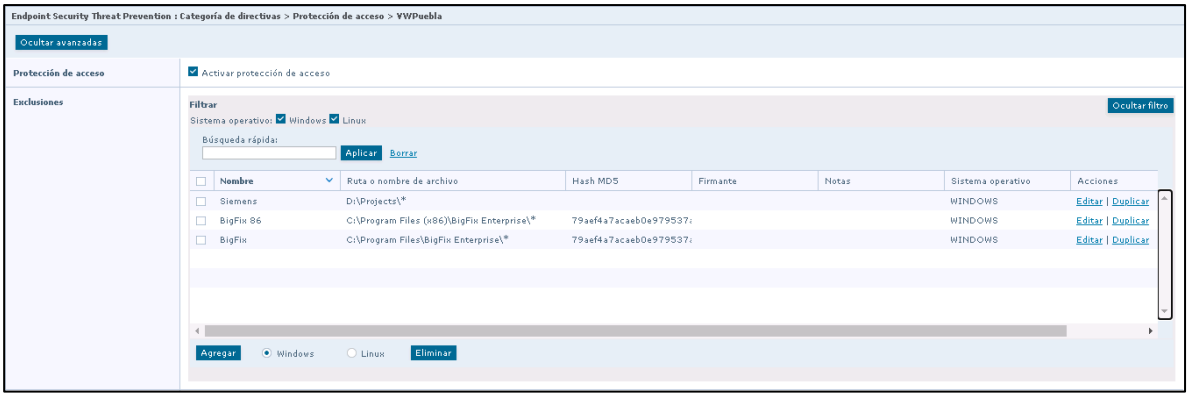



Figura 70: Protección de acceso habilitado y exclusiones aplicadas para protección de acceso.

En la siguiente opción, se agregaron 3 reglas para el bloqueo relacionado con Ransomware, y se validaron las políticas que vienen definidas por McAfee. En la figura 71 se observan las reglas aplicadas.

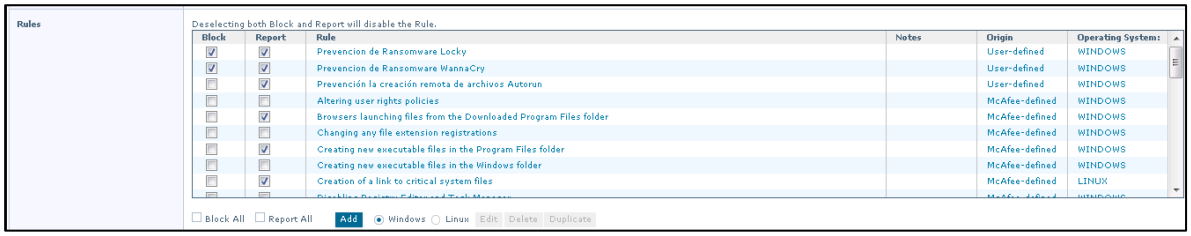



Figura 71: Reglas aplicadas para protección de acceso.

A continuación, mostramos las configuraciones que se tienen en la directiva de Exclusiones_Servidores_Perceptron para la categoría de Protección de acceso. Para esta categoría se realizó una directiva para servidores de Perceptron.

En la opción de protección de acceso se indicó que la política va a estar habilitada y se agregaron las exclusiones correspondientes de aplicaciones utilizadas para los servidores de Perceptron. En la figura 72 se observan las configuraciones aplicadas.

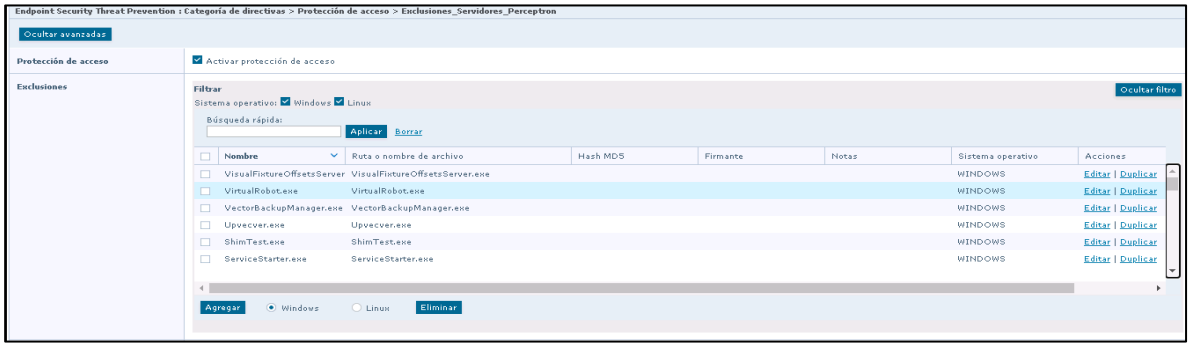



Figura 72: Protección de acceso habilitado y exclusiones aplicadas para protección de acceso.

En la siguiente opción, se agregaron 3 reglas para el bloqueo relacionado con Ransomware y se validaron las políticas que vienen definidas por McAfee. En la figura 73 se observan las reglas aplicadas.


Figura 71: Reglas aplicadas para protección de acceso.

A continuación, mostramos las configuraciones que se tienen en la directiva de VWPuebla_ENS_Down. Es importante mencionar que esta directiva es creada con la finalidad de deshabilitar la protección en los equipos o servidores.

La casilla de habilitar protección de acceso no se encuentra seleccionada, por lo que esta directiva se encuentra deshabilitada. En la figura 72 se observa la directiva deshabilitada.

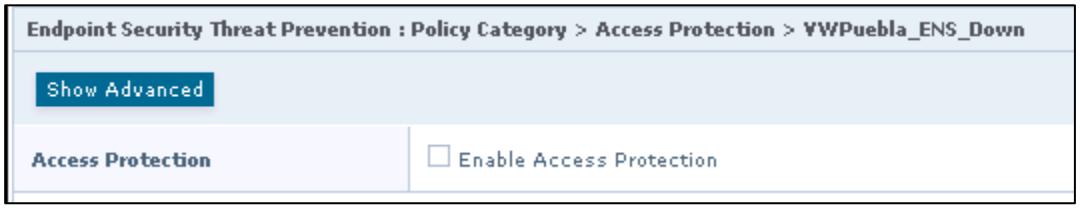



Figura 72: La protección de acceso se encuentra deshabilitada

**Prevención de exploit.**

Prevención de exploit Impide el desbordamiento de búfer, el uso ilegal de API y los exploits de red. Se crean reglas expertas para evitar el desbordamiento de búfer y el uso ilegal de API de exploits y proteger los archivos, claves de Registro, valores de Registro, procesos y servicios.

En la categoría de prevención de exploit vamos a observar los diferentes tipos de bloqueos que se pueden aplicar, como la prevención de exploit, escalación de privilegios, la ejecución de datos y la intrusión de red, también se pueden aplicar exclusiones sobre procesos o registros, firmas de seguridad y reglas de protección de aplicaciones.

A continuación, mostramos las configuraciones que se tienen en la directiva de VWPuebla para la categoría de prevención de exploit.

En la primera parte se habilito la prevención de exploit, de momento no fue requerido habilitar la escalación de privilegios, le ejecución de datos y la intrusión de red. En la figura 73 se observa la directiva habilitada.

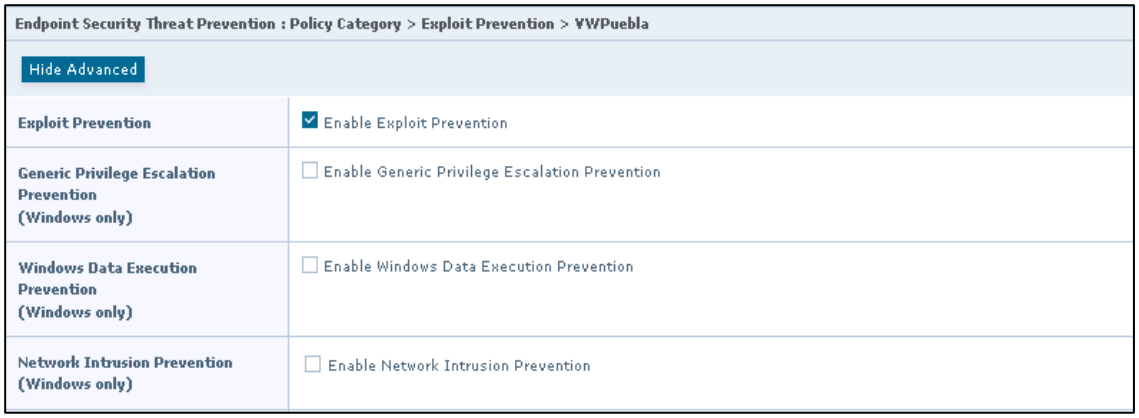



Figura 73: Directiva de prevención de exploit habilitada.

En la siguiente opción vamos a validar vamos a validar las firmas de seguridad que se tienen definidas por McAfee, de momento las reglas quedaron configuradas conforme a las recomendaciones de McAfee. En la figura 74 se observan las firmas definidas para prevención de exploit.

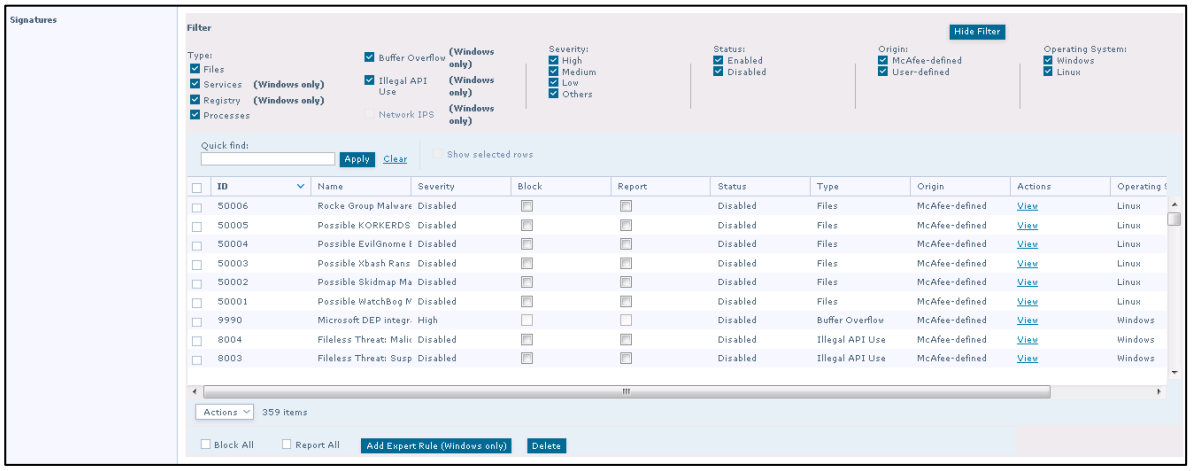



Figura 74: Firmas de seguridad asignadas para prevención de exploit.

Por último, vamos a validar las reglas de protección para aplicaciones, de momento las reglas quedaron configuradas conforme a las recomendaciones de McAfee. En la figura 75 se observan las reglas de protección de aplicaciones.

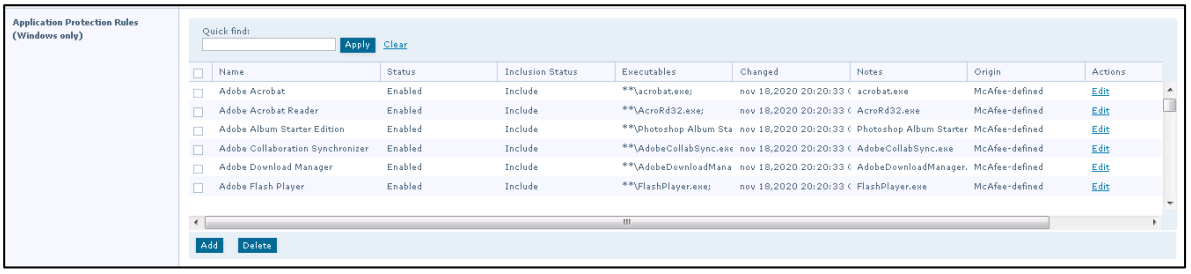



Figura 75: Reglas de protección de aplicaciones para prevención de exploit.

A continuación, mostramos las configuraciones que se tienen en la directiva de Exclusiones_Servidores_Perceptronpara la categoría de prevención de exploit.

En la primera parte se habilito la prevención de exploit, de momento no fue requerido habilitar la escalación de privilegios, le ejecución de datos y la intrusión de red, de igual manera se observan los servicios y procesos que fueron excluidos para esta directiva. En la figura 76 se observa la directiva habilitada y las exclusiones aplicadas.

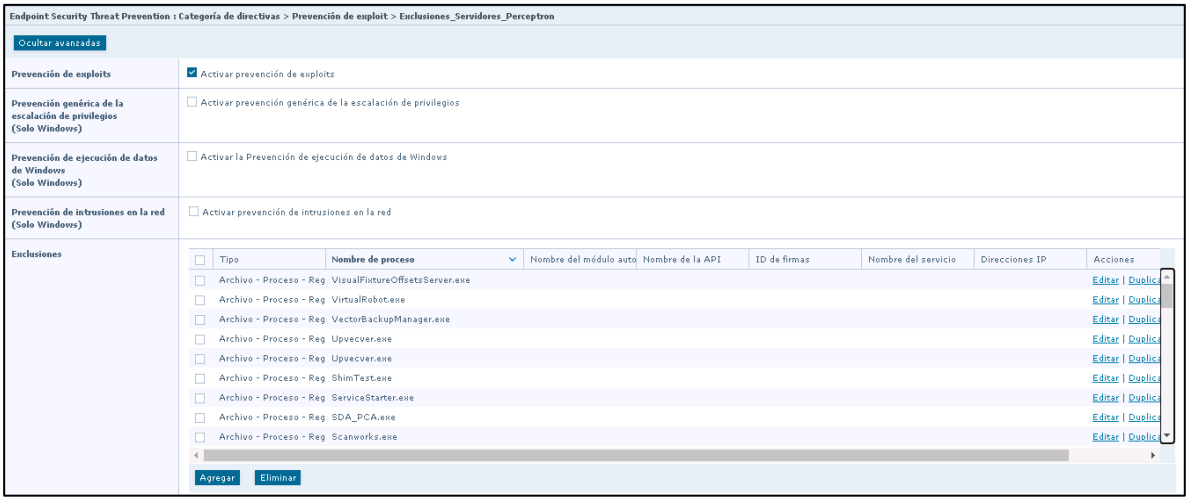



Figura 76: Directiva de prevención de exploit habilitada y exclusiones agregadas.

En la siguiente opción vamos a validar vamos a validar las firmas de seguridad que se tienen definidas por McAfee, de momento las reglas quedaron configuradas conforme a las recomendaciones de McAfee. En la figura 77 se observan las firmas definidas para prevención de exploit.

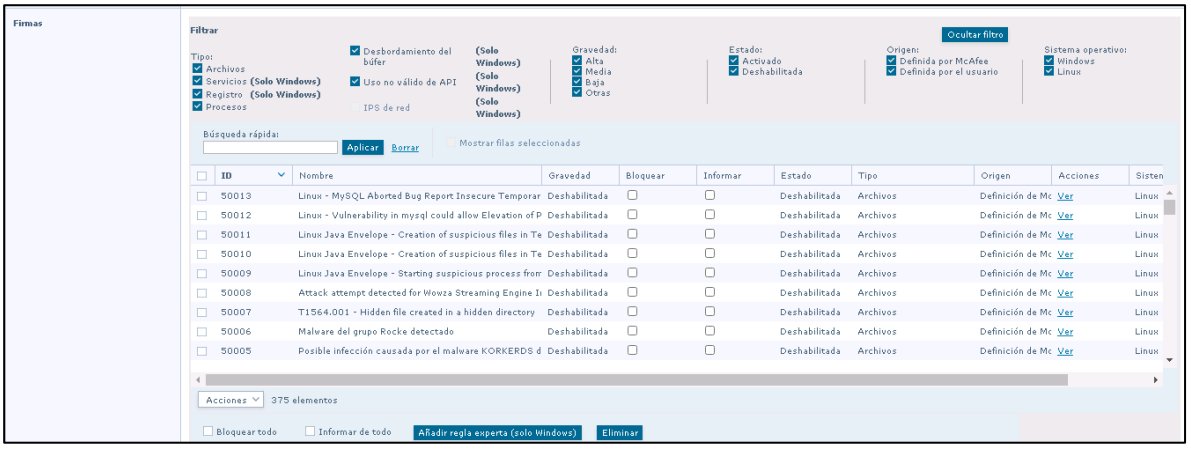



Figura 77: Firmas de seguridad asignadas para prevención de exploit.

Por último, vamos a validar las reglas de protección para aplicaciones, de momento las reglas quedaron configuradas conforme a las recomendaciones de McAfee. En la figura 78 se observan las reglas de protección de aplicaciones.

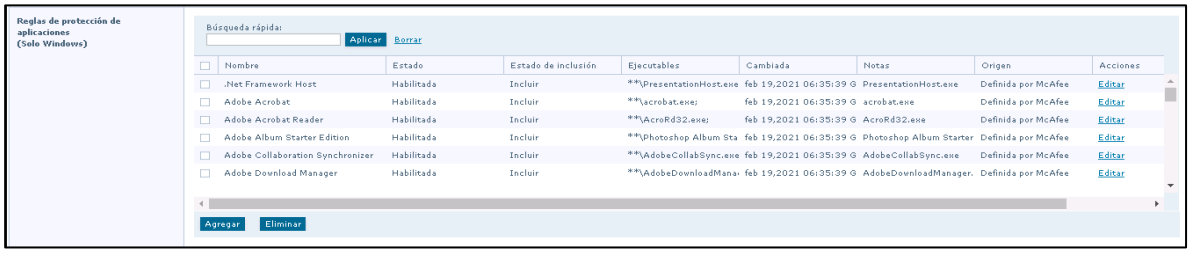



Figura 78: Reglas de protección de aplicaciones para prevención de exploit.

A continuación, mostramos las configuraciones que se tienen en la directiva de VWPuebla_ENS_Down. Es importante mencionar que esta directiva es creada con la finalidad de deshabilitar la protección en los equipos o servidores.

La casilla de habilitar prevención de exploit no se encuentra seleccionada, por lo que esta directiva se encuentra deshabilitada. En la figura 79 se observa la directiva deshabilitada.


Figura 79: La prevención de exploit se encuentra deshabilitada.

## Configuración de directivas para McAfee Endpoint Security Firewall

En el siguiente apartado vamos a mostrar las directivas que se tienen configuradas para el producto de McAfee Endpoint Security Firewall, para este producto vamos a observa las categorías de Options (User-Based Policy) y Rules (User-Based Policy).

Es importante mencionar que por indicaciones del cliente se decidió dejar estas directivas deshabilitadas, por lo que estaremos mostrando la directiva deshabilitada.

A continuación, mostramos las configuraciones que se tienen en la directiva de VWPuebla para la categoría Options (User-Based Policy) y Rules (User-Based Policy).

### Options (User-Based Policy)

En esta categoría podemos habilitar o deshabilitar el módulo Firewall, configurar las opciones de protección y definir redes y ejecutables de confianza que se van a utilizar en reglas y grupos. La casilla de habilitar Firewall no se encuentra seleccionada, por lo que esta directiva se encuentra deshabilitada En la figura 80 se observa la directiva de Firewall deshabilitada.

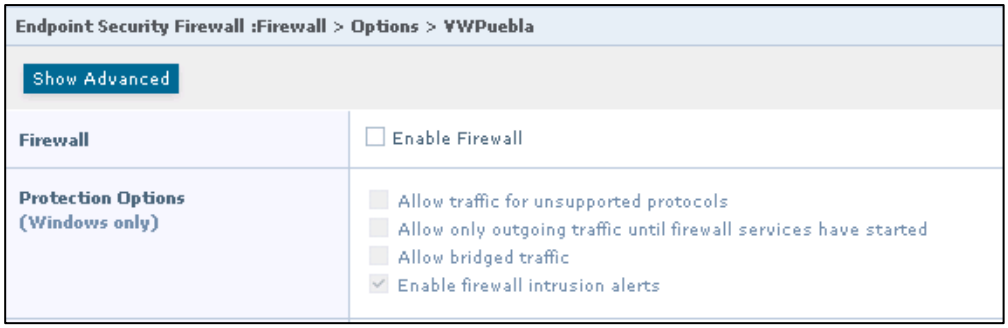



Figura 80: La directiva de opciones de encuentra deshabilitada para Firewall.

### Rules (User-Based Policy)

En esta categoría podemos agregar y eliminar reglas y grupos en el grupo Agregado por usuario. Firewall mueve de manera automática a este grupo las reglas que se acaban de agregar. Para restablecer la configuración predeterminadas de las reglas, solo basta con seleccionar Restablecer a predeterminado. En la figura 81 se observan las reglas que se tienen configurada en la directiva de Firewall.

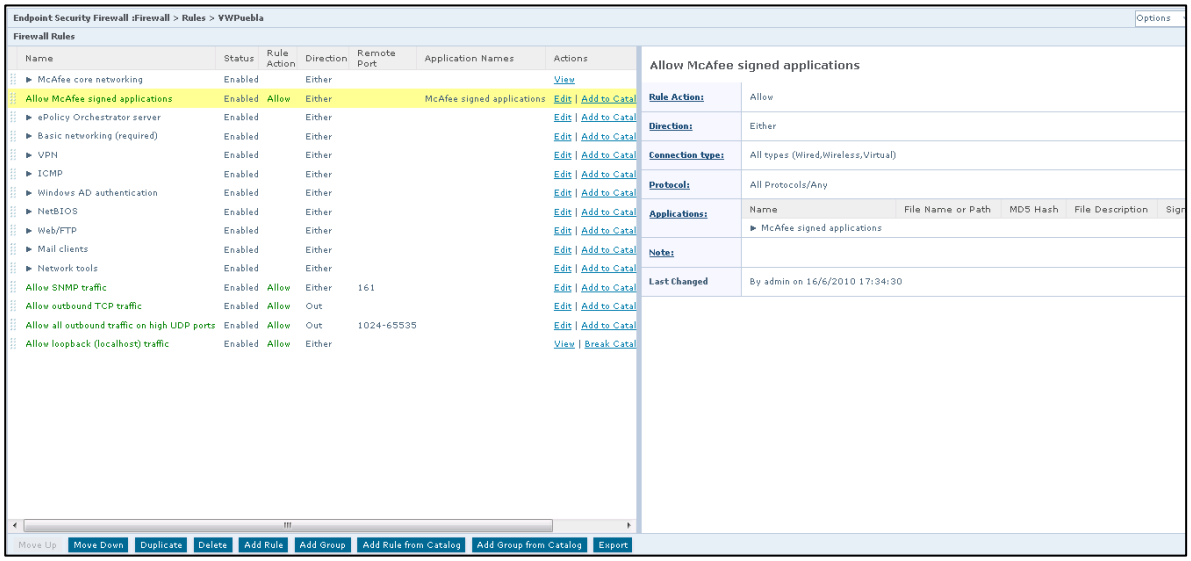



Figura 81: Reglas configuradas para la directiva Firewall VW_Puebla.

## McAfee Data Loss Prevention - DLP

McAfee Data Loss Prevention es un paquete de productos que protege frente a la fuga de datos mediante su identificación y puesta a salvo en la red y fuera de ella. Las directivas de **McAfee DLP** ayudan a comprender los tipos de datos en su red, cómo se accede a ellos, cómo se transmiten y si contienen información confidencial

McAfee Device Control es el producto con el que trabajamos, el cual se encarga de controlar el contenido de carácter confidencial copiado en dispositivos extraíbles. **McAfee DLP** Endpoint inspecciona también las acciones de los usuarios de empresa en contenido de carácter confidencial al enviar por correo electrónico, mediante las aplicaciones de nube y al registrar en sitios web o recursos compartidos de red.

### Configuración inicial de Data Loss Prevention - DLP

Antes de iniciar a configurar directivas de DLP es necesario ingresar el licenciamiento para que se habilite el módulo de Device Control, la licencia se puede obtener ingresando desde la consola al menú de Administrador de Software o en el sitio de descargar de McAfee, solo se requiere el Grant Number (Numero de concesión y el correo registrado. De igual

manera vamos a configurar el recurso compartido para almacenar la evidencia. En la figura 82 se observan el licenciamiento agregado y el recurso compartido configurado.

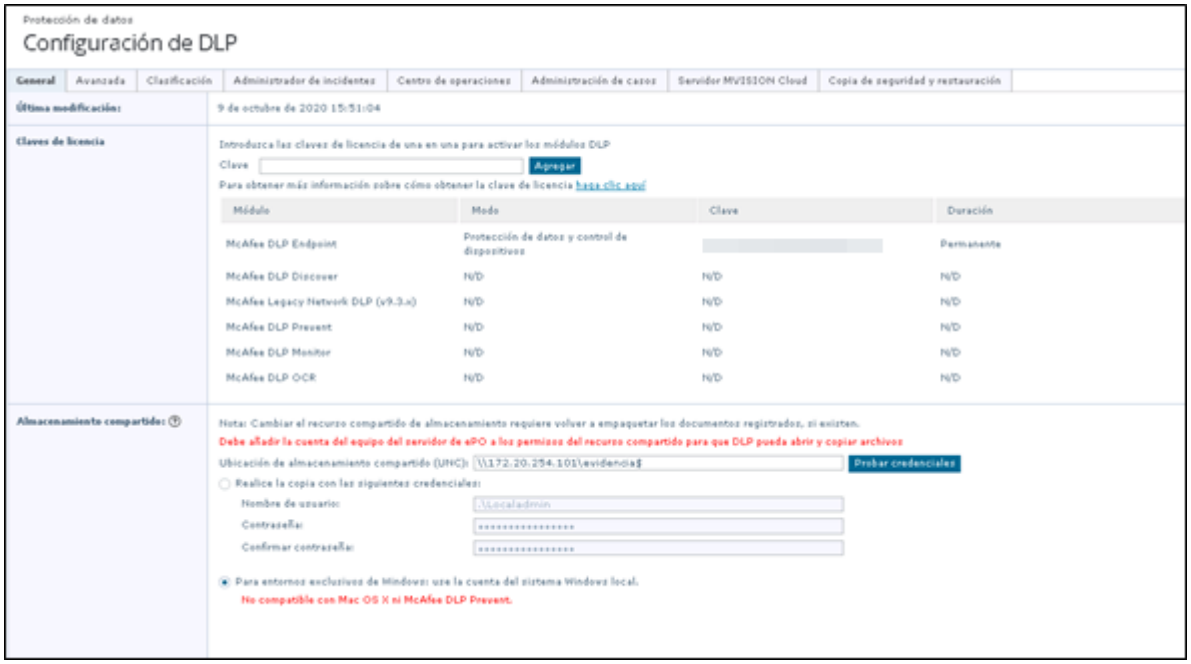



Figura 82: Licenciamiento de DLP Endpoint y recurso compartido para almacenar evidencia.

**Configuración de directivas para McAfee Data Loss Prevention - DLP**

A continuación, vamos a mostrar las directivas que se crearon para McAfee DLP Endpoint, es importante mencionar que este módulo solo está diseñado para el bloqueo de dispositivos de almacenamiento externo. Es importante mencionar que, por solicitud del cliente, se realizaron directivas por nave, sin embargo, solo se trabajó en la directiva de DLP de bloqueo general la cual se etiqueto como DIR-BLOQ_USB_GRAL.

Antes de iniciar con la creación de directivas, es necesario crear las plantillas, las cuales son requeridas al momento de crear las directivas.

La primero que tenemos que realizar en la Definición, aquí indicamos el tipo de dispositivos que queremos bloquear, en este caso seleccionamos IDE/SATA, SD y USB. En la figura 83 se observan los tipos de dispositivos que queremos bloquear.

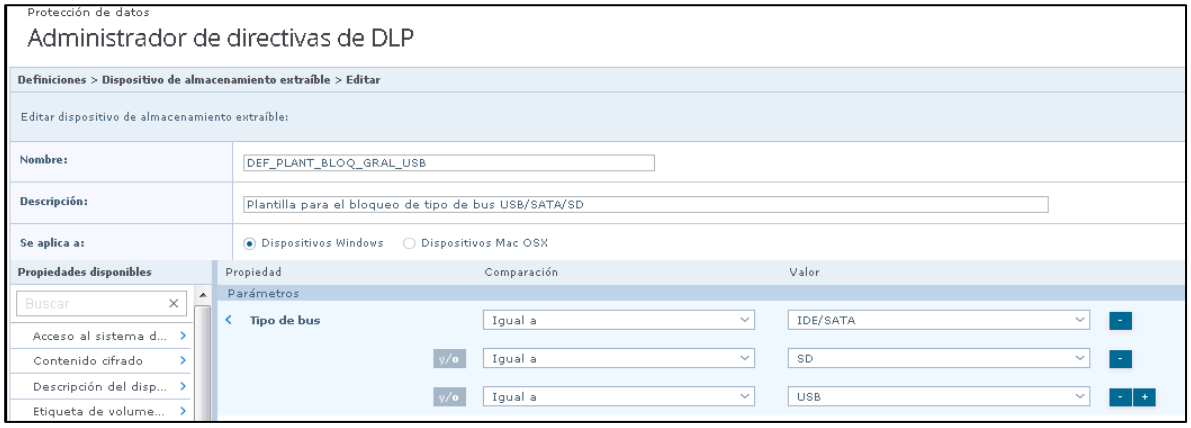



Figura 83: Tipos de dispositivos externos que se van a bloquear.

También vamos a crear una Definición para la exclusión de dispositivos externos, aquí se definió excluir los dispositivos externos por medio del número de serie, por lo que se obtuvo el número de serie de los dispositivos externos que no tenían que ser bloqueados y se agrega su plantilla de exclusión. En la figura 84 se observan los numero de serie de los dispositivos externos que se excluyeron.

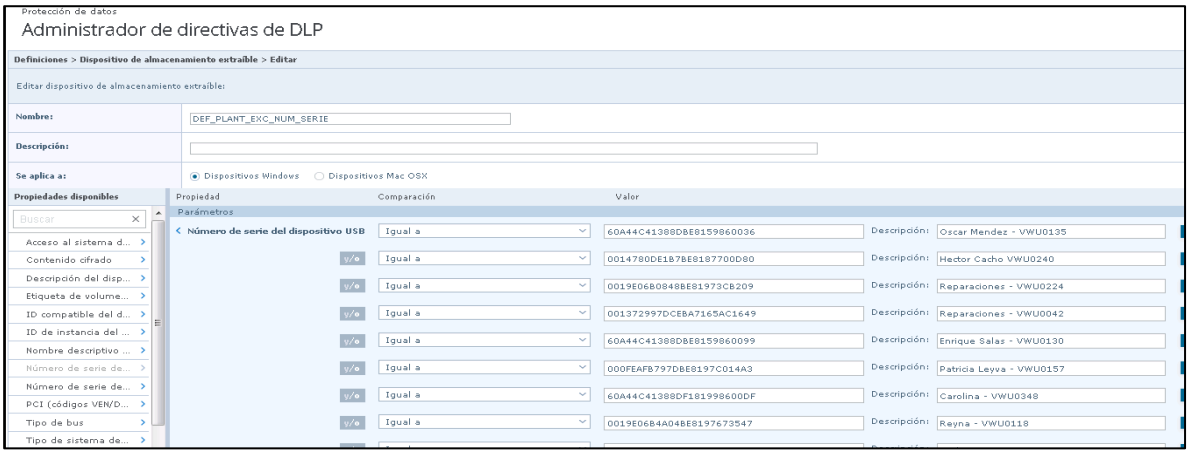



Figura 84: Número de serie de los dispositivos externos que se excluyeron.

Después de crear nuestras plantillas para bloqueos y exclusiones, procedemos a crear nuestras reglas, esto para iniciar con el bloqueo de dispositivos externos conforme a la configuración aplicada. En la primera parte de la configuración de esta regla vamos a observar el nombre asignado “REG_BLOQ_GRAL_USB”, después una descripción de la regla, el estado, gravedad y el tipo de sistema operativo donde se implementó.

A continuación, se observan 3 pestañas, la primera pestaña es Condición donde indicamos los usuarios que aplicaran para esta regla, después el tipo de dispositivos que deseamos bloquear, en esta parte vamos a seleccionar las plantillas previamente creadas. En la figura 85 se muestra la configuración aplicada para esta regla.

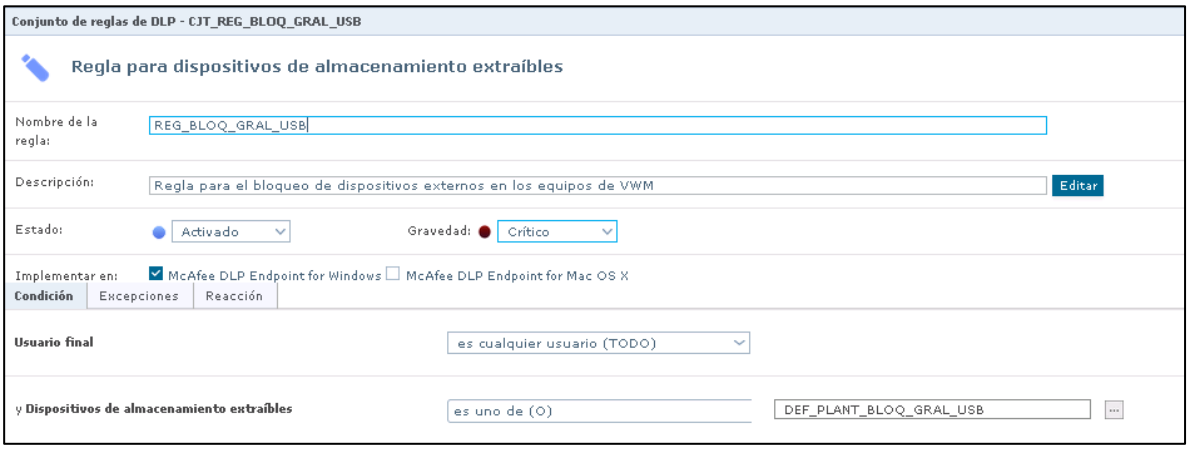



Figura 85: Configuración aplicada en la primera parte de la regla de REG_BLOQ_GRAL_USB.

En la pestaña de Excepciones de la misma regla, vamos a indicar los dispositivos que excluimos, en este caso seleccionamos la opción de Plantillas de dispositivos excluidas, activamos las exclusiones y seleccionamos las plantillas que previamente creamos para excluir dispositivos. En la figura 86 observamos las exclusiones agregadas.

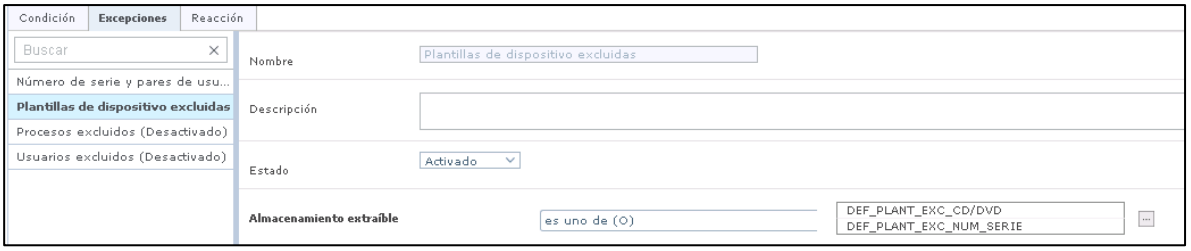



Figura 86: Exclusiones aplicadas para la regla de REG_BLOQ_GRAL_USB.

En la pestaña de reacción se indicó la acción a tomar, es esta regla será bloquear, para la notificación del usuario se utiliza una plantilla previamente realizará e indicamos que se cierre la notificación en 10 segundos, seleccionamos la casilla de notificación de incidentes y por último indicamos que aun estando fuera de la red corporativa aplique el bloqueo de dispositivos externos. En la figura 87 se observa las acciones a realizar en la regla configurada.

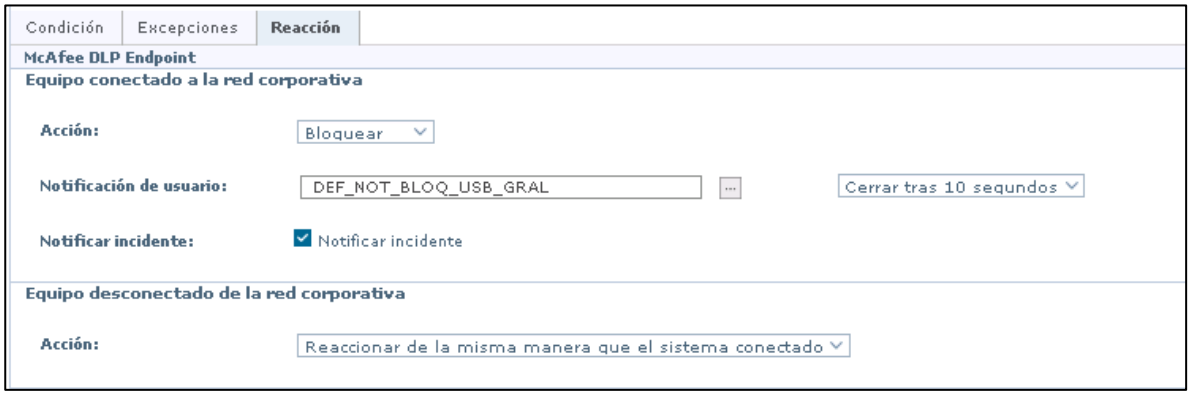



Figura 87: Acciones a realizar en la regla de REG_BLOQ_GRAL_USB.

## Configuración de tarea

Al iniciar McAfee ePO por primera vez, se instalan automáticamente algunas tareas cliente preconfiguradas a fin de ayudarle a gestionar sus productos de McAfee. Esas tareas cliente proporcionan una seguridad básica para la mayoría de los usuarios y se ejecutan de manera predeterminada.

Las tareas cliente están configuradas para ejecutarse en función de distintos criterios. Por ejemplo, algunas tareas cliente se ejecutan:

- **De manera continua:** se trata de tareas cliente que analizan automáticamente programas y archivos en busca de amenazas conforme estas se producen.
- **Cuando se producen eventos configurados:** se trata de tareas cliente que se ejecutan durante el intervalo de comunicación agente-servidor o el intervalo de implementación de directivas.
- **Conforme a la planificación:** se trata de tareas cliente que se ejecutan en el momento configurado en el despliegue o la directiva del producto.

El proceso de configuración de tareas en la consola ePolicy Orchestrator se aplicó para los siguientes productos:

- Endpoint Security Threat Prevention
- McAfee Agent

**Configuración de tareas para McAfee Agent**

Las tareas para McAfee principalmente se encargan de para instalar y actualizar productos de seguridad gestionados en los sistemas gestionados desde el Repositorio principal. Es posible crear y administrar objetos de tarea de despliegue individuales mediante el Catálogo de tareas cliente y, a continuación, asignarlos para que se ejecuten en grupos o en un sistema concreto.

A continuación, mostramos las tareas que fueron creadas al momento de la implementación, estas tareas tienen la finalidad de realizar la instalación de productos como Data Loss Prevention y Endpoint Security, así como las actualizaciones de las firmas de seguridad de AMCore y DAT. En la figura 88 se muestran las tareas creadas.

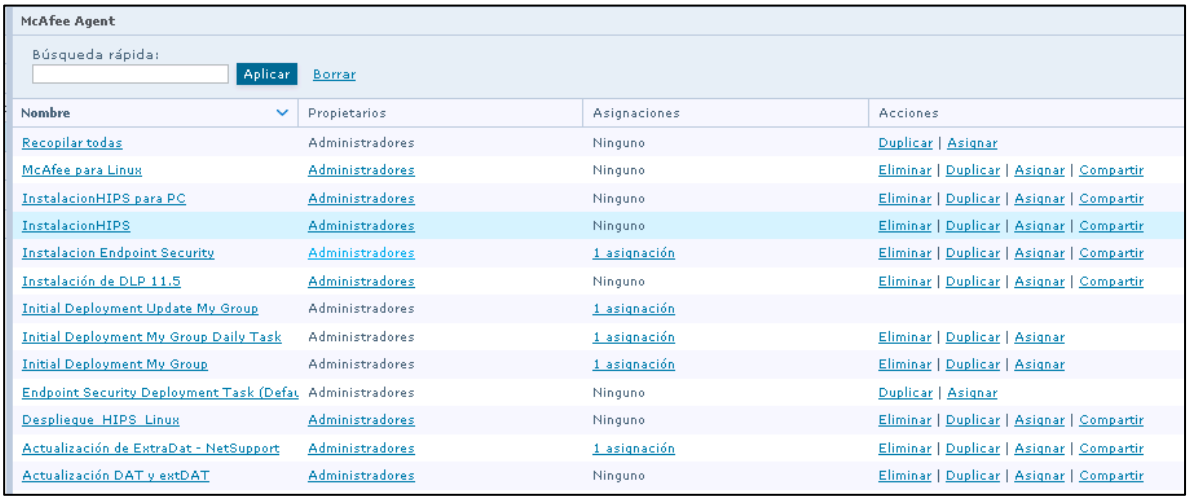



Figura 88: Catalogo de tareas de cliente para despliegue y actualizaciones.

La tarea de despliegue de los productos de Endpoint Security fue creada para realizar la instalación de los productos de seguridad de McAfee, los cuales constan de los productos

de Threat Prevention, Platform y Firewall. En la figura 89 se observan los productos a instalar, la acción a realizar y las plataformas a trabajar.

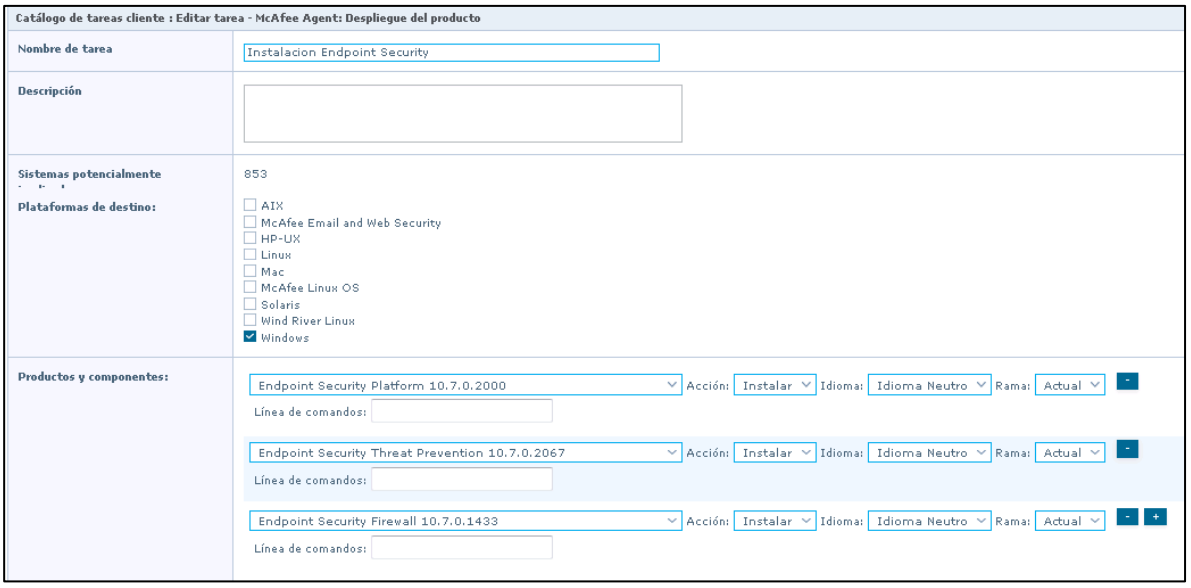



Figura 89: Tarea para el despliegue de Endpoint Security.

La tarea de despliegue de los productos de Data Loss Prevention fue creada para realizar la instalación del producto de prevención de fuga de información de McAfee, el cual consta solo del producto de McAfee Data Loss Prevention. En la figura 90 se observa el producto a instalar, la acción a realizar y las plataformas a trabajar.

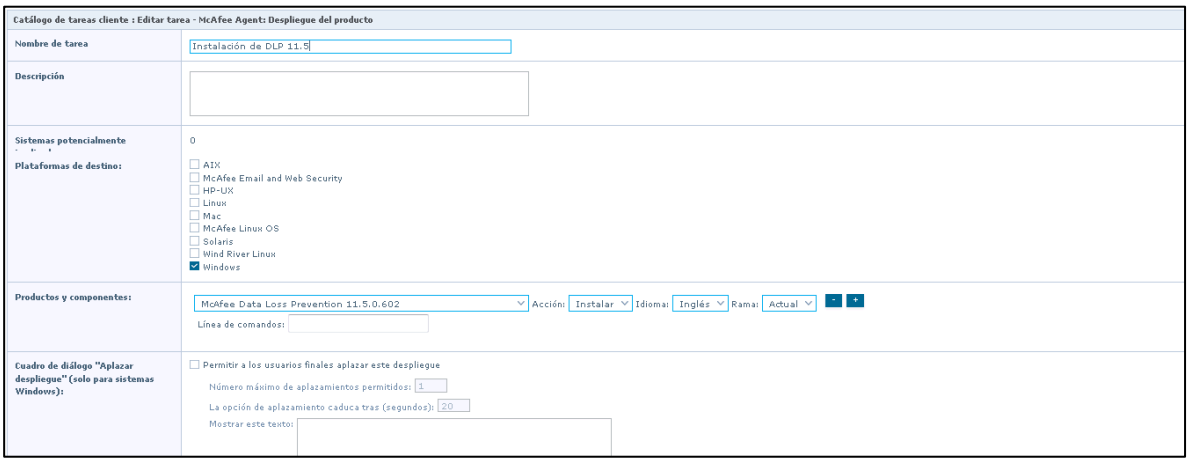



Figura 90: Tarea para el despliegue de Data Loss Prevention.

La tarea de actualización de firmas y motores de seguridad de McAfee fue creada para realizar la actualización de las firmas de seguridad de AMCore y DAT, así como los motores

de Engine y Exploit Prevention Content. En la figura 91 se observan las firmas y motores de seguridad a actualizar.

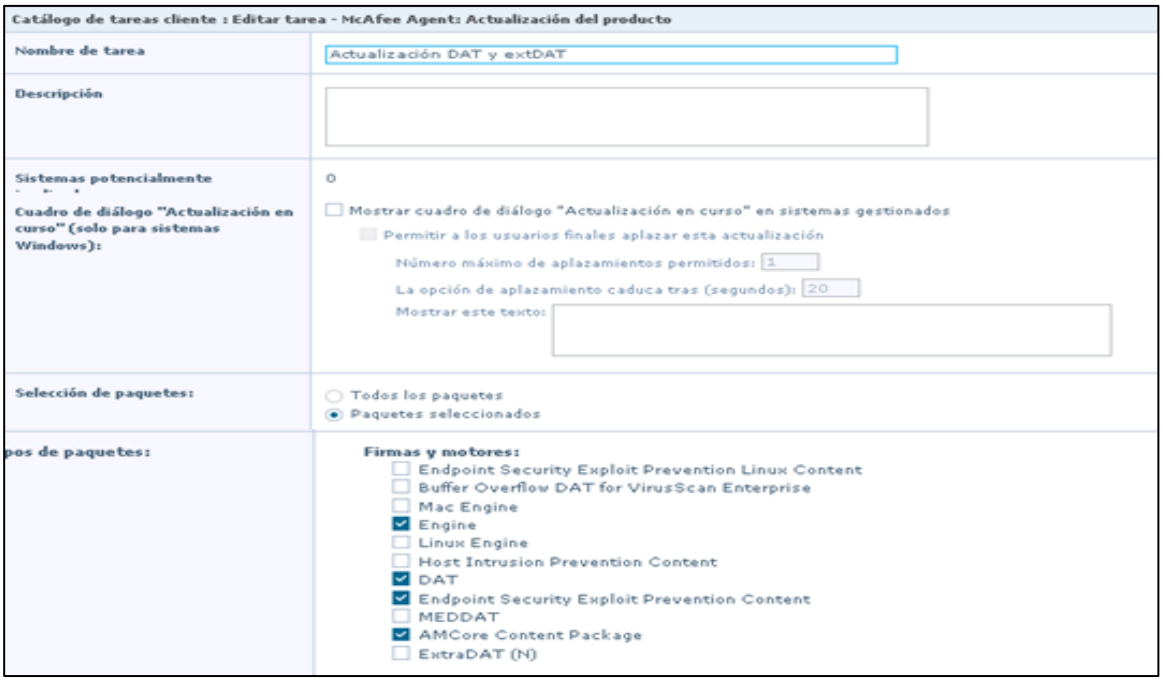



Figura 91: Firmas y motores de seguridad a actualizar.

### Configuración de tareas para Endpoint Security

Para las tareas para Endpoint Security se encargan principalmente de realizar los análisis personalizados bajo demanda, pausar o cancelar un análisis bajo demanda y restaurar desde cuarentena. En la figura 92 se observan los tipos de tareas que se pueden crear para Endpoint Security.

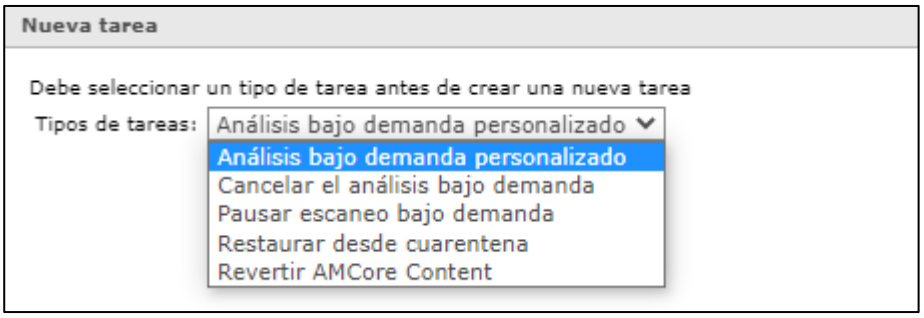



Figura 92: Tipos de tareas que se pueden crear para Endpoint Security

A continuación, mostramos las tareas que se crearon al momento de la implementación para Endpoint Security, dichas tareas están configuradas para indicar que se van a analizar,

las ubicaciones del análisis, los tipos de archivos, si hay que excluir algún análisis y las acciones que se van a realizar al momento de una detección sospechosa.

Para la primera parte de la configuración vamos a indicar el nombre de la tarea, una descripción (opcional), indicamos que se analicen sectores y archivos de almacenamientos, seleccionamos que analice programas no deseados, amenazas desconocidas y macros. En la figura 93 se observa la configuración inicial aplicada.

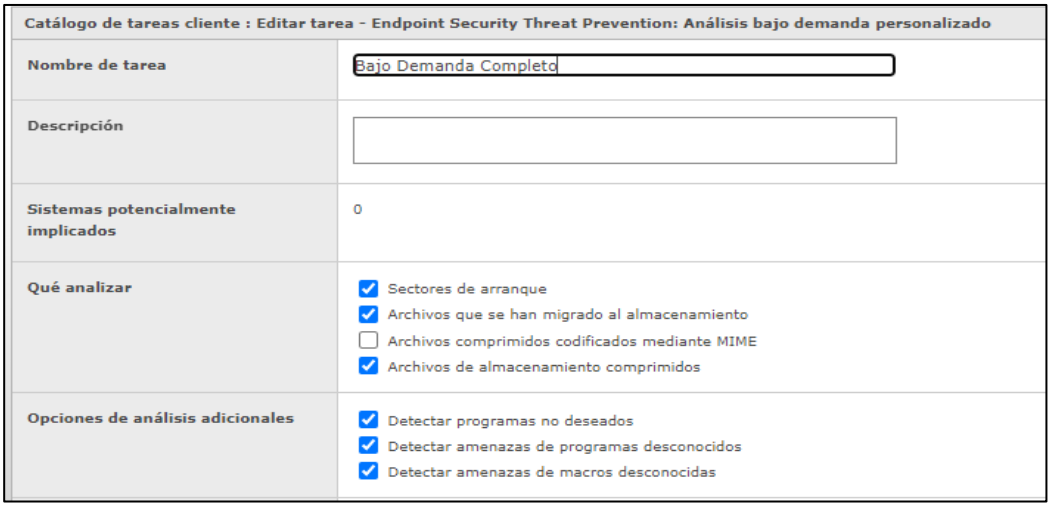



Figura 93: Configuración adicional para el análisis bajo demanda personalizado.

Después vamos a seleccionar las ubicaciones que queremos analizar, también vamos a seleccionar que se analicen subcarpetas. En la figura 94 se observan las ubicaciones a analizar en el análisis bajo demanda personalizado.

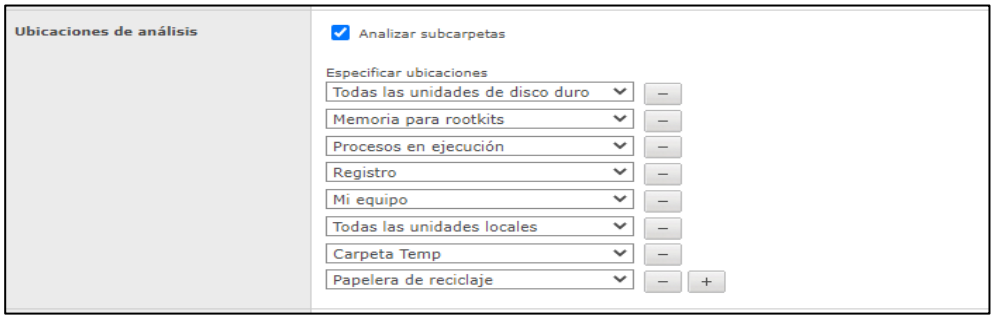



Figura 94: Ubicaciones que se desean analizar en el análisis bajo demanda personalizado.

Y por último vamos a seleccionar los tipos de archivos que queremos analizar, habilitamos el apartado de McAfee GTI, las acciones a realizar al momento de detectar

actividad sospechosa, opciones análisis planificado y las opciones de rendimiento del equipo durante el análisis. En la figura 95 se observan las configuraciones finales para el análisis personalizado.

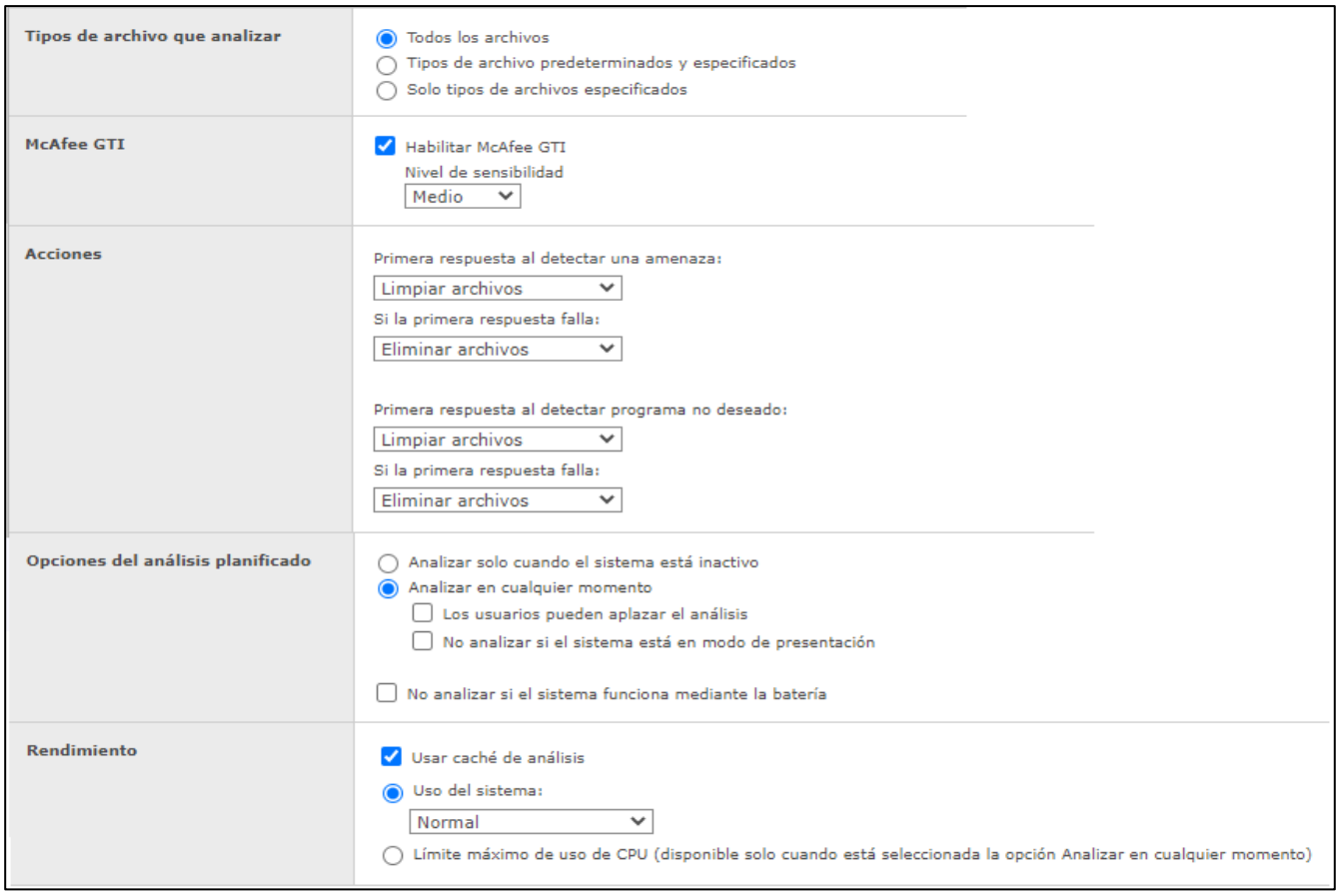



Figura 95: Configuraciones finales para el análisis bajo demanda personalizado.

# VI. SOLUCIÓN DESARROLLADA Y SUS ALCANCES

## Despliegue de la solución

Esta sección describe en forma general el número de equipos registrados a la consola de McAfee ePO al momento de la implementación, la asignación de directivas para los productos de McAfee Agent, Endpoint Security y Data Loss Prevention, así como la asignación de tareas.

A continuación, se muestra una gráfica con el número total de equipos registrados a la consola de administración McAfee ePO, es importante mencionar que estos datos se registraron al momento de realizar la entrega de la implementación. En la figura 96 se muestra la gráfica con el número de equipos asignados por grupos.

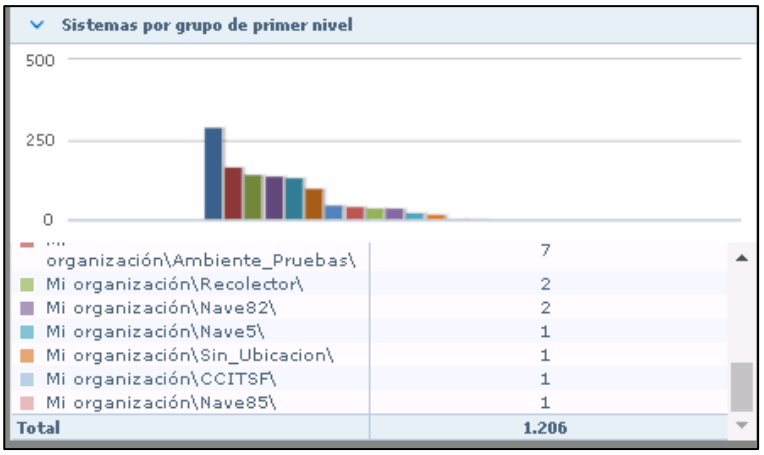



Figura 96: Gráfica con el número de equipos asignados por grupos.

### Asignación de directivas

A continuación, se muestra las directivas asignadas a nivel organización, estas reglas están aplicando para todos los equipos y se estarán asignando políticas puntuales a los grupos de árbol de sistema conforme a las necesidades de la operación. Es importante mencionar que la directiva general que se utiliza para todos los equipos es VWPuebla.

La directiva para el producto de McAfee Agent asignada a nivel organización es VWPuebla. En la figura 97 se muestra la directiva asignada para cada una se las categorías de McAfee Agent.


Figura 97: Directiva asignada para las categorías de McAfee Agent.

La directiva para el producto de Endpoint Security Common asignada a nivel organización es VWPuebla. En la figura 98 se muestra la directiva asignada para la categoría de Opciones.


Figura 98: Directiva asignada para las categorías de Endpoint Security Common.

La directiva para el producto de Endpoint Security Threat Prevention asignada a nivel organización es VWPuebla. En la figura 99 se muestra la directiva asignada para cada una se las categorías de Endpoint Security Threat Prevention.


Figura 99: Directiva asignada para las categorías de Endpoint Security Threat Prevention.

La directiva para el producto de Data Loss Prevention estas asignadas por Default, ya que al momento de la implementación fue solicitado solo agregar la política de bloqueo de dispositivos externos solo a dos equipos, dicha directiva esta identificada como DLP

DIR_BLOQ_USB. En la figura 100 se muestran los equipos que tienen asignada la directiva de DLP DIR_BLOQ_USB.


Figura 100: Equipos que cuentan con la directiva de DLP DIR_BLOQ_USB.

## Asignación de Tareas

A continuación, se muestra las tareas asignadas a nivel organización, solo se crearon dos tareas las cuales tienen como finalidad realizar la instalación de las firmas y motores de seguridad de manera recurrente a los equipos gestionados, así como la instalación de los productos de Endpoint Security en los equipos que se reporten a la consola de administración McAfee ePO.  En la figura 101 se muestran las tareas creadas y asignadas.

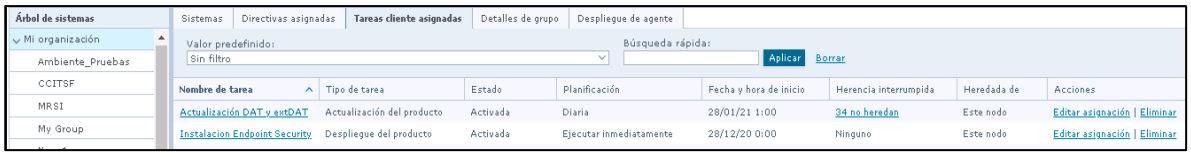



Figura 101: Equipos que cuentan con la directiva de DLP DIR_BLOQ_USB.

La tarea para la instalación de firmas y motores de seguridad consta de la siguiente configuración. En la primera sección vamos a seleccionar el producto, el tipo de tarea y el nombre de la tarea (previamente configurada), después vamos a indicar a partir de que grupo va a heredar la tarea, indicaremos si queremos bloquear la herencia de la tarea, indicamos si se realizara a todos los equipos o equipos con etiquetas y por último vamos a indicar si la tarea va a estar activada o desactivada. En la Figura 102 se observan las configuraciones aplicadas para la tarea de actualización de firmas y motores de seguridad.

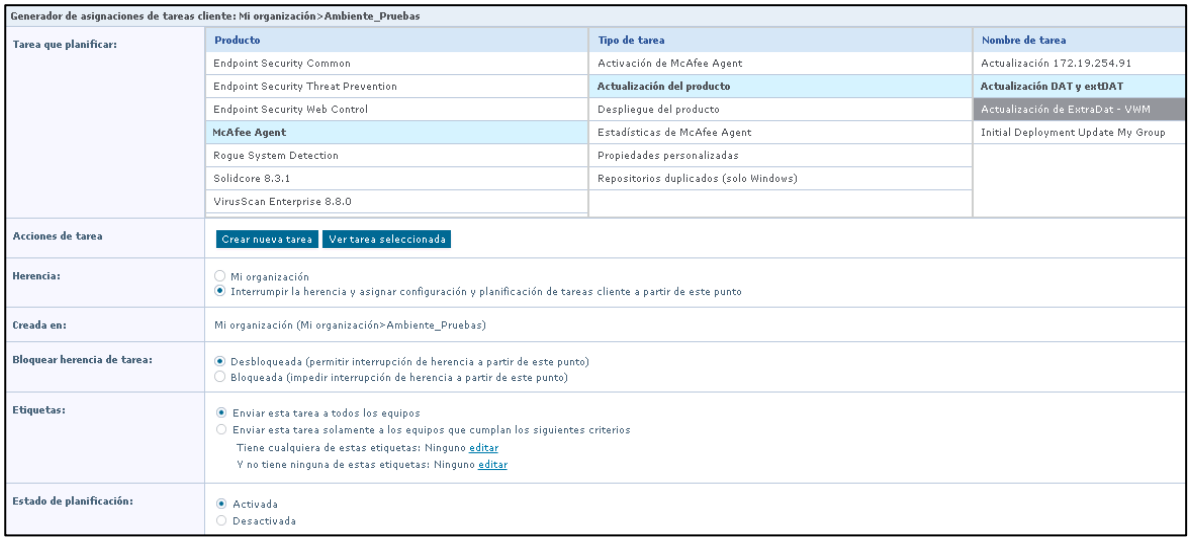



Figura 102: Configuraciones aplicadas para la tarea de actualización de firmas y motores de seguridad.

Después vamos a indicar cuando queremos que se aplique esta tarea, se indicara la fecha de inicio y no tendrá una fecha de finalización, la hora en que se ejecutara la tarea y el periodo en que se estará ejecutando, la zona horaria y las opciones adicionales durante la ejecución. En la figura 103 se observan la planificación aplicada.


Figura 103: Planificación aplicada a la tarea de actualización de firmas y motores de seguridad.

La tarea para la instalación de productos de Endpoint Security consta de las siguientes configuraciones. En la primera sección vamos a seleccionar el producto, el tipo de tarea y el nombre de la tarea (previamente configurada), indicaremos si queremos bloquear la herencia de la tarea, indicamos si se realizara a todos los equipos o equipos con etiquetas, vamos a indicar si la tarea va a estar activada o desactivada y por último la planificación que tomara la

acción de ejecutar de inmediato.  En la figura 104 se observan las configuraciones aplicadas para la tarea de instalación de los productos de Endpoint Security.

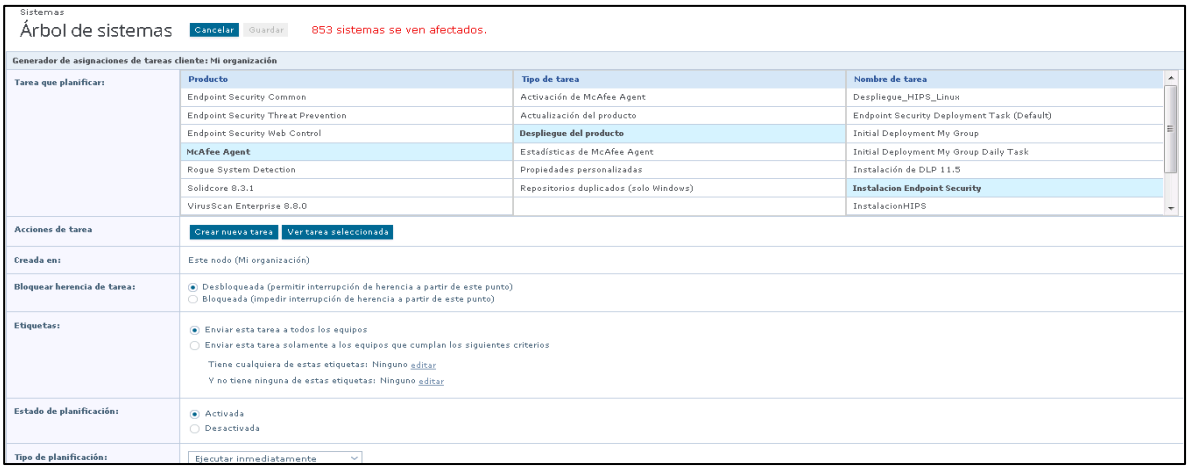



Figura 104: Configuraciones aplicadas para la tarea de instalación de Endpoint Security.

## Consultas

Las consultas permiten recopilar información y ejecutarla de forma gráfica en la consola de administración McAfee ePO. La mayoría de las consultas también se utilizan como monitores de panel, lo que permite la supervisión de los sistemas prácticamente en tiempo real. Los resultados de las consultas se exportan a distintos formatos, los cuales se pueden descargar o enviar como datos adjuntos en un mensaje de correo electrónico.

Durante la implementación, se realizaron diversos reportes, esto con la finalidad de contar con un panorama más amplio sobre la gestión de los equipos administrados. Las consultas generadas están relacionadas al nivel de cumplimiento de los agentes, donde vamos a poder observar equipos duplicados, equipos que no se han comunicado a la consola en el tiempo configurado, las versiones de agentes de McAfee, Endpoint Security y Data Loss Prevention, así como los tipos de eventos de amenaza a reportar, ya sea por equipo, por grupo o por tipo de amenaza.

A continuación, vamos a mostrar la consulta que fue creada para validar que los equipos cuenten con la versión 5.6 de McAfee Agent instalada y que se hayan comunicado en las en las últimas dos semanas, si los equipos no cumplen con estos criterios, se estarán reportando

como Fuera de Cumplimiento. En la figura 105 se muestran los parámetros configurados para esta consulta.

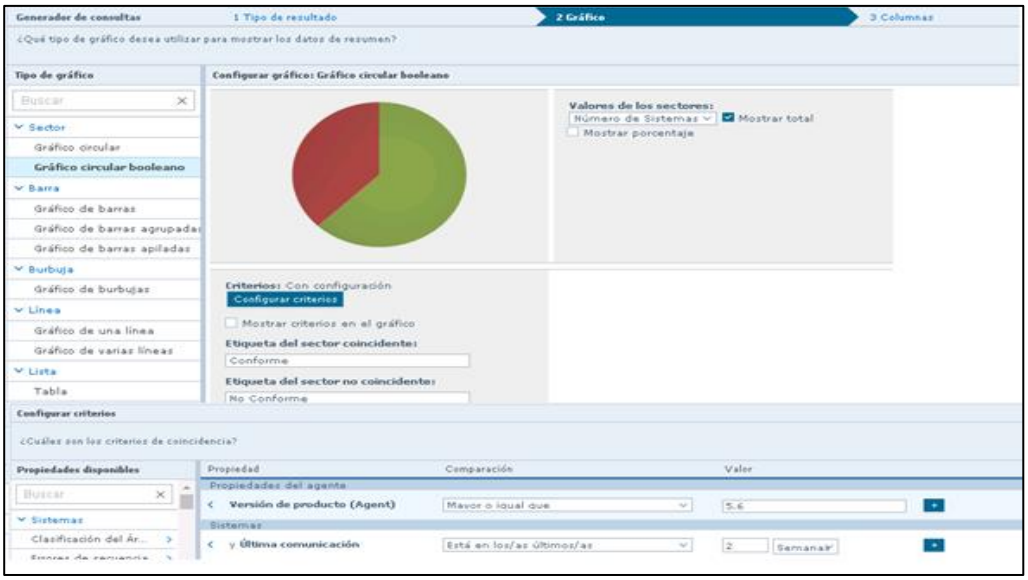



Figura 105: Parámetros aplicados para la consulta de conformidad de McAfee Agent.

La siguiente consulta fue creada para validar que los equipos cuenten con el agente de DLP instalado, donde los únicos criterios que se configuraron es que se tenga instalada la versión 11.5 de DLP, si los equipos no cumplen con estos criterios los equipos se reportaran como Fuera de Cumplimiento. En la figura 106 se observan los criterios configurados para el agente de DLP.

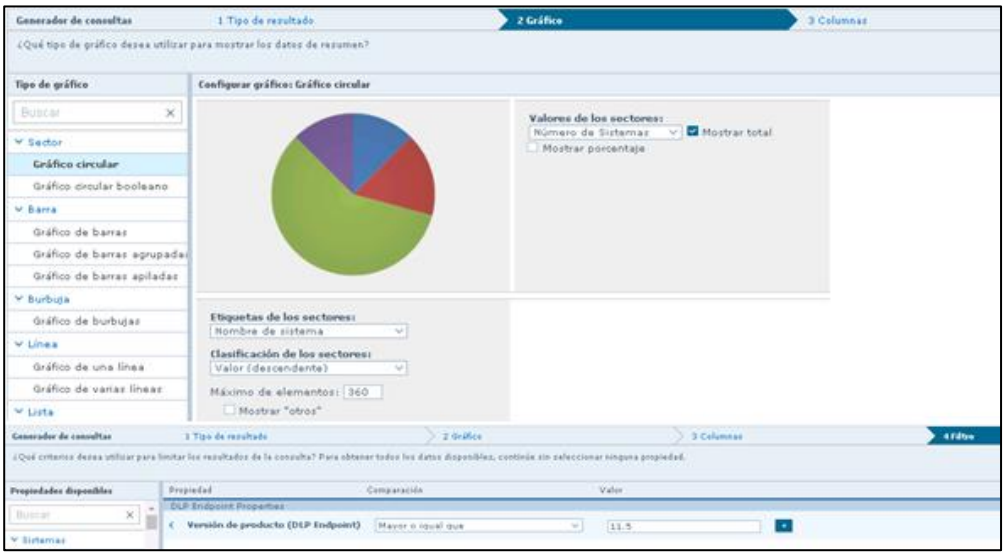



Figura 106: Parámetros aplicados para la consulta de conformidad de Data Loss Prevention.

La siguiente consulta esta generada para validar los equipos que se encuentran duplicados dentro del árbol de sistema de la consola de administración McAfee. Es importante mencionar que esta consulta se cumplirá, solo si los equipos están duplicados por nombre del equipo.  En la figura 107 se observan los parámetros configurados para esta consulta.

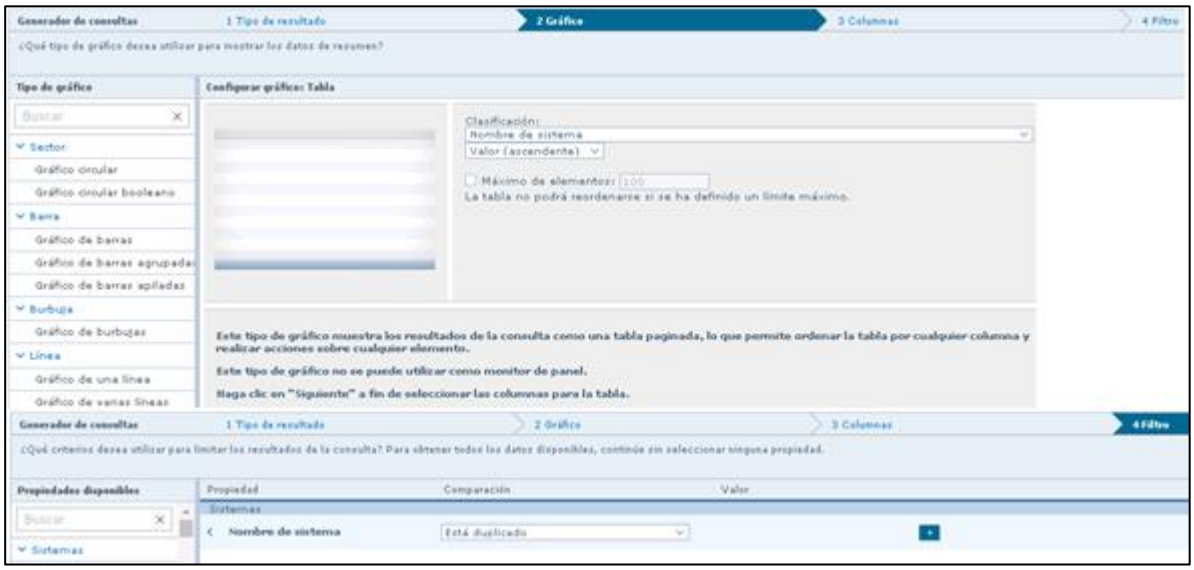



Figura 107: Parámetros aplicados para la consulta de equipos duplicados por nombre del equipo.

La siguiente consulta está configurada con la finalidad de validar que los equipos gestionados cuenten con la versión 10.7 de Endpoint Security, así como los equipos que no cuenten con el producto instalado. En la figura 108 se observan los parámetros configurados para las versiones de Endpoint Security.

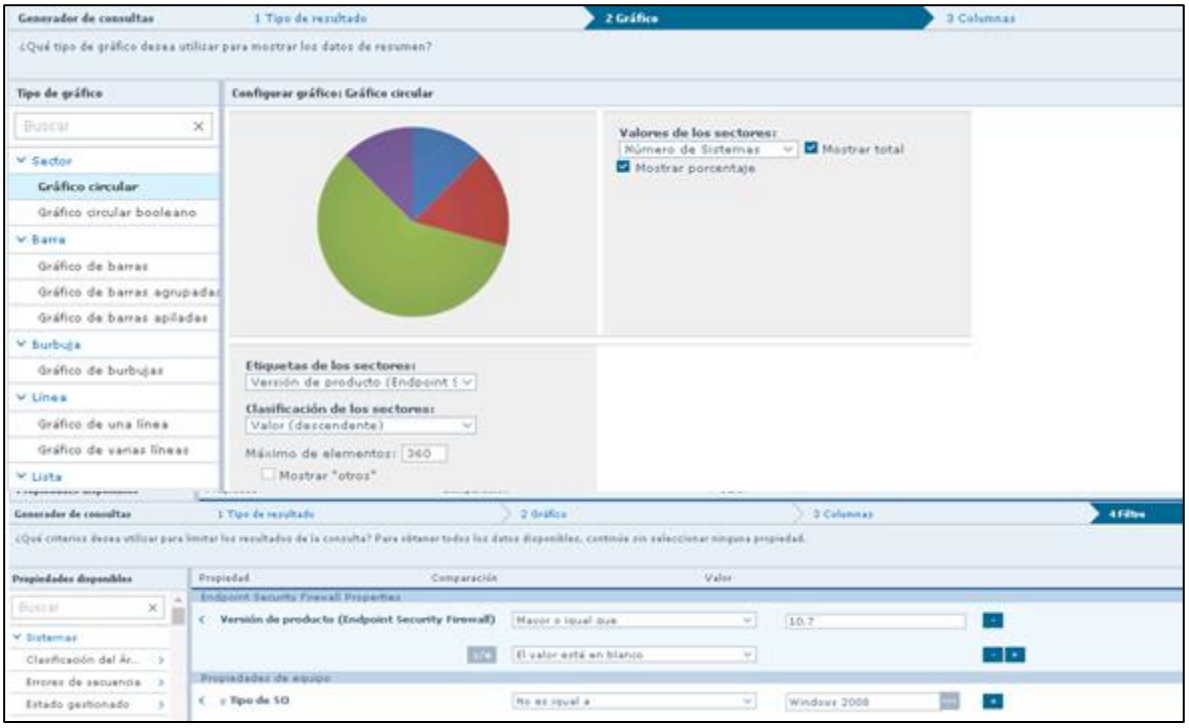



Figura 108: Parámetros aplicados para la consulta de versiones de Endpoint Security instalada.

La siguiente consulta esta generada con la finalidad de validar el Top 10 de los eventos de amenaza detectados en las últimas 24 horas, en la primera parte indicaremos el nombre donde se detectó la amenaza, así como el número de equipos a reportar y el número de amenazas detectadas por detección. En la figura 109 se observa la primera parte de la configuración para la consulta de eventos de amenaza por equipo.

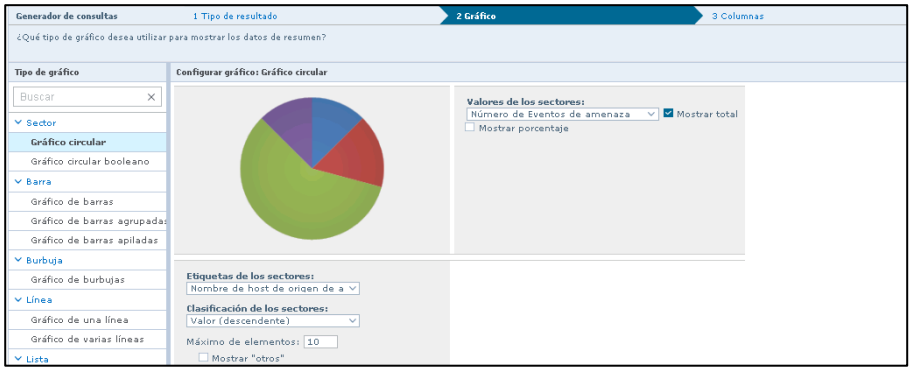



Figura 109: Primera parte de la configuración de la consulta de eventos de amenaza por equipo.

En la segunda parte de la configuración vamos a indicar el producto de la detección, definir el tiempo en que se detectó la amenaza y los tipos de amenaza que se van a estar

reportando. En la figura 110 se muestra la parte final de la configuración de eventos de amenaza por equipo.

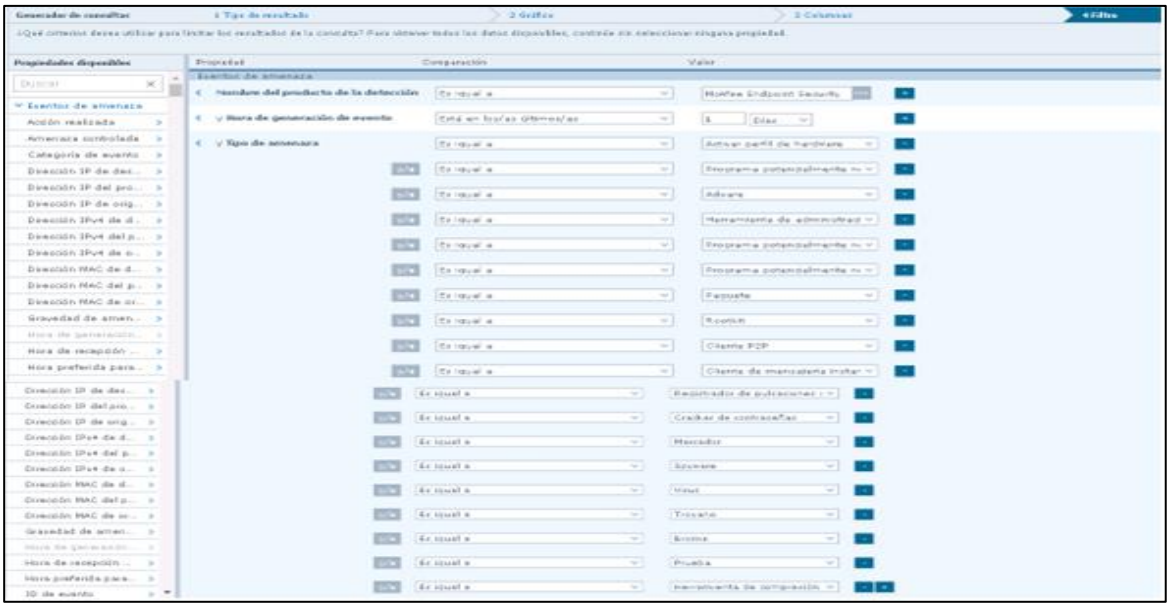


Figura 110: Segunda parte de la configuración de la consulta de eventos de amenaza por equipo.

## Paneles (Dashborad)

Los paneles son consultas agregadas en este apartado que te ayudan a mantener en monitoreo de manera grafica todo el entorno que se tiene gestionado en la consola de administración McAfee ePO, lo que permite la supervisión de los sistemas prácticamente en tiempo real. Al momento de incorporar cualquier paquete de los productos de McAfee se crean paneles predeterminados, los cuales no pueden ser modificados, sin embargo, se pueden crear panales personalizados según las necesidades de la operación o lo que se requiere monitorear en una forma gráfica y fácil de interpretar.

A continuación, mostramos los paneles que fueron creados durante la implementación. Se realizó un panel para el producto de Endpoint Security con la finalidad de validar el nivel de cumplimiento de los productos y los eventos de amenaza detectados, el otro panel se realizó para el producto de Data Loss Prevention donde solo se solicitó validar los equipos que cuentan con el producto instalado.

En el Panel de Endpoint Security la primera grafica indica el cumplimiento de los equipos, los equipos que no se han comunicado a la consola de administración McAfee ePO aparecen con la leyenda de No Conformes, en las siguientes graficas se muestran las versiones instaladas para los productos de Platform, Threat Prevention y Firewall. En la figura 111 se muestra la primera parte del panel para valida el nivel de cumplimiento Endpoint Security.

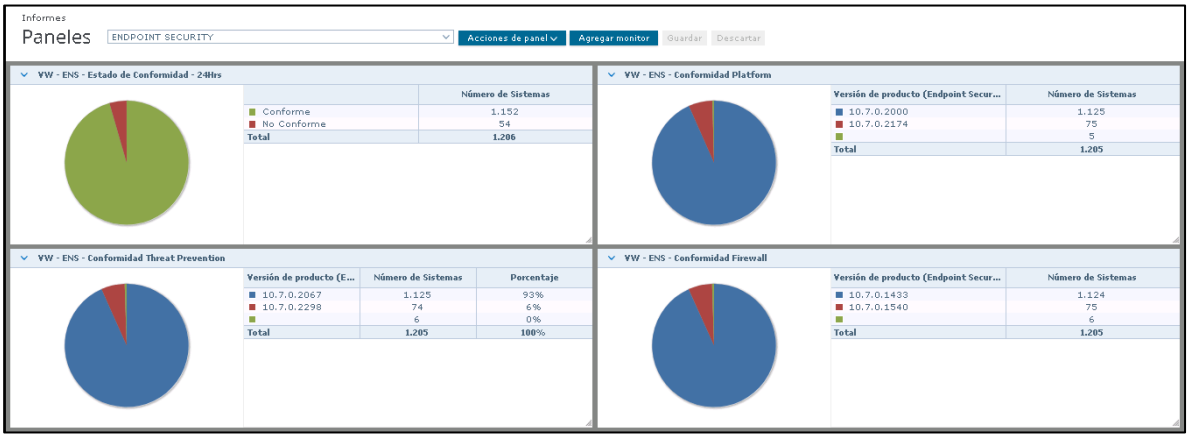



Figura 111: Primera parte del panel para el validar el nivel de cumplimiento de Endpoint Security.

En la segunda parte del panel primero se muestra el Top 10 de las amenazas por equipo en las últimas 24 horas, después se muestran el Top 10 de las amenazas detectadas por tipo de amenaza en las últimas 24 horas y por último el Top 10 de los principales grupos (Naves) que detectan eventos en las últimas 24 horas, al momento de la implementación no se detectaron amenazas, por ello no se muestran eventos. En la figura 112 se muestran las gráficas de los eventos de amenaza detectados en las últimas 24 horas.

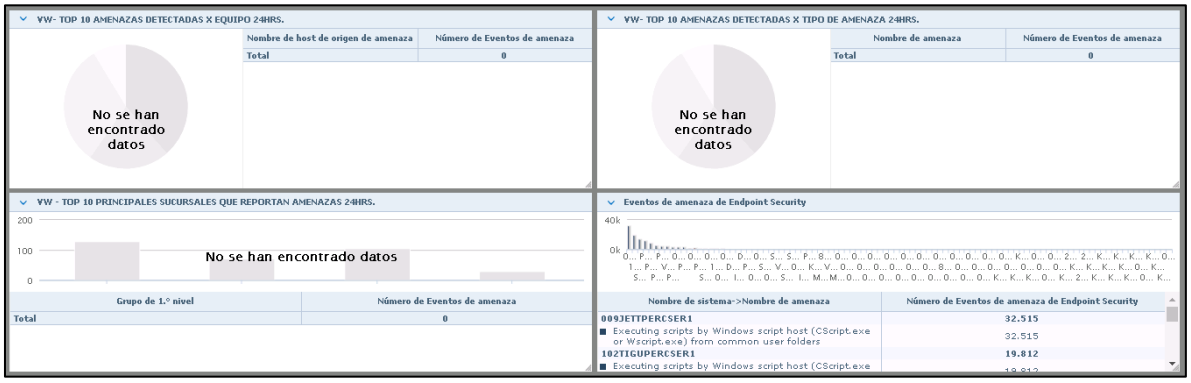



Figura 112: Eventos de amenaza en las últimas de Endpoint Security.

En el panel para el producto de Data Loss Prevention, al momento de la implementación solo se solicitó crear un panel para validar los equipos que contaban con el producto instalado, por lo que solo se observan los 3 equipos que cuentan con el producto de DLP instalado al momento de la implementación. En la Figura 113 se observan el panel para los equipos cuentan con DLP instalado.

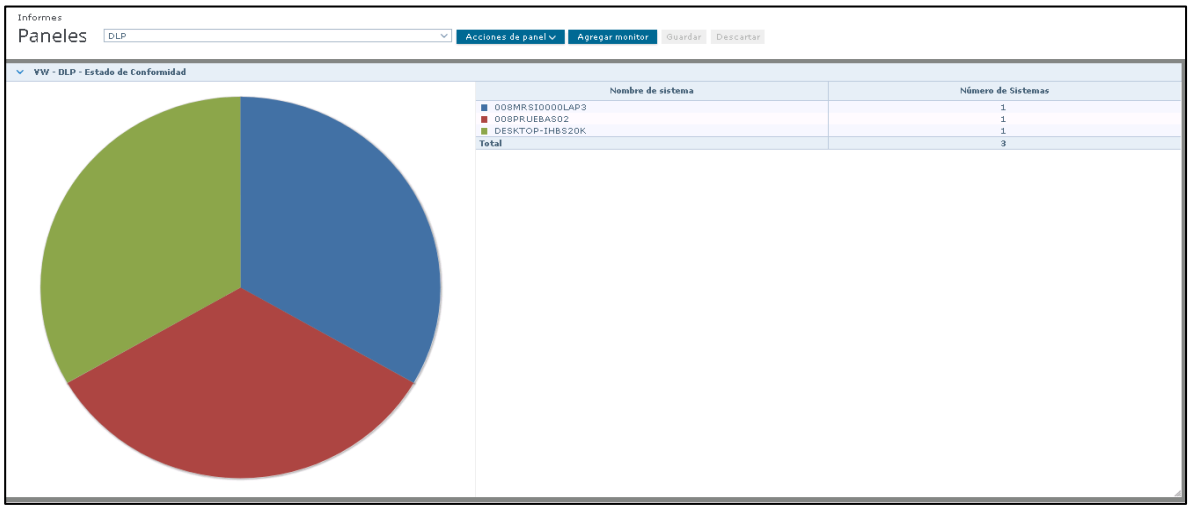



Figura 113: Panel para validar estado de cumplimiento de instalación de productos de DLP.

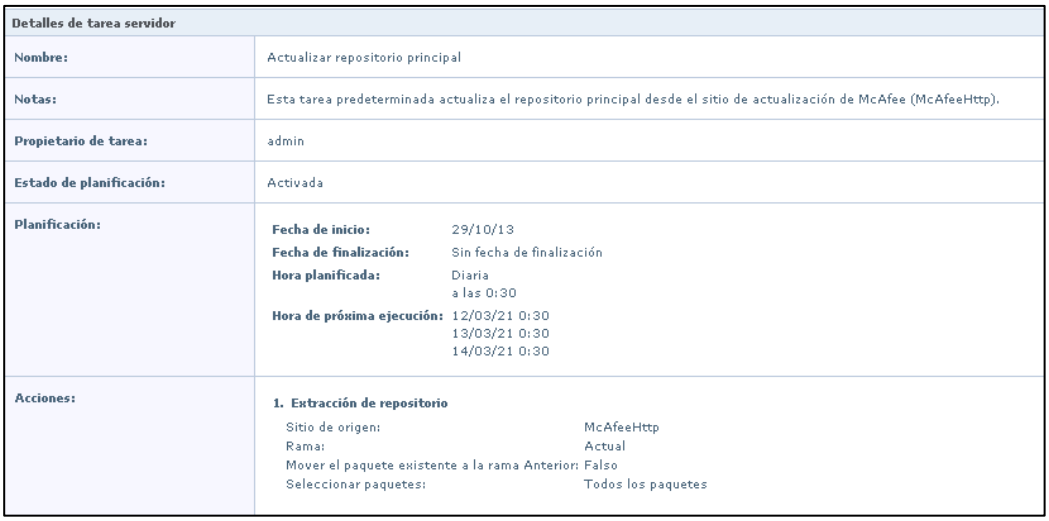
## Tareas del servidor

Las tareas servidor son acciones configurables que se ejecutan en McAfee ePO según las horas o intervalos planificados. Puede emplear las tareas servidor para automatizar las tareas repetitivas. McAfee ePO incluye tareas servidor y acciones preconfiguradas. La mayoría de los productos de software adicionales que se gestionan con McAfee ePO también incorporan tareas servidor preconfiguradas.

En el siguiente apartado, vamos a validar las tareas de servidor que se configuraron al momento de la implementación, tenemos tareas para la actualización del repositorio principal y descargar la lista de productos de software desde McAfee, así como él envió de reportes de eventos de amenaza a correos electrónicos definidos por los administradores.

La primera tarea está configurada para la actualización del repositorio principal, la cual está configurada para que se realice de manera diaria a las 0:30 horas y haga la validación a

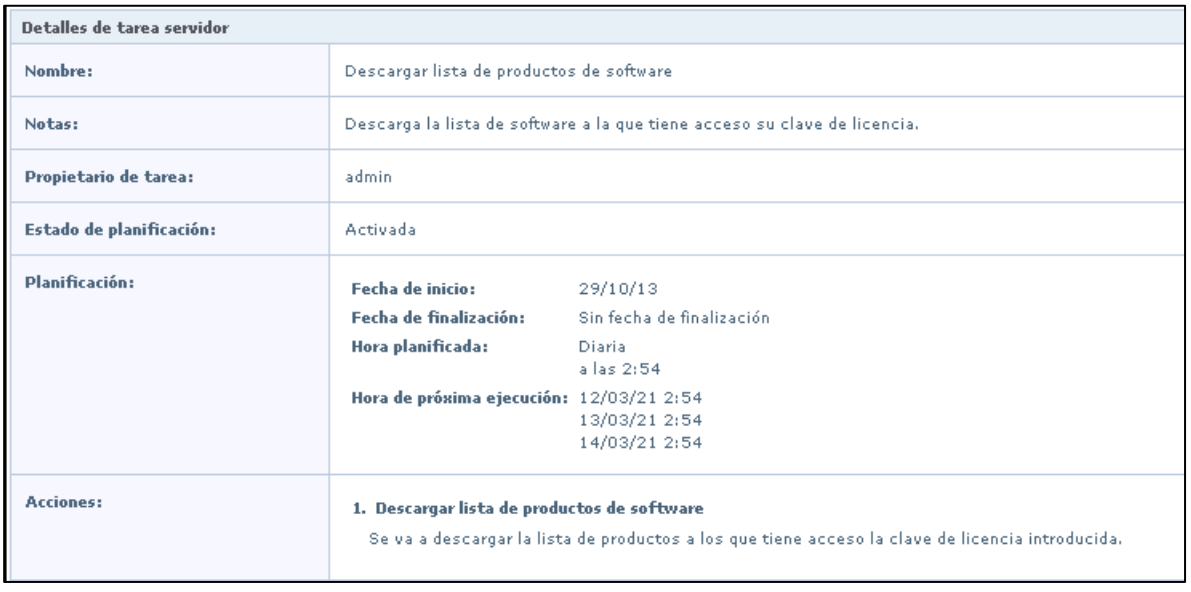
los sitios oficiales de McAfee. En la figura 114 se muestran los detalles de la tarea para actualizar el repositorio principal.



| Detalles de tarea servidor | |
|---|---|
| **Nombre:** | Actualizar repositorio principal |
| **Notas:** | Esta tarea predeterminada actualiza el repositorio principal desde el sitio de actualización de McAfee (McAfeeHttp). |
| **Propietario de tarea:** | admin |
| **Estado de planificación:** | Activada |
| **Planificación:** | **Fecha de inicio:** 29/10/13<br>**Fecha de finalización:** Sin fecha de finalización<br>**Hora planificada:** Diaria a las 0:30<br>**Hora de próxima ejecución:** 12/03/21 0:30, 13/03/21 0:30, 14/03/21 0:30 |
| **Acciones:** | **1. Extracción de repositorio**<br>Sitio de origen: McAfeeHttp<br>Rama: Actual<br>Mover el paquete existente a la rama Anterior: Falso<br>Seleccionar paquetes: Todos los paquetes |

Figura 114: Tarea del servidor para actualizar el repositorio principal.

La segunda tarea está configurada para descargar los productos de software de McAfee conforme a la clave de licencia que se tiene contratada, esta tarea está configurada para que se realice de manera diaria a las 02:54 horas y va a validar los productos que se tienen habilitados conforme a la clave de licencia agregada. En la figura 115 se muestran los detalles de la tarea para descargar los productos de software de McAfee.



| Detalles de tarea servidor | |
|---|---|
| **Nombre:** | Descargar lista de productos de software |
| **Notas:** | Descarga la lista de software a la que tiene acceso su clave de licencia. |
| **Propietario de tarea:** | admin |
| **Estado de planificación:** | Activada |
| **Planificación:** | **Fecha de inicio:** 29/10/13<br>**Fecha de finalización:** Sin fecha de finalización<br>**Hora planificada:** Diaria a las 2:54<br>**Hora de próxima ejecución:** 12/03/21 2:54, 13/03/21 2:54, 14/03/21 2:54 |
| **Acciones:** | **1. Descargar lista de productos de software**<br>Se va a descargar la lista de productos a los que tiene acceso la clave de licencia introducida. |

Figura 115: Tarea del servidor para descargar productos de software de McAfee.

La tercera tarea está configurada para el envío de reporte de amenazas detectas en las últimas 24 horas, la cual está configurada para que se envié de manera diaria cada 8 horas y se enviaran las consultas de Endpoint Security y VirusScan a los correos electrónico que se definieron al momento de la implementación. En la figura 116 se muestran los detalles de la tarea para el envío por correo electrónico de los reportes de las últimas 24 horas de Endpoint Security y VirusScan.

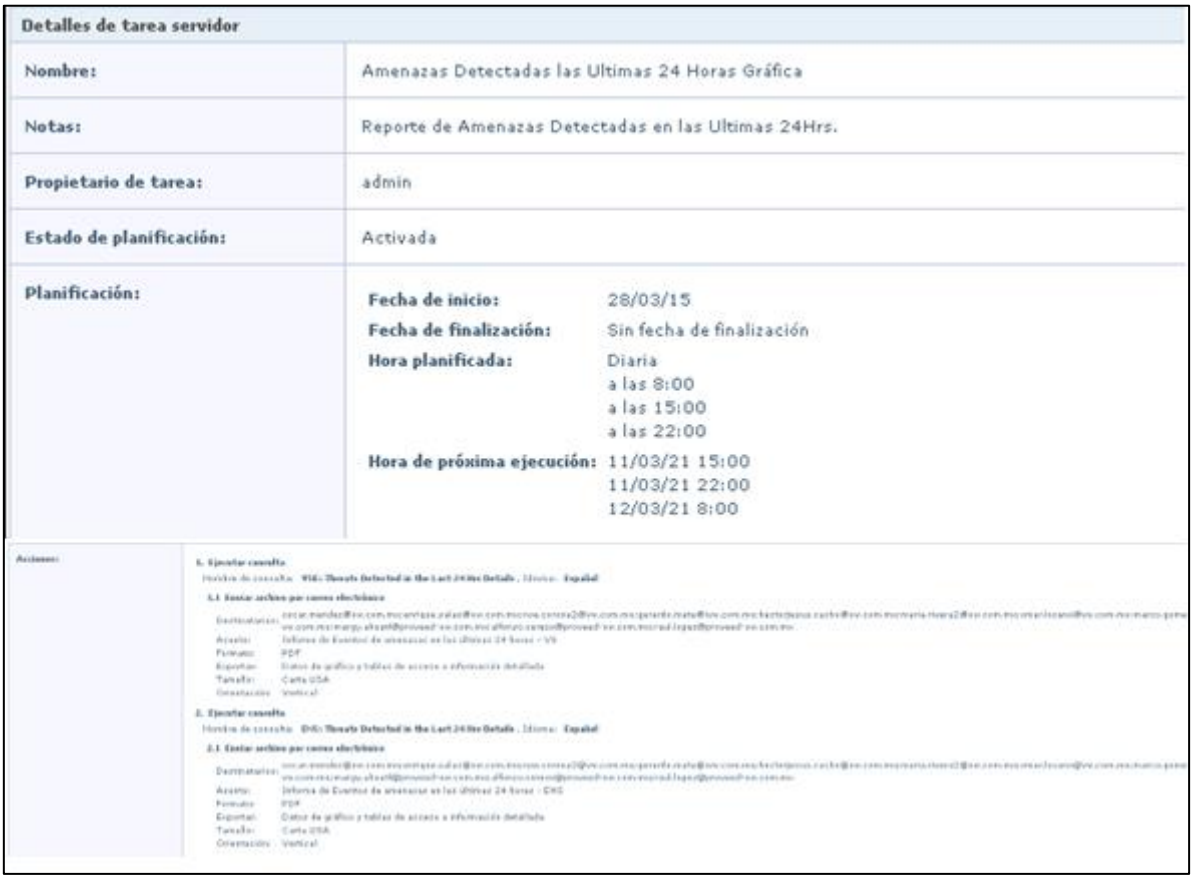



Figura 116: Tarea del servidor para envió de reportes de amenaza de las últimas 24 horas.

La cuarta tarea está configurada para el envío de reporte de amenazas detectas en los últimos 7 días, la cual está configurada para que se envié todos los lunes a las 08:00 horas y se enviaran las consultas de Endpoint Security y VirusScan a los correos electrónico que se definieron al momento de la implementación. En la figura 117 se muestran los detalles de la tarea para el envío por correo electrónico de los reportes de los últimos 7 días de Endpoint Security y VirusScan.


Figura 117: Tarea del servidor para envió de reportes de amenaza de los últimos 7 días.

# VII. IMPACTO DE LA EXPERIENCIA LABORAL

**VolksWagen de Mexico** planta de **Puebla** requiere realizar la actualización de versión de la consola de administración **McAfee ePO**, los agentes de comunicación, los agentes de protección de antimalware y la implementación de **McAfee Data Loss Prevention** en su módulo de **Device Control** para iniciar con el bloqueo de dispositivos de almacenamiento externo, ya que se valida que por este medio se han detectado el mayor número de amenazas potenciales.

Se inicia con el análisis pertinente, validando que la versión que se tienen actualmente de la consola de administración es **McAfee ePolicy Orchestrator 5.0.1,** también se valida que se cuenta con agentes de protección **McAfee VirusScan** y los agentes de comunicación, los cuales se encuentran en las versiones más obsoletas que existen al momento de la implementación. También es importante mencionar que se cuentan con Workstation y servidores legacy.

La versión que se tiene actualmente de la consola fue liberada en el año de 2013 la cual ya está detectada como ***End of Life*** (EOL). Para la instalación del producto de **McAfee Data Loss Prevention** solo es soportado a partir de la versión de **McAfee ePolicy Orchestrator 5.9.1** en adelante.

Es de suma importancia mencionar que estas versiones obsoletas de productos de **McAfee** representan un riesgo de seguridad de la información, ya que, al no estar actualizadas, no recibirán las actualizaciones correspondientes a las amenazas que se han detectado en la actualidad, así como las mejoras que se realizan a los productos para el óptimo funcionamiento de cada componente.

Después de realizar el análisis completo, se valida que para realizar la actualización de la consola es necesario ir escalando versiones hasta llegar a la versión **McAfee ePolicy Orchestrator 5.10,** por lo que se determinado conveniente realizar la instalación desde cero.

De igual manera se valida que para la protección de antimalware se cuenta con **McAfee Endpoint Security**, este producto remplaza completamente la solución de **McAfee VirusScan** ya que integra nuevas funcionalidades que permiten brindar una mayor protección a los equipos finales.

Se plática con el cliente para informarle todo lo que se detectó en el análisis realizado previamente y se le recomienda realizar la instalación es un ambiente completamente separado al de la consola actual. Sim embargo, se recomienda mantener la consola actual en operación ya que aún se cuentan con Workstation y servidores legacy [27] y derivado a esto las versiones actuales de McAfee ya no soportan versión legacy de sistemas operativos.

El cliente está de acuerdo con la que se propuso y nos prepara dos servidores virtuales nuevos, en un servidor se prepara la base de datos y en otro servidor se inicia con la instalación de la consola de administración **McAfee ePO** en su versión 5.10 parche 8.

Después de contar con la consola de **McAfee ePO** en la versión 5.10 y actualizada al parche 8, se realizó la incorporación de paquetes y extensiones de los productos **de McAfee Agent, McAfee Endpoint Security y Data Loss Prevention**. Es importante mencionar que la mayoría de los productos se incorporan al momento de integrar la licencia que se tiene contratada con McAfee y solo hay que validar que se cuente con los productos necesarios para la administración.

Las directivas fueron copiadas de la protección de **McAfee VirusScan** de la consola obsoleta y solo se acoplaron a la nueva estructura de **McAfee Endpoint Security**, de igual manera se agregaron nuevas directivas que fueron requeridas por los usuarios finales. Las directivas, reglas, conjunto de reglas y políticas para **McAfee Data Loss Prevention** fueron creadas desde cero y se necesitó pláticas con el cliente para conocer sus necesidades y saber que era requerido bloquear.

[27] Un sistema legacy un sistema, tecnología o aplicación de software antiguo o desactualizado que sigue en uso dentro de una organización porque sigue desempeñando las funciones para las que fue diseñado. (Stackscale, 2021)

Al momento de la implementación fue requerido aplicar el bloqueo solamente para dispositivos de almacenamiento externo como USB´s y Discos Externos. Se aclaro con el cliente que este producto de McAfee no bloquea los puertos de USB de los equipos, más bien aplica el bloqueo a tipo de dispositivo conectado y se puede bloquear por tipo de Bus, número de serie, marca, modelo, etcétera. Esto se define dependiendo de los dispositivos que tiene el cliente, para esta ocasión el bloqueo se manejó como tipo de bus (USB, IDE/SATA, SD).

La configuración de tareas se realizó de una manera más fácil, ya que la mayoría de las tareas que se encontraban en la consola obsoleta fueron exportadas e importadas a la consola que recién se había instalado, solamente se realizaron pequeños ajustes a las tareas para acoplarlas a los nuevos productos instalados.

La asignación de directivas y tareas consistió en realizar una comparativa de la consola obsoleta para realizar la asignación de manera adecuada, donde se tuvieron que realizar grupos en el árbol de sistema de la consola y también se crearon directivas puntuales para asignarlas a los grupos correspondientes conforme su solicitado por el cliente.

Las consultas y los paneles fueron realizados basándonos en las consultas que se tenían anteriormente en la consola obsoleta, de igual manera se realizaron nuevas consultas para los nuevos productos que se integraron, esto con la finalidad de tener una mayor visión de la administración de la consola, así como cumplimiento de los agentes, equipos sin comunicación, equipos con productos no instalados o actualizados, mayor número de amenazas o eventos de **DLP** detectados. Estas consultas también fueron utilizadas para crear paneles en la página de inicio de la consola y se tuviera una visión grafica de los que se tiene gestionado en la consola de administración **McAfee ePO.**

Las tareas del servidor son tareas que se encargan de actualizar y descargar productos al repositorio principal de la consola de administración, así como las firmas de seguridad de los motores de antimalware, también podemos realizar reportes automatizados de las consultas creadas para que sean enviados por correo electrónico, esto dependiendo de la planificación que se configure.

# VIII. REFERENCIAS DE CONSULTA


*¿Qué es el RDP?* (30 de Nov de 2021). Obtenido de https://nordvpn.com/es/blog/acceso-remoto-rdp/

Gartner, I. (Mayo de 2021).

Infocyte. (10 de marzo de 2021). Obtenido de https://www.infocyte.com/es/blog/2019/10/02/ir-planning-the-critical-6-steps-of-cyber-security-incident-response/

Infogram. (Mayo de 2021). Obtenido de https://www.evaluandoerp.com/logrando-una-implementacion-exitosa-de-un-erp/

McAfee. (2018). *Guía del producto de McAfee ePolicy Orchestrator 5.10.0.*

McAfee. (14 de jun de 2019). *Acerca de Politicas*. Obtenido de https://docs.trellix.com/es-ES/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-A9D09D98-03D2-4FA9-8101-3AF084631475.html

McAfee. (2019). Guía de instalación de McAfee ePolicy Orchestrator 5.10.0. 8-9.

McAfee. (22 de Abril de 2021). *Plataformas compatibles con ePolicy Orchestrator.* Obtenido de https://kc.mcafee.com/corporate/index?page=content&id=KB86693&locale=es_ES&viewlocale=es_ES

McAfee. (s.f.). *ePolicy Orchestrator* .

McAfeeGTI. (2018). *Cómo funciona McAfee GTI*. Obtenido de Guía del producto de McAfee Endpoint Security 10.7.x - Windows: https://docs.trellix.com/es-ES/bundle/endpoint-security-10.7.x-product-guide-windows/page/GUID-3371B693-4802-4BCE-9ADE-31912E37CB16.html

Microsoft. (2022). *Windows Server 2003*. Obtenido de https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2003-

Microsoft, S. (27 de Abril de 2022). *Microsoft SQL Server*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Microsoft_SQL_Server

Number, M. G. (January de 2018). *Embedded Partner Support Terms and Conditions or "Embedded Support Terms".* Obtenido de Embedded Support Terms: https://www.mcafee.com/enterprise/en-us/assets/legal/embedded-partner-support-terms.pdf

Proxy, M. (2022). *McAfee Blogs*. Obtenido de Que es un proxy: https://www.mcafee.com/blogs/es-es/privacy-identity-protection/que-es-un-proxy/

RealTime, M. (15 de FEB de 2019). *Cómo funcionan los análisis en tiempo real*. Obtenido de Guía del producto de McAfee Endpoint Security 10.7.x - Windows: https://docs.trellix.com/es-ES/bundle/endpoint-security-10.7.x-product-guide-windows/page/GUID-5A870D4E-FFBB-4F32-866E-A0F26F327501.html

Server, S. (11 de marzo de 2022). *Instancias del motor de base de datos (SQL Server)*. Obtenido de https://docs.microsoft.com/es-es/sql/database-engine/configure-windows/database-engine-instances-sql-server?view=sql-server-ver16

Stackscale. (31 de 08 de 2021). *¿Qué es un sistema legacy?* Obtenido de https://www.stackscale.com/es/blog/sistemas-legacy/

Techopedia. (28 de Diciembre de 2016). *End-of-Life Product (EOL Product)*. Obtenido de https://www.techopedia.com/definition/30051/end-of-life-product-eol-product

Trellix. (2022). *What Is a Zero-Day Exploit?* Obtenido de https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-a-zero-day-exploit.html

VirusScan. (2010). *McAfee.* Obtenido de https://community.mcafee.com/nysyc36988/attachments/nysyc36988/virusscan-enterprise/19515/1/vse_880_product_guide_en-us.pdf

XP, M. (2022). *Windows XP*. Obtenido de https://learn.microsoft.com/en-us/lifecycle/products/windows-xp