centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1208

Procedimiento de Empleo Seguro
Mcafee Endpoint Security

Agosto de 2021

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.01.28 10:39:34 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-21-170-9

Fecha de Edición: agosto de 2021

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. McAfee Endpoint Security es un producto que ha sido **cualificado para las familias de Antivirus/EPP (*Endpoint Protection Platform*) y EDR (*Endpoint Detection and Response*)**, incluidas en la taxonomía de productos definida en la guía CCN-STIC-140.
2. Este producto protege servidores, estaciones de trabajo, portátiles y tabletas contra amenazas conocidas y desconocidas. Estas amenazas incluyen *malware*, comunicaciones sospechosas, sitios web no seguros y archivos descargados.
3. Endpoint Security facilita que múltiples tecnologías de defensa se comuniquen en tiempo real para analizar y proteger contra amenazas.
4. El producto consta de los siguientes módulos de seguridad:
   - Prevención de amenazas: evita que las amenazas accedan a los sistemas, analiza los archivos automáticamente cuando se accede a ellos y ejecuta análisis específicos en busca de malware en los sistemas cliente.
   - *Firewall*: supervisa la comunicación entre el equipo y los recursos de la red e Internet. Intercepta las comunicaciones sospechosas.
   - Control web: supervisa las búsquedas web y la actividad de navegación en los sistemas cliente, y bloquea los sitios web y las descargas según las calificaciones de seguridad y el contenido.
   - Protección adaptable frente a amenazas: analiza el contenido de su empresa y decide cómo responder en función de la reputación de los archivos, las reglas y los umbrales de reputación.
5. El módulo '*Ajustes Generales*' proporciona la configuración necesaria para las funciones comunes, como la seguridad de interfaz y el registro. Este módulo se instala automáticamente si se instala cualquier otro módulo.
6. Todos los módulos se integran en una única interfaz de *Endpoint Security* en el sistema cliente. Cada módulo funciona de forma conjunta e independiente para proporcionar varios niveles de seguridad.
7. *McAfee Endpoint Security* puede ser utilizado para proteger entornos Windows, Linux y Mac, tanto en plataformas servidor como estaciones de trabajo
8. *McAfee Endpoint Security* se integra con otros componentes de McAfee para dotar a los *endpoints* de la mejor protección:
   - *McAfee ePolicy Orchestrator (ePO)* – elemento de gestión de McAfee para todas las soluciones de protección del *endpoint* incluyendo soluciones de protección basadas en tecnologías de lista blanca, soluciones de cifrado o de prevención de fugas de información. ePO permite desplegar, configurar y supervisar el uso de los módulos de *Endpoint Security* en la organización pudiendo ser desplegado tanto en infraestructuras *on-premise*, como en el cloud de McAfee (*MVision ePO*), como en infraestructuras de nube públicas.

- *MVision Insights* – permite mejorar la postura de seguridad anticipándose a los ataques antes de que ocurran. Podría definirse *MVision Insights* como una herramienta de threat intelligence (inteligencia de amenazas) que mapea cada campaña de *malware* activa con la configuración de seguridad desplegada en la organización. *MVision Insights* aporta:

  i. Evaluación del nivel de seguridad en función de la configuración de organización y perfil de riesgo único.

  ii. Inteligencia sobre amenazas sobre las principales campañas priorizadas por relevancia para la empresa

  iii. Paso a la acción mediante la priorización de acciones para proteger de manera proactiva frente a amenazas.

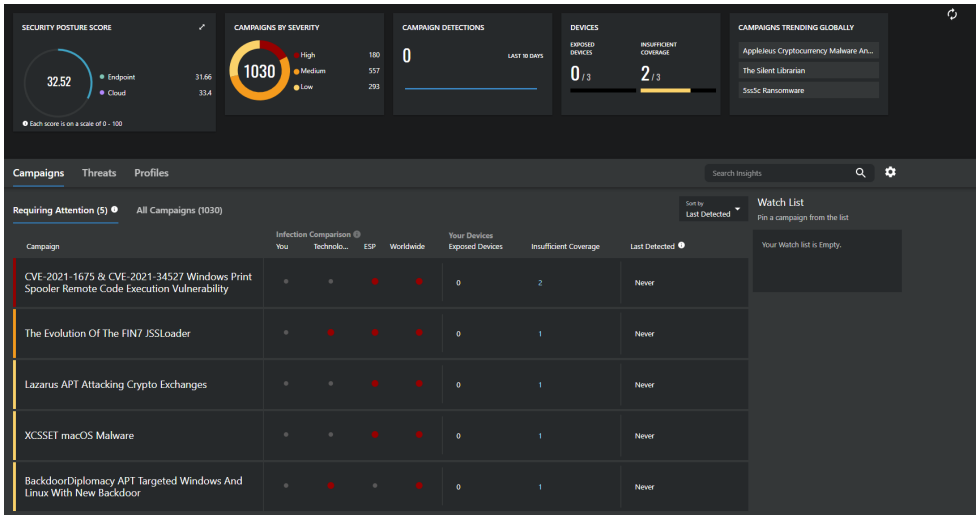

Ilustración 1. *MVision Insights*

- *MVision EDR* – permite simplificar la detección y respuesta a las amenazas persistentes avanzadas (APT) con controles EDR integrados.

  i. Minimiza la sobrecarga de alertas y da sentido a los datos a través de investigaciones guiadas por inteligencia artificial.

  ii. Reduce el tiempo de respuesta medio gracias a detecciones de alta fidelidad para impedir que los ataques consigan su objetivo.

  iii. Acelera la concienciación y la contención de amenazas a través del modelo de tácticas y técnicas MITRE ATT&CK.

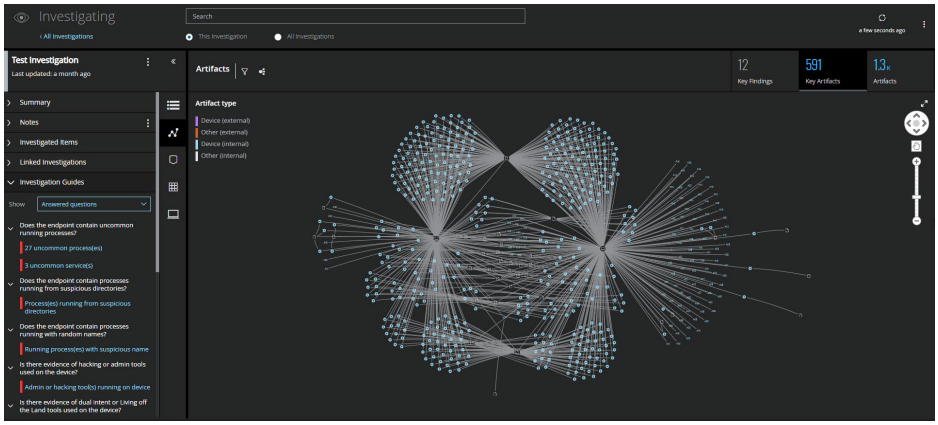

Ilustración 2. *MVision EDR*

- *MVision Mobile* – una solución que detecta las amenazas y las vulnerabilidades en dispositivos Apple iOS o Google Android, las redes a las que se conectan y las aplicaciones que han descargado los usuarios. Las funciones de detección incorporadas en el dispositivo ofrecen protección tanto si el dispositivo está online como si no. MVISION Mobile utiliza funciones de aprendizaje automático con información de miles de millones de puntos de datos procedentes de millones de dispositivos con el fin de identificar las amenazas y los ataques en curso o inminentes, incluidos los que nunca se habían visto antes

2. OBJETO Y ALCANCE

9. El objetivo de este documento es presentar las opciones de **despliegue, configuración y operación de seguridad de *McAfee Endpoint Security* 10.6 siendo gestionado por McAfee ePO 5.3.**

3. ORGANIZACIÓN DEL DOCUMENTO

10. Se indica la estructura de los diferentes apartados de este documento:

    a) **Apartado 4.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.

    b) **Apartado 5.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

    c) **Apartado 6.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

    d) **Apartado 7.** En este apartado se incluye un *checklist* para verificar las tareas de configuración segura mencionadas a lo largo del documento.

    e) **Apartado 8.** Incluye un listado de la documentación que ha sido referenciada a lo largo del documento.

    f) **Apartado 9.** Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

11. Cuando un organismo adquiere una de las *suites* que incluyen *McAfee ePO* y *Endpoint Security*, recibe un correo electrónico en la dirección indicada en el pedido de compra que contendrá su Carta de Concesión (*Grant Letter*)
12. En dicha Carta de Concesión aparecen dos (2) informaciones importantes:
    a) El listado de productos adquiridos con sus fechas de caducidad.
    b) El Número de Concesión (*Grant Number*) que debe ser usado tanto para acceder a la descarga de los productos adquiridos como al servicio de soporte oficial de McAfee.
13. Una vez recibida la Carta de Concesión, se puede acceder a https://www.mcafee.com/enterprise/en-us/downloads/my-products.html para descargar los productos a instalar. Para acceder a la página de descargas es necesario utilizar el Número de Concesión y una dirección de correo electrónico válida.
14. Los productos a descargar deben incluir al menos:
    a) El paquete de instalación de McAfee ePO.
    b) Las extensiones de cada uno de los módulos de *Endpoint Security*:
        i. *Endpoint Security Platform*
        ii. *Endpoint Security Threat Prevention*
        iii. *Endpoint Security Web Control*
        iv. *Endpoint Security Firewall*
        v. *Threat Detection Reporting*
        vi. *Endpoint Security Adaptive Threat Prevention*

        Estas extensiones deben ser instaladas en McAfee ePO en el orden indicado.
    c) Los paquetes de instalación de cada uno de los módulos indicados anteriormente, excepto *Threat Detection Reporting*. Estos paquetes deben ser incorporados en el repositorio maestro de *software* que forma parte de McAfee ePO.

4.2 ENTORNO DE INSTALACIÓN SEGURO

15. McAfee ePO utiliza una base de datos *Microsoft SQL* para alojar la configuración del sistema y los eventos generados en los *endpoint*. Adicionalmente, como parte de la arquitectura de McAfee ePO, se puede desplegar un componente llamado *Agent Handler* que se encarga de manejar las conexiones de los agentes desplegados en los *endpoints* con la base de datos de ePO. Este elemento tiene dos (2) casos de usos principales:

a) Situar un *Agent Handler* en una DMZ para habilitar la comunicación de los *endpoint* con *McAfee ePO* cuando los equipos se encuentren en Internet.

b) Distribuir la carga de conexiones de los *endpoints* en entornos con un número elevado de dispositivos gestionados.

16. Se recomienda que todos estos elementos: *McAfee ePO*, su base de datos y los posibles *Agent Handlers* sean emplazados en un lugar seguro. Tanto el acceso físico como el acceso lógico deben ser controlados y monitorizados.

4.3 REGISTRO Y LICENCIAS

17. Ni *McAfee ePO* ni *Endpoint Security* requieren de un proceso de registro como tal. Únicamente es necesario disponer un código de licencia válido para la instalación de McAfee ePO.

18. Dicho código de licencia se obtiene en la página de descargas de McAfee (https://www.mcafee.com/enterprise/en-us/downloads/my-products.html) a la que se accede con el Número de Concesión y una dirección de correo electrónico válida.

4.4 CONSIDERACIONES PREVIAS

19. Los entornos soportados por McAfee ePO pueden ser consultados aquí: *https://kc.mcafee.com/corporate/index?page=content&id=KB51569.*

20. Los entornos soportados por Endpoint Security pueden ser consultados aquí:

a) Entornos Windows:
https://kc.mcafee.com/corporate/index?page=content&id=KB82761

b) Entornos Linux:
https://kc.mcafee.com/corporate/index?page=content&id=KB91326
https://kc.mcafee.com/corporate/index?page=content&id=KB87073

c) Entornos Mac:
https://kc.mcafee.com/corporate/index?page=content&id=KB84934

21. Adicionalmente, se deben valorar los siguientes aspectos:

a) McAfee ePO:

i. Tipo de instalación a realizar – se soportan instalaciones *on-premise*, instalación en clúster utilizando los servicios de clúster de Microsoft, instalación en modo FIPS o despliegue en servicios cloud públicos (AWS y Azure) o en el cloud de McAfee (MVision ePO). **Los despliegues en cloud están fuera del alcance de la cualificación, por lo que se recomienda el despliegue *on-premise*.**

ii. Utilizar entornos virtuales o físicos.

iii. Planes de escalabilidad para cubrir un crecimiento futuro.

iv. Ubicación del servidor ePO y de los *Agent Handlers* en la red para obtener visibilidad desde todos los *endpoints* a gestionar.

v. Distribución geográfica y posibles problemas de ancho de banda entre sedes.

vi. Para estimar el crecimiento de la base de datos es importante conocer el número de nodos a gestionar, las aplicaciones McAfee que se van a desplegar y el periodo de retención de eventos en la base de datos.

vii. Para la instalación de McAfee ePO es necesario contar con una cuenta de acceso a Microsoft SQL Server con permisos de *sysadmin*, *DBcreator* y *public*.

viii. El servidor SQL donde se aloje la base de datos de ePO debe tener habilitado el protocolo TCP/IP y el servicio *SQL Server Browser* en ejecución.

ix. Como parte del proceso de instalación se ejecuta la herramienta *Pre-Installation Auditor* que revisa que el entorno al completo cumpla con los requisitos de instalación. Es importante que todos los *checks* realizados por *Pre-Installation Auditor* sean validados antes de la instalación.

x. Validar que los puertos que se usan en las comunicaciones entre los elementos que forman la arquitectura de ePO están libres y abiertos en la red. Se puede consultar el listado completo de puertos en *https://kc.mcafee.com/corporate/index?page=content&id=KB66797*.

b) Endpoint Security

i. Considerar los entornos soportados indicados anteriormente para cada sistema operativo.

ii. Analizar que módulos es necesario desplegar en cada tipo de *endpoint*.

4.5 INSTALACIÓN

22. El proceso de instalación de McAfee ePO está basado en un asistente sencillo de gestionar. Durante el proceso se realizan, entre otras, las siguientes acciones:

a) Se instalará automáticamente cualquier *software* de Microsoft necesario para el correcto funcionamiento de *McAfee ePO*.

b) Seleccionar el servidor SQL que alojará la base de datos ePO y autenticar con un usuario que tengo los privilegios indicados anteriormente.

c) Elegir los puertos TCP/UDP a utilizar para la comunicación entre los diferentes elementos que forman parte de la arquitectura de ePO. Se recomienda modificar los puertos por defecto por tratarse de puertos bien conocidos en la industria. Hay que tener en cuenta que se debe adaptar el entorno para permitir las comunicaciones entre los elementos si existen dispositivos que apliquen listas de control de acceso.

d) Definir la contraseña para la cuenta de administración por defecto y para el cifrado del almacén de las claves de comunicación entre los *endpoints* y el servidor ePO. **Estas claves deben tener una complejidad alta**. Para ello, seguir los criterios de complejidad de contraseñas definidos en el apartado 5.3.1.a).

23. Una vez instalado el servidor ePO es necesario desplegar el componente *McAfee Agent*, encargado de gestionar las comunicaciones entre el servidor de gestión y los productos desplegados en los *endpoints*. En concreto, *McAfee Agent* se encarga de contactar con el servidor ePO para recoger nuevas directivas y tareas configuradas en el servidor y para subir al servidor los eventos generados en el *endpoint* y las propiedades del mismo (inventario *hardware* y *software* generado por el propio agente)

24. *McAfee Agent* puede ser desplegado de múltiples maneras:

    a) Desde la consola de gestión *McAfee ePO*. Se deben cumplir varios requisitos como que el recurso *Admin$* en sistemas *Windows* sea accesible desde ePO o que el servicio SSH está activado en sistemas Linux o Mac.

    b) Manual usando el paquete de instalación *FramePkg.exe* que puede ser generado en ePO.

    c) Mediante herramientas de distribución de *software* de terceros.

    d) Usando un *script* de inicio de sesión en sistemas Windows.

    e) Utilizando la funcionalidad *McAfee Smart Install* que añade la opción de ubicar los equipos en el Árbol de Sistemas[1] en el grupo adecuado.

    f) Mediante herramientas de clonado de sistemas. En este caso es imprescindible eliminar el identificador del agente (GUID) antes de obtener la imagen maestra.

25. Por último, se debe desplegar el *software* de protección *McAfee Endpoint Security*. Como se ha mencionado anteriormente, para poder desplegar *Endpoint Security* desde *McAfee ePO* es necesario incorporar los paquetes de instalación al repositorio maestro de ePO. Adicionalmente, es necesario tener *McAfee Agent* previamente instalado en los equipos.

26. La instalación de *Endpoint Security* se realiza mediante tareas de despliegue configuradas en *McAfee ePO*. Si se utiliza el método habitual, una vez instalado en el equipo, *Endpoint Security* aplicará la política por defecto definida por *McAfee*. Si se desea implementar una directiva personalizada desde el momento de la instalación se recomienda utilizar la herramienta *Endpoint Security Package Designer.*

[1] El árbol de sistemas es una representación gráfica de cómo está organizada la red gestionada. Organiza los sistemas de la red en grupos y subgrupos.

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

27. McAfee ePO soporta el modo de cumplimiento Common Criteria, llamado modo FIPS. **Se debe configurar el producto para que haga uso del modo FIPS.**
28. En modo FIPS, McAfee ePO:
    a) Establece restricciones adicionales respecto de los tipos de métodos de seguridad permitidos.
    b) Realiza pruebas adicionales durante el inicio.
    c) Solo permite conexiones procedentes de una versión de *McAfee Agent* conforme con FIPS.
29. Para instalar ePO en modo FIPS es necesario acceder a una línea de comandos y ejecutar el siguiente comando: ***setup.exe ENABLEFIPSMODE=1***
30. Para comprobar si un servidor ePO se está ejecutando en modo FIPS se puede consultar el archivo *server.ini* y buscar el valor *FipsMode*. Si este valor está a 1 significa que el servidor está ejecutando en modo FIPS. En caso contrario, el valor estará a 0.

5.2 AUTENTICACIÓN

31. En el ecosistema McAfee ePO existen diferentes mecanismos de autenticación y aseguramiento de las comunicaciones entre los distintos elementos.
32. El acceso a la consola de gestión de *McAfee ePO* se realiza a través de navegador con una conexión SSL a un puerto definido durante el proceso de instalación. Por defecto, se utiliza un certificado autofirmado que **debe ser sustituido por un certificado SSL** estándar siguiendo las instrucciones indicadas en el siguiente artículo: *https://kc.mcafee.com/corporate/index?page=content&id=KB72477*
33. Para el acceso de los usuarios a la consola de gestión se pueden utilizar tres (3) métodos de autenticación:
    a) Usuarios locales cuyas credenciales se almacenan cifradas en la base de datos de ePO. El usuario *admin* creado durante la instalación es un usuario de tipo local.
    b) Integración con servidores LDAP. Se realiza mediante la opción de Servidores registrados en el servidor ePO. Los servidores soportados son *Active Directory* de *Microsoft* y servidores *OpenLDAP*. En ambos casos, se deben utilizar conexiones SSL para proteger las comunicaciones entre ePO y el servicio LDAP. Una vez registrado el servidor LDAP, se crean los usuarios, indicando su nombre (login) y el dominio al que pertenecen.
    c) Autenticación basada en certificados. El primer paso para configurar esta opción es acceder a la configuración del servidor ePO y habilitar el uso de

certificados para la autenticación de los usuarios. Como parte de la configuración se indica la Autoridad de Certificados responsable de la firma de los certificados. **Se debe también verificar el estado de validez de los certificados.** Para ello, se puede añadir una CRL (Lista de certificados revocados) o se puede utilizar OCSP (*Online Certificate Status Protocol*) como método alternativo para confirmar la validez de un certificado. Una vez habilitada la funcionalidad, se deben crear los usuarios indicando el Distinguised Name del certicado y cargando el certificado en ePO.

34. Las comunicaciones entre los diferentes elementos que componen la arquitectura de McAfee ePO se aseguran utilizan un conjunto de certificados generados y almacenados por el propio ePO. Estos certificados deben ser regenerados si se sospecha que han sido vulnerados o, por seguridad, cada cierto tiempo. Una vez regenerados, cada elemento cambiará el certificado en la siguiente conexión con el servidor.

35. En el caso de *McAfee Endpoint Security*, mediante la directiva *de 'Opciones de Endpoint Security Common'*, es posible:

    a) Limitar el acceso a la consola de gestión local mediante contraseña, no permitiendo acceder a las opciones de configuración avanzadas.

    b) Proteger completamente el acceso a la configuración en local mediante la definición de una contraseña.

    c) Definir criterios para bloquear el acceso a la interfaz de gestión local en base a número de intentos de autenticación fallidos.

    d) En esta misma directiva, además se pueden configurar la autoprotección de archivos, carpetas, entradas de registro y procesos de *Endpoint Security*.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

36. Existen dos (2) formas de gestionar el servidor ePO:

    a) A través de navegador, ya sea local en servidor o desde un equipo remoto. Esta conexión se realiza a través de conexión SSL a un puerto definido durante el proceso de instalación. Se pueden establecer mecanismos para asegurar el acceso de los usuarios a la consola. Siempre bajo las opciones de configuración del servidor, se debe:

        i. Definir un mensaje personalizado tipo *banner* que se muestre en la pantalla de *login*.

        ii. Bloquear una cuenta de usuario si se produce un número determinado de intentos de autenticación fallidos. Se recomienda que las cuentas de usuario se bloqueen al realizar, como máximo, 5 intentos fallidos.

iii. Crear una lista blanca y una lista de direcciones IP para acceder al servidor ePO. La lista negra se puede alimentar automáticamente si se producen 10 intentos de autenticación en un periodo de 60 segundos.

iv. Definir criterios de rotación y complejidad de las contraseñas de usuario:

- Las contraseñas deben contener al menos una mayúscula, una minúscula, un número y un carácter especial (#?!@$%^&*-).
- Las contraseñas deben tener una longitud mínima de 12 caracteres.
- Cuando se cambia la contraseña, esta tendrá que diferir de la anterior en, al menos, las 5 contraseñas anteriores.
- El cambio de contraseña debe realizarse cada cierto tiempo, máximo de 60 días para los administradores.
- Desde el cambio de contraseña, esta no puede ser cambiada en un mínimo de 4 días.
- Algunas buenas prácticas en la selección de la contraseña, son: evitar palabras de diccionario, secuencias numéricas, secuencias de caracteres seguidos en el teclado, evitar añadir números al final de la palabra o números al final de la contraseña anterior, caracteres repetidos, información personal, etc.

v. Definir un intervalo de tiempo de inactividad para cerrar una sesión de usuario.

vi. Limitar las sesiones a una única IP simultánea.

b) Mediante el de la WebAPI presentada por *McAfee ePO*. La documentación de la API puede ser consultada aquí: https://docs.mcafee.com/es-ES/bundle/epolicy-orchestrator-web-api-reference-guide/page/GUID-D87A6839-AED2-47B0-BE93-5BF83F710278.html. Adicionalmente, se puede consultar la lista de métodos soportados usando la siguiente URL: *https://IP_ePO:Puerto_gestión_ePO/remote/core.help*.

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

37. Los permisos asignados a un administrador de *McAfee ePO* se configuran mediante la opción '*Conjuntos de Permisos*'. *McAfee ePO* incluye cuatro (4) conjuntos de permisos predeterminados:

a) Revisor ejecutivo: proporciona permisos de visualización para los paneles, eventos y contactos, así como para la información relacionada con todo el Árbol de sistemas.

b) Revisor global: proporciona acceso de visualización global para el conjunto de la funcionalidad, los productos y el Árbol de sistemas, excepto para

extensiones, datos acumulados de varios servidores, servidores registrados y software.

c) Administrador global: proporciona permisos de visualización y modificación para el conjunto de las funciones de McAfee ePO. Los usuarios a los que se asigna este conjunto de permisos necesitan al menos un conjunto de permisos adicional que conceda acceso a los productos y grupos necesarios del Árbol de sistemas.

d) Revisor de grupo: concede permisos de visualización para todas las funciones de *McAfee ePO*. Los usuarios a los que se asigne este conjunto de permisos necesitan al menos un conjunto de permisos adicional que conceda acceso a los productos y grupos necesarios del Árbol de sistemas.

38. Los conjuntos de permisos varían en función de las extensiones instaladas en McAfee ePO, es decir, en función de los productos gestionados de la consola. A medida que se instalan extensiones para nuevos productos se añaden nuevas opciones a los conjuntos de permisos. Esto dota a la gestión de permisos de una granularidad total, pudiendo elegir qué usuarios tienen acceso a la gestión de que máquinas, qué productos pueden gestionar en esos equipos y qué pueden hacer dentro de la gestión de cada producto.

39. Se recomienda revisar con periodicidad la lista de usuarios y el conjunto de permisos asignados a cada uno de ellos para evitar "*cuentas durmientes*".

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

40. McAfee ePO monta tres (3) servicios tras su instalación:

a) Servidor de *McAfee ePolicy Orchestrator* que corresponde con el servidor Web incluido en el ePO (*Apache*) y que se encarga de gestionar las comunicaciones de los agentes.

b) Servidor de Aplicaciones de *McAfee ePolicy Orchestrator* que corresponde con el servidor de aplicaciones incluido en ePO (*Tomcat*) y que soporta la interfaz de gestión

c) Analizador de eventos de *McAfee ePolicy Orchestrator* que es el servicio encargado de escribir la información en la base de datos de ePO

d) Todos los servicios se ejecutan bajo la cuenta *Local System de Microsoft Windows.*

41. Como se ha mencionado anteriormente, cada uno de los puertos que se utilizan en las comunicaciones entre los diferentes componentes de ePO son personalizables durante la instalación. **Se recomienda modificar todos los puertos por defecto.**

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

42. Todo el entorno McAfee ePO usa **TLS v1.2. Se debe garantizar que se usa esta versión y no versiones anteriores inseguras.** Para configurar el entorno y

deshabilitar las versiones 1.0 y 1.1, se debe seguir lo indicado en el siguiente documento:
https://kc.mcafee.com/corporate/index?page=content&id=KB86318.

5.6 GESTIÓN DE CERTIFICADOS

43. **Se deben sustituir los certificados auto-firmados por defecto en ePO por unos certificados personalizados generados por una Autoridad de Certificados de confianza.** Para ello, se debe seguir lo indicado en el apartado 5.2 de este documento

5.7 SERVIDORES DE AUTENTICACIÓN

44. En el apartado 5.2 se indica también cómo integrar ePO con un servicio de directorio externo LDAP para la autenticación de usuarios.

5.8 ACTUALIZACIONES

45. Antes de iniciar el proceso de actualización de McAfee ePO es necesario comprobar que el entorno cumple con los requisitos *hardware* y *software* de la nueva versión y, sobre todo, que las versiones de las extensiones instaladas en ePO están soportadas en la versión de destino. En el caso de que alguna versión no esté soportada, será necesario actualizarla o eliminarla si se trata de un producto *legacy*.

46. La actualización de *McAfee ePO* se realiza utilizando el programa de instalación de la versión de destino. Como parte del proceso de instalación se ejecuta la herramienta *Pre-Installation Auditor*. Esta herramienta se encarga de revisar el entorno actual para comprobar que se cumplen todos los requisitos para actualizarlo.

47. Si bien el procedimiento estándar es el definido en el párrafo anterior, existen versiones que incluyen cambios que exigen acciones adicionales, por ejemplo, si la nueva versión incluye un cambio en la longitud de los certificados que aseguran las comunicaciones cliente-servidor, será necesario propagar este cambio a los equipos.

48. En el caso de *Endpoint Security*, la actualización de producto se realiza de manera similar a la instalación inicial. Es necesario instalar las extensiones de la nueva versión, incorporar los paquetes de instalación al repositorio maestro, replicar el contenido del repositorio maestro a los repositorios distribuidos (si existen) y crear una tarea de instalación que asignar a los equipos que se vayan a actualizar.

49. Como buena práctica, se recomienda utilizar la rama *Evaluación* del repositorio maestro para la incorporación inicial de los paquetes de instalación. A continuación, se selecciona un conjunto de máquinas y se les aplica la actualización. Una vez validado el despliegue en el entorno piloto se deben mover paquetes desde la rama *Evaluación* a la rama *Actual* en el repositorio

maestro e iniciar la distribución de la actualización a todo el parque de equipos protegidos.

50. En cuanto a las actualizaciones de los contenidos de seguridad que utilizan los diferentes módulos de *Endpoint Security*, el flujo es el siguiente: Sitio de origen (*https://update.nai.com/Products/CommonUpdater*) → Repositorio maestro → Repositorios distribuidos → Equipos protegidos

51. Para completar el flujo es necesario definir o configurar las siguientes tareas:

a) McAfee ePO incluye por defecto una tarea de actualización del repositorio maestro. Esta tarea es editable para adaptar su configuración a las necesidades de cada organización

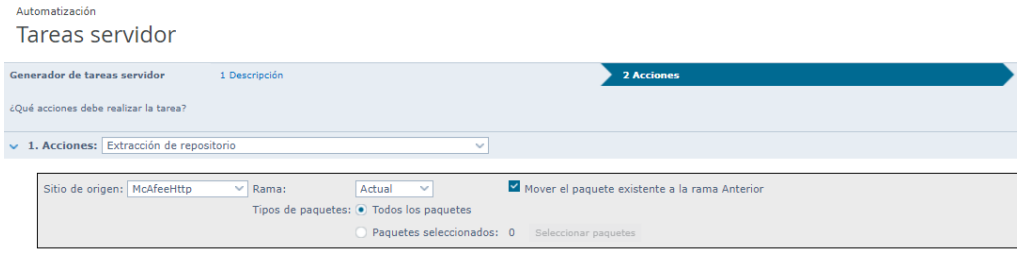

Ilustración 3. Actualización de repositorio

b) A continuación, es necesario replicar el contenido del repositorio maestro a los repositorios distribuidos, si existen. Para ello es necesario crear una tarea de servidor que incluya una acción de Replicación de repositorio

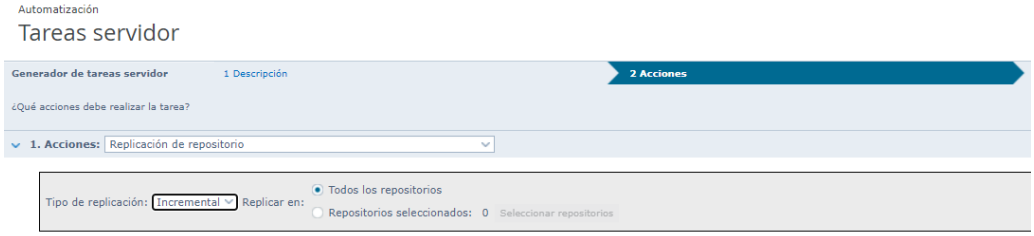

Ilustración 4. Selección de tipo de replicación

c) Es posible ejecutar la extracción del repositorio maestro y la replicación de repositorios distribuidos bajo la misma tarea de servidor encadenando ambas acciones. De esta manera, la replicación se ejecutar inmediatamente después de la extracción.

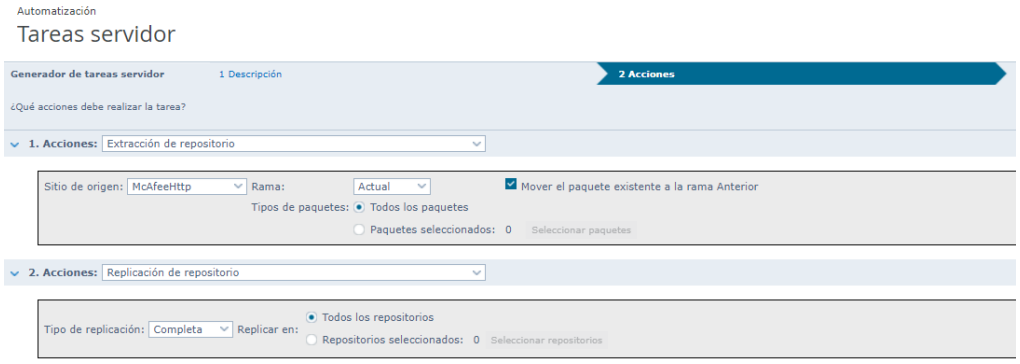

Ilustración 5. Encadenamiento de acciones

d) Una vez actualizada toda la arquitectura de ePO, el último paso es actualizar los contenidos de seguridad de *Endpoint Security*. Para ello, se utiliza una tarea de cliente de McAfee Agent de tipo '*Actualización de Producto'*.

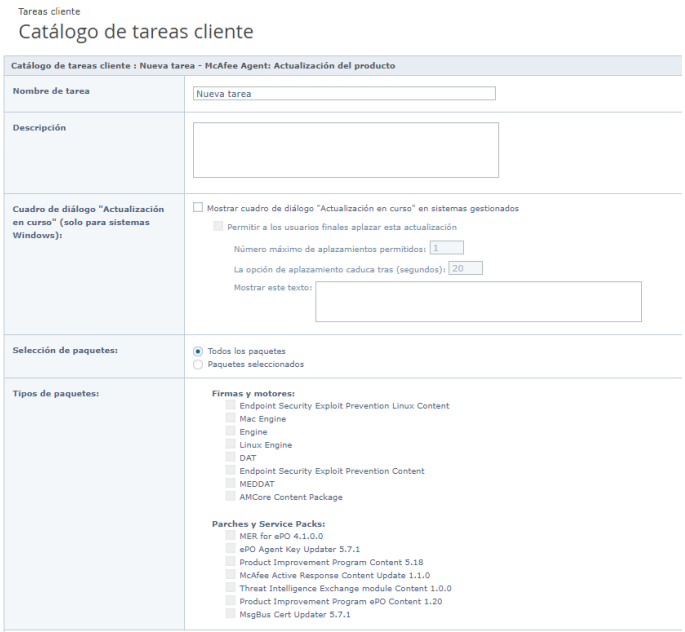

Ilustración 6. Tarea de actualización de producto

e) En las tareas de actualización de producto se pueden desplegar todas las actualizaciones o las seleccionadas. Se recomienda crear al menos dos tareas: una que actualice los contenidos de seguridad diarios y otra que actualice el motor del módulo *antimalware.*

f) Por último, es necesario asignar la tarea de cliente a los *endpoints* en el Árbol de Sistemas

5.9 SNMP

52. McAfee ePO permite registrar servidores SNMP con el objetivo de configurar respuestas automáticas que envíen capturas al servidor SNMP de los eventos recogidos en ePO. La configuración se realiza en la opción Servidores Registrados de ePO

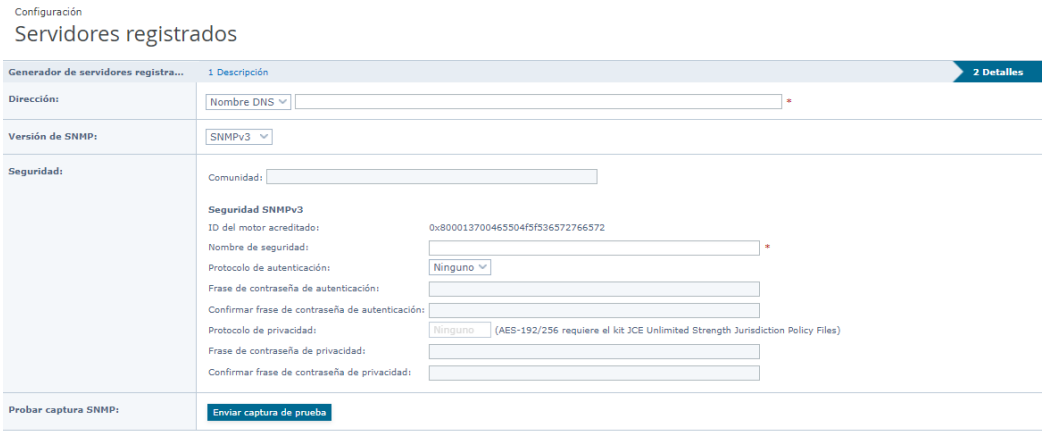

Ilustración 7. Tarea de actualización de producto

53. **Se debe utilizar la versión SNMPv3**. A continuación se crea una Respuesta automática cuya acción es el envío de una captura al servidor SNMP.

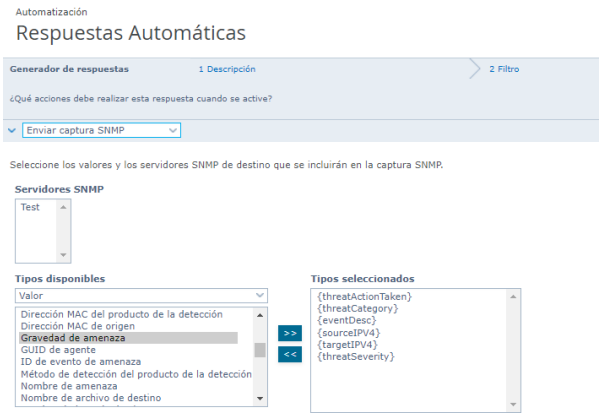

Ilustración 8. Tarea de actualización de producto

5.10 ALTA DISPONIBILIDAD

54. McAfee ePO soporta los servicios de clúster de Microsoft aunque no es una opción que se utilice con frecuencia. Los motivos son los siguientes:

    a) La proliferación del uso de entornos virtuales con herramientas tipo *snapshot* incluidas hace que la recuperación de un servidor ePO sea una cuestión de minutos.

    b) ePO incluye su propia funcionalidad de *snapshot* que permite guardar toda la configuración del servidor en la base de datos de ePO. Para obtener el *snapshot* de ePO existe una tarea de servidor por defecto. Para la recuperación, basta con lanzar el programa de instalación de ePO y, en la primera pantalla, se puede seleccionar un *check* para indicar que se desea recuperar el servidor desde un *snapshot*

55. Sin embargo, si se utiliza un servidor SQL físico para alojar la base de datos de ePO, sí se recomienda utilizar un entorno en clúster de Microsoft SQL Server

56. En cuanto a la funcionalidad de *Agent Handler* de ePO, la configuración permite desplegar una granja de servidores *Agent Handler* detrás de un balanceador. Esto permite dotar de alta disponibilidad a la arquitectura y, si el balanceador lo permite, optimizar las conexiones de los agentes con los *Agent Handler.*

57. Por último, si se precisa proteger un entorno de clúster, se deben instalar tanto *McAfee Agent* como *Endpoint Security* en todos los nodos del clúster de manera independiente.

5.11 AUDITORÍA

5.11.1 REGISTRO DE EVENTOS

58. McAfee ePO utiliza un archivo de *log* para cada uno de los servicios que levanta:

    a) Servidor de Aplicaciones de *McAfee ePolicy Orchestrator* (*Tomcat*): *orion.log* u *orion_nombreservidor.log.* Situado en:

    \<*epoinstallationdirectory*>*server**logs*\

    b) Analizador de eventos de *McAfee ePolicy Orchestrator*: *eventparser.log* o *eventparser_nombreservidor.log.* Situado en:

    \<*epoinstallationdirectory*>*db**logs*\

    c) Servidor de *McAfee ePolicy Orchestrator* (*Apache*): el *archive server.log* o *server_nombreservidor.log*. Situado en:

    \<*epoinstallationdirectory*>*db**logs*\

59. La siguiente tabla describe los archivos de log anteriores y algunos adicionales:

Nombre de archivo	Tipo	Ubicación	Descripción
EpoApSvr_<nombre_servidor>.log	Principal	[directorio_instalación]\DB\Logs	Archivo de registro del servidor de aplicaciones con detalles sobre las acciones del repositorio, tales como las siguientes: • Tareas de extracción • Inserción de paquetes de despliegue en el repositorio • Eliminación de paquetes de despliegue del repositorio **NOTA:** Este archivo no está presente hasta después del inicio del servicio inicial.
Errorlog.<fecha_y_hora_actuales>	Apache	[directorio_instalación]\Apache2\logs	Contiene los detalles del servicio Apache. **NOTA:** Este archivo no está presente hasta que se inicia el servicio Apache por primera vez.
Eventparser_<nombre_servidor>.log	Principal	[directorio_instalación]\DB\Logs	Contiene detalles de servicios del analizador de eventos de McAfee ePO, como el análisis de eventos de producto correcto o con errores.

Nombre de archivo	Tipo	Ubicación	Descripción
Jakarta_service_<fecha>_<nombre_servidor>.log	Tomcat	*[directorio_instalación]\Server\logs*	Contiene detalles del servicio de servidor de aplicaciones de McAfee ePO. **NOTA:** Este archivo no está presente hasta después del inicio del servicio Tomcat inicial.
Localhost_access_log.<fecha>.txt	Tomcat	*[directorio_instalación]\Server\logs*	Registra todas las solicitudes del servidor de McAfee ePO recibidas de los sistemas cliente. **NOTA:** Este archivo no está presente hasta después del inicio del servicio Tomcat inicial.
Orion_<nombre_servidor>.log	Principal	*[directorio_instalación]\Server\logs**	Contiene detalles de la plataforma y todas las extensiones cargadas de forma predeterminada. **NOTA:** Este archivo no está presente hasta que se inicia el servicio de servidor de aplicaciones de McAfee ePO por primera vez.

Nombre de archivo	Tipo	Ubicación	Descripción
Replication_<nombre_servidor>.log	Servidor	*[directorio_instalación]\DB\Logs*	El archivo de registro de replicación del servidor de McAfee ePO. Este archivo solo se genera cuando se cumplen todos estos criterios: • Hay repositorios distribuidos. • Se ha configurado una tarea de replicación. • Se ha ejecutado una tarea de replicación.
Server_<nombre_servidor>.log	Principal	*[directorio_instalación]\DB\Logs*	Contiene detalles relacionados con los siguientes servicios del servidor de McAfee ePO: • Comunicaciones agente-servidor • Controlador de agentes de McAfee ePO **NOTA:** Este archivo no está presente hasta después del inicio del servicio inicial.
Stderr_<nombre_servidor>.log	Tomcat	*[directorio_instalación]\Server\logs**	Contiene cualquier salida de error estándar capturada por el servicio Tomcat. **NOTA:** Este archivo no está presente hasta después del inicio del servicio Tomcat inicial.

Nombre de archivo	Tipo	Ubicación	Descripción
<GUID_agente>_<marca_tiempo>_Server_manifest.xml	Directiva	*[directorio_instalación]\DB\DEBUG*	Contiene detalles sobre los problemas de actualización de directivas. Para activar este archivo, se debe hacer lo siguiente: • Buscar esta clave de Registro: *HKEY_LOCAL_MACHINE\Software\Network Associates\ePolicy Orchestrator* • Crear este parámetro DWORD con el valor 1: *SaveAgentPolicy* • Reiniciar el servicio de servidor de McAfee ePolicy Orchestrator (Apache). **SUGERENCIA:** se debe activar este archivo durante la menor cantidad de tiempo posible para capturar la información necesaria, ya que los archivos resultantes crecen rápidamente.

60. La siguiente tabla muestra los archivos de registro de *McAfee Agent:*

Nombre de archivo de *McAfee Agent*	Tipo	Ubicación	Descripción
masvc_<nombre_host>.log	Servidor	*[Ruta de DATA del agente]\logs*	Se genera cuando se utiliza *masvc.exe*. Este archivo contiene información relativa a lo siguiente: • Recopilación de propiedades • Implementación de directivas • Planificación de tareas • Comunicación agente-servidor • Sesiones de actualización

Nombre de archivo de *McAfee Agent*	Tipo	Ubicación	Descripción
macmnsvc_<nombre_host>.log	*McAfee Agent*	*[Ruta de DATA del agente]\logs*	Se genera cuando se utiliza macmnsvc.exe. Este archivo contiene información relativa a: • Servidor punto a punto • SuperAgent • Activación • RelayServer
macompatsvc_<nombre_host>.log	*McAfee Agent*	*[Ruta de DATA del agente]\logs*	Se genera cuando se utiliza macompatsvc.exe. Este archivo contiene información relacionada con la compatibilidad de los productos gestionados con los servicios de *McAfee Agent*.
masvc_<nombre_host>_backup_<número_copia_seguridad>.log	*McAfee Agent*	*[Ruta de DATA del agente]\logs*	Se genera como archivos de copia de seguridad de los servicios de agente.
marepomirror.log	Servidor		Se genera cuando se utiliza *marepomirror.exe*. Este archivo contiene información relacionada con la duplicación del repositorio.
FrmInst_<nombre_host>.log	*McAfee Agent*	*%temp%\McAfeeLogs*	Se genera cuando se utiliza *FrmInst.exe* para instalar *McAfee Agent*. Este archivo contiene lo siguiente: • Mensajes informativos • Mensajes de progreso • Mensajes de error si falla la instalación

Nombre de archivo de *McAfee Agent*	Tipo	Ubicación	Descripción
McScript.log	Depuración de McAfee Agent	*[Ruta de DATA del agente]\logs*	Contiene el resultado de los comandos de script utilizados durante el despliegue y la actualización del agente. A fin de activar el modo de depuración en este registro, establezca este valor de DWORD en la clave de Registro del cliente: *HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\TVD\SHARED COMPONENTS\FRAMEWORK\DWDEBUGSCRIPT=2.* NOTA: Elimine esta clave cuando haya finalizado la solución de problemas.
MFEAgent.msi. <system time stamp>.log	McAfee Agent	*%temp%\McAfeeLogs*	Contiene detalles sobre la instalación del archivo MSI del agente.
UpdaterUI_<sistema>.log	McAfee Agent	*%temp%\McAfeeLogs*	Contiene detalles sobre las actualizaciones de productos gestionados en el sistema cliente.

61. En el caso de *McAfee Endpoint Security*, todos los archivos de registro de actividades y depuración se almacenan en *%ProgramData%\McAfee\Endpoint Security\Logs.* La siguiente tabla muestra los archivos:

Función o tecnología	Nombre de archivo
Plataforma	*EndpointSecurityPlatform_Activity.log*
	EndpointSecurityPlatform_Debug.log
Autoprotección	*SelfProtection_Activity.log*
	SelfProtection_Debug.log
Actualizaciones	*PackageManager_Activity.log*
	PackageManager_Debug.log
Errores	*EndpointSecurityPlatform_Errors.log* Contiene registros de errores de todos los módulos.
Cliente de *Endpoint Security*	*MFEConsole_Debug.log*

5.11.2 ALMACENAMIENTO LOCAL

62. Toda la configuración de *McAfee ePO*, así como la información de amenazas, está alojada en dos (2) lugares: el directorio de instalación de *McAfee ePO* y la base de datos SQL de ePO.

5.11.3 ALMACENAMIENTO REMOTO

63. ePO puede reenviar los eventos de amenaza recibidos directamente a un servidor *syslog*, que se define en ePO como servidor registrado

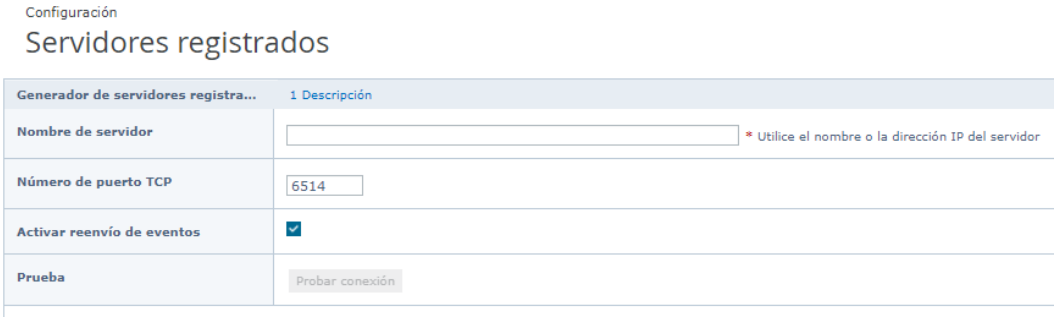

Ilustración 9. Configuración de servidor *syslog*

64. Adicionalmente, la mayoría de los fabricantes comerciales de soluciones SIEM incluyen una conexión nativa con McAfee ePO, por ejemplo, *McAfee Enterprise Security Manager.*

5.12 BACKUP

65. **Se deben realizar tareas de *backup* del entorno ePO**. Para ello, se requiere dos (2) pasos que deben ser sincronizados:

    a) Planificar la tarea de servidor llamada *Disaster Recovery Snapshot Server*, que se incluye por defecto con ePO, para que se ejecute en el horario más adecuado para la organización. Esta tarea vuelca toda la configuración del servidor ePO a la base de datos

    b) Planificar, aproximadamente 15 minutos después de la tarea de obtención del *snapshot* de ePO, el plan de mantenimiento de la base de datos recomendado por McAfee que incluye un *backup* de la misma y que se explica en el siguiente documento:

    https://kb.mcafee.com/corporate/index?page=content&id=KB67184

5.13 SERVICIOS DE SEGURIDAD

66. *McAfee Endpoint Security* es una solución de seguridad integrada y ampliable que protege servidores, sistemas de equipos, portátiles y tabletas contra amenazas conocidas y desconocidas. Las posibles amenazas incluyen *malware*, comunicaciones sospechosas, sitios web no seguros y archivos descargados.

67. Endpoint Security facilita que múltiples tecnologías de defensa se comuniquen en tiempo real para analizar y proteger contra amenazas. Consiste en estos módulos de seguridad:

    a) Prevención de amenazas: evita que las amenazas accedan a los sistemas, analiza los archivos automáticamente cuando se accede a ellos y ejecuta análisis dirigidos en busca de malware en los sistemas cliente.

    b) Firewall: supervisa la comunicación entre el equipo y los recursos de la red e Internet. Intercepta las comunicaciones sospechosas.

c) Control web: supervisa las búsquedas web y la actividad de navegación en los sistemas cliente y bloquea los sitios web y descargas según las calificaciones de seguridad y el contenido.

d) Protección adaptable frente a amenazas: analiza el contenido de su empresa y decide cómo responder en función de la reputación de los archivos, las reglas y los umbrales de reputación. Protección adaptable frente a amenazas es un módulo opcional de Endpoint Security.

68. El módulo '*Ajustes Generales*' proporciona la configuración para las funciones comunes, tales como la seguridad de interfaz y el registro. Este módulo se instala automáticamente si se instala cualquier otro módulo.

69. Todos los módulos se integran en una única interfaz de *Endpoint Security* en el sistema cliente. Cada módulo funciona conjuntamente e independiente para proporcionar varios niveles de seguridad.

70. Las características clave de **Prevención de amenazas** protegen el entorno de amenazas y *malware* y corrigen problemas limpiando o reparando los archivos infectados.

    a) Protección – Protege los sistemas frente a intrusiones antes de que otros accedan al entorno con estas funciones.

        i. Protección de acceso: protege los sistemas cliente de cambios no deseados restringiendo el acceso a determinados archivos, datos compartidos y claves y valores de Registro, además de evitar o restringir la ejecución de procesos y servicios que representen una amenaza.

        ii. Prevención de *exploits*: Prevención de amenazas utiliza firmas en las actualizaciones de contenido para proteger frente a los siguientes exploits:

            1. Protección contra desbordamiento de búfer: impide la ejecución de código arbitrario debido a desbordamientos del búfer.

            2. Uso no válido de API: impide que aplicaciones desconocidas o comprometidas que se ejecutan en el sistema realicen llamadas maliciosas a la API.

            3. Prevención de intrusiones en la red (IPS de red): impide los ataques de denegación de servicio en la red y los relacionados con el ancho de banda que deniegan o reducen el tráfico de la red.

            4. Reglas expertas: proporciona parámetros adicionales y permite una flexibilidad superior a la de las reglas personalizadas de Protección de acceso. Sin embargo, para crear reglas expertas, hay que familiarizarse con la sintaxis específica de McAfee.

    b) Detección - Detecta amenazas cuando se produzcan en el entorno.

i. Análisis en tiempo real: analiza en busca de amenazas mientras se leen archivos en el disco o se escriben en este. Realiza análisis únicamente cuando el sistema esté inactivo. Se integra con la interfaz de análisis antimalware (AMSI) para proporcionar un análisis mejorado en busca de amenazas en scripts no basados en navegador.

ii. Análisis bajo demanda: ejecuta y planifica análisis predefinidos, lo que incluye análisis para detectar entradas de Registro relacionadas con spyware que no se limpiaron anteriormente.

iii. Programas potencialmente no deseados: detecta programas potencialmente no deseados, como *spyware* y *adware*, e impide que se ejecuten en el entorno.

iv. Cuarentena: pone en cuarentena los elementos infectados e intenta limpiarlos o repararlos. También puede eliminarlos automáticamente.

v. Paneles y monitores: permite consultar estadísticas sobre Prevención de amenazas, lo que incluye información sobre la duración de los análisis, el estado de actualización del contenido y las aplicaciones con más exploits.

vi. Consultas e informes: permite obtener información detallada sobre Prevención de amenazas, como el número de amenazas, los análisis finalizados, la respuesta de detección, los eventos de mitigación de falsos positivos y el nivel de sensibilidad de *McAfee GTI*.

vii. *Antimalware* de inicio al arranque: complementa la función ELAM de Windows 8 y versiones posteriores. ELAM obtiene la lista de controladores de dispositivo cargados durante el ciclo de arranque y los analiza una vez que se ejecuten los servicios de análisis.

c) Corrección - Corrige problemas de seguridad, controla las detecciones, mejora el rendimiento y optimiza la protección

i. Acciones: realiza la acción especificada cuando se produzcan las detecciones.

ii. Alertas: notifica las detecciones cuando se produzcan y limita el tráfico mediante filtros.

iii. Archivos *Extra.DAT*: protegen frente a nuevas amenazas, como un ataque de virus importante.

iv. Análisis planificados: realiza análisis en momentos de poca actividad para mejorar el rendimiento del sistema y del análisis.

v. Repositorios de contenido: reduce el tráfico de red que soportan las redes intranet e Internet de la empresa trasladando el repositorio de archivos de contenido a una ubicación más próxima a los sistemas cliente.

vi. Archivos de registro (Cliente de *Endpoint Security*): permiten consultar un historial de elementos detectados, que se pueden utilizar para determinar si es necesario cambiar la configuración para mejorar la protección o el rendimiento del sistema.

vii. Paneles y monitores: supervisan la actividad y utilizan esa información para ajustar la configuración de Prevención de amenazas.

71. Las funciones clave de ***Control web*** protegen los sistemas frente a amenazas basadas en web, detectan amenazas y corrigen problemas con las descargas de archivos.

a) Protección – Protege los sistemas de las descargas y los sitios web maliciosos:

i. Lista de bloqueos y permisos: impide que los usuarios visiten URL o dominios específicos, o bien permite siempre el acceso a sitios que sean importantes para la empresa.

ii. Acciones de calificación y bloqueo de categorías web: utiliza las calificaciones de seguridad y las categorías web definidas por McAfee para controlar el acceso de los usuarios a sitios, páginas y descargas.

iii. Búsqueda segura: bloquea sitios peligrosos automáticamente para que no se muestren en los resultados de búsqueda de acuerdo con la calificación de seguridad.

iv. Autoprotección: evita que los usuarios desactiven el complemento Control web o que desinstalen o cambien los archivos, las claves y los valores de Registro, los servicios y los procesos de Control web.

b) Detección – Detecta los sitios web maliciosos:

i. Botón Control web de la ventana del navegador: el complemento Control web muestra un botón que indica la calificación de seguridad del sitio. Haciendo clic en el botón se obtiene más información sobre el sitio.

ii. Icono Control web en las páginas de resultados de búsqueda: aparece un icono junto a cada sitio de la lista. El color del icono indica la calificación de seguridad del sitio web. Pasando el cursor sobre el icono se obtiene más información sobre el sitio.

iii. Informes del sitio: se muestran detalles sobre cómo se ha calculado la calificación de seguridad según los tipos de amenaza detectados, los resultados de la prueba y otros datos.

iv. Paneles y monitores: permiten consultar estadísticas sobre la actividad de Control web, lo que incluye las visitas y las descargas de los sitios según su calificación, el tipo de contenido y la lista de permitidos o bloqueados.

v. Consultas e informes: permiten obtener información detallada sobre los eventos de navegador de Control web y guardarlo en los informes.

c) Corrección – Supervisar y ajustar el comportamiento de Control web:

i. Interbloqueo con otros productos de McAfee: *Control web* se desactiva automáticamente si se detecta un *appliance* de gateway web, o si *McAfee Client Proxy* está instalado y se encuentra en modo de redirección.

ii. Análisis de archivos descargados: *Control web* envía archivos a Prevención de amenazas para el análisis. Si se detecta una amenaza, Prevención de amenazas responde con una acción configurada, como limpiar, y avisar al usuario.

iii. Paneles y monitores: permiten supervisar la actividad de navegación y, a continuación, utiliza esa información para ajustar la configuración de *Control web*.

iv. Exclusiones: evitan que *Control web* califique o bloquee direcciones IP específicas.

72. Las funciones clave de **Firewall** protegen frente a amenazas, detectan problemas de seguridad y corrigen falsos positivos.

a) Protección - Proteja su red y las aplicaciones con estas funciones de Firewall:

i. Reglas: definen los criterios que utiliza *Firewall* para determinar si bloquear o permitir el tráfico entrante y saliente.

ii. Grupos de reglas: organizar las reglas de *firewall* para realizar tareas de administración de forma sencilla aplicando reglas de forma manual o planificada y procesar el tráfico únicamente en función del tipo de conexión.

iii. Filtrado e inspección de paquetes con seguimiento de estado: realiza un seguimiento del estado de conexión de la red y las características mediante una tabla de estados para permitir únicamente paquetes que coincidan con una conexión abierta conocida.

iv. Control basado en la reputación: bloquea archivos ejecutables que no sean de confianza o todo el tráfico de una red que no sea de confianza, en función de la reputación.

b) Detección – Detectar problemas de seguridad:

i. Paneles y monitores: consultar los eventos de intrusión y detección de *McAfee GTI* y *Firewall*.

ii. Consultas e informes: obtener información detallada sobre *Firewall*, incluidos errores, reglas de cliente y eventos de intrusión y bloqueo, e incluir esa información en informes.

iii. Alertas: consultar alertas de tráfico bloqueado, en función de la reputación de la red o el archivo ejecutable.

iv. Registro de tráfico: registra todo el tráfico bloqueado o permitido.

c) Corrección - Reducir o eliminar los falsos positivos:

i. Modo de adaptación: crea reglas automáticamente en el sistema cliente para permitir la actividad legítima. Una vez creadas las reglas de cliente, se analizan y se decide cuáles de ellas debe convertir en directivas impuesta por el servidor.

ii. Redes definidas: definir redes de confianza para permitir el tráfico de las redes que la organización considere como seguras.

iii. Archivos ejecutables de confianza: mantener una lista de archivos ejecutables seguros para reducir la cantidad de falsos positivos.

iv. Catálogo de *Firewall*: definir las reglas y los grupos que se agregarán a varias directivas, o bien las redes y las aplicaciones que se agregarán a las reglas de firewall.

v. Opciones de cliente: permite a los usuarios desactivar Firewall temporalmente para solucionar problemas.

vi. Paneles y monitores: supervisan la actividad y las intrusiones detectadas y, a continuación, se utiliza esa información para ajustar la configuración de *Firewall*.

73. Las características clave de **Protección adaptable frente a amenazas** protegen la empresa de los archivos de reputación desconocida, detectan patrones maliciosos y corrigen falsos positivos.

a) Protección - Protege la empresa bloqueando o conteniendo archivos de reputación desconocida:

i. Control de archivos basado en la reputación: Protección adaptable frente a amenazas avisa cuando un archivo desconocido entra en el entorno. En lugar de enviar la información del archivo a McAfee para su análisis, Protección adaptable frente a amenazas puede bloquear el archivo de inmediato.

ii. Integración con el servidor de TIE: si está disponible, el servidor de TIE proporciona información sobre cómo se ha ejecutado el archivo en varios sistemas. *Advanced Threat Defense* ayuda a determinar si el archivo es una amenaza.

iii. Contención dinámica de aplicaciones: permite que los archivos desconocidos se ejecuten en un contenedor, por lo que se limitan las acciones que estos pueden realizar. La primera vez que una empresa utiliza un archivo cuya reputación se desconoce, Protección adaptable frente a amenazas puede ejecutarlo en un contenedor. Las reglas de contención definen las acciones que no puede realizar la aplicación

contenida. La Contención dinámica de aplicaciones también contiene procesos cuando estos cargan archivos PE (ejecutables de tipo portable) y DLL (bibliotecas de enlace dinámico) que reduzcan la reputación del proceso.

b) Detección - Detectar patrones maliciosos y *malware* en la memoria:

   i. Análisis de *Real Protect*: realiza un análisis de reputación automatizado. *Real Protect* inspecciona archivos y actividades sospechosos en sistemas cliente para detectar patrones maliciosos mediante técnicas de aprendizaje automático. Los análisis de Real Protect basados en cliente y en la nube incluyen el análisis de archivos DLL para evitar que los procesos de confianza carguen archivos PE y DLL que no sean de confianza.

c) Corrección - Limpiar archivos y eliminar falsos positivos:

   i. Limpieza de archivos: Protección adaptable frente a amenazas puede limpiar archivos cuando la reputación de éstos alcance un umbral determinado.

   ii. Exclusión de archivos personalizados: si un archivo personalizado es de confianza, pero tiene reputación de archivo malicioso de forma predeterminada, este queda bloqueado. Se puede excluir del análisis o cambiar la reputación del archivo para que sea de confianza y permitir que se ejecute en la organización sin solicitar un archivo DAT actualizado de McAfee.

   iii. Paneles e informes de *McAfee ePO*: se muestran detecciones y actividad, que se puede utilizar para ajustar la configuración de Protección adaptable frente a amenazas.

6. FASE DE OPERACIÓN

74. McAfee recomienda realizar ciertas tareas de forma diaria, semanal y mensual para garantizar que los sistemas gestionados estén protegidos y que el servidor de McAfee ePO funcione de forma eficiente.

75. Como todas las redes son distintas, cada entorno puede requerir pasos más detallados o solamente algunos de los pasos descritos en esta sección.

76. Las **tareas diarias** que deben ser realizadas para asegurar el uso seguro del producto son las siguientes:

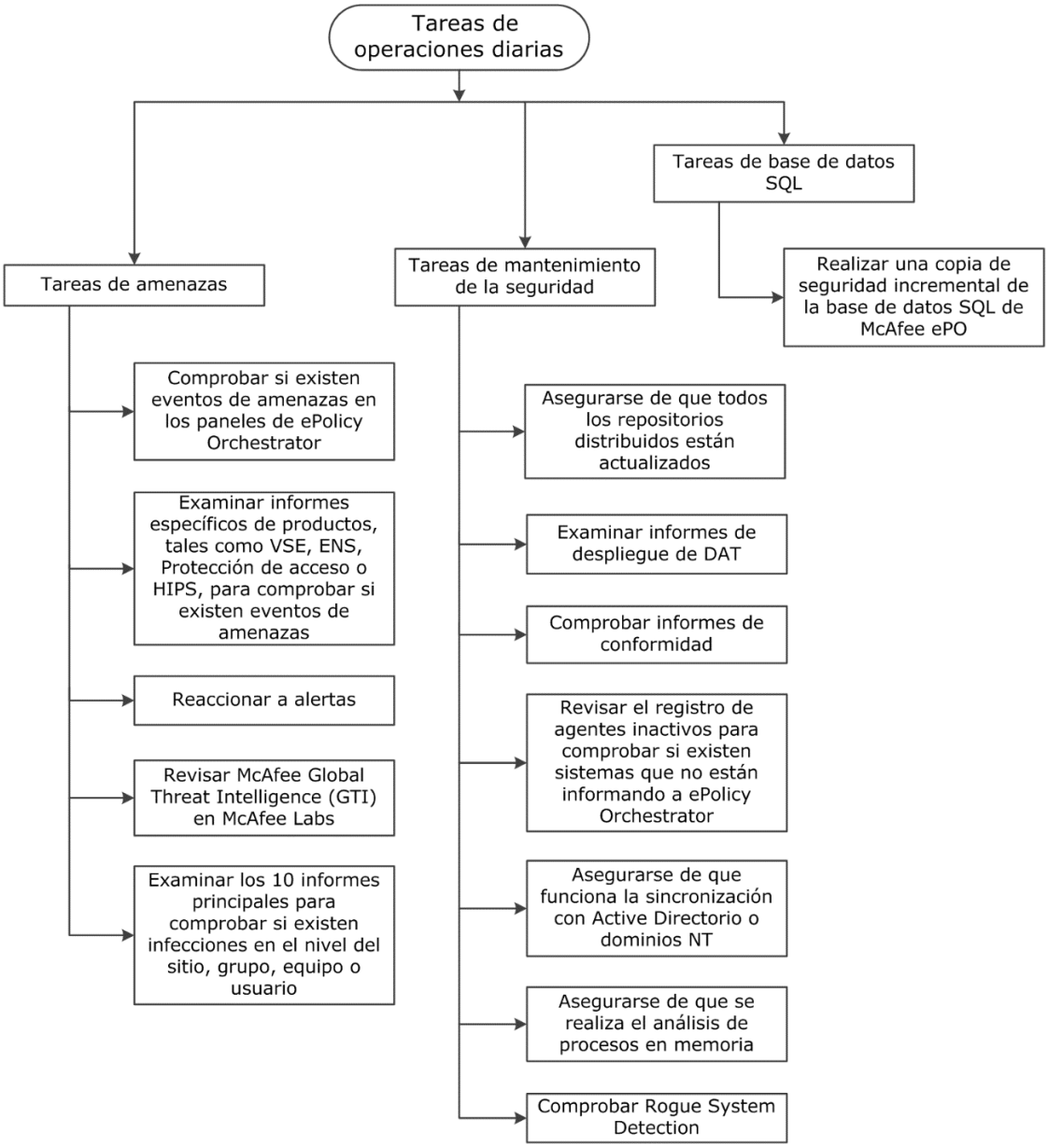

Ilustración 10. Tareas diarias

Tarea	Descripción
Tareas diarias frente a amenazas	
Comprobar los paneles de *McAfee ePO* en busca de eventos de amenaza	A lo largo del día, revisar los paneles en busca de amenazas, detecciones y tendencias. **NOTA:** Configurar respuestas automáticas para enviar mensajes de correo electrónico a los administradores cuando se alcancen los umbrales de actividad de las amenazas.
Examinar informes específicos de productos, como *VirusScan Enterprise, Endpoint Security*, protección de acceso o *McAfee Host IPS* en busca de eventos de amenaza	Examinar los informes en busca de eventos que puedan indicar una nueva vulnerabilidad en el entorno. Crear una tarea servidor para planificar consultas y recibir los resultados. Con estos datos, se podría crear directivas o editar las existentes.
Reaccionar ante las alertas	Si se detectan alertas nuevas, seguir el procedimiento interno de la empresa para gestionar el *malware*. Recopilar y enviar muestras a McAfee, además de limpiar el entorno. Asegurarse de que los archivos de firmas estén actualizados y ejecutar análisis bajo demanda cuando proceda. Véase '*Procedimiento para resolver problemas y buscar archivos que pueden estar infectados*', *KB53094*. Ejecutar consultas o revisar los paneles periódicamente para ver si se han recopilado alertas de los dispositivos gestionados. Buscar también las siguientes señales de alerta: • Uso intensivo de la CPU en procesos indeterminados • Aumentos inesperados del tráfico de red • Servicios añadidos o eliminados por otras personas • Imposibilidad de acceso a la red o a los recursos compartidos administrativos • Aplicaciones o archivos que dejan de funcionar • Adición de claves de registro desconocidas para iniciar una aplicación • Cualquier página de inicio del navegador

Tarea	Descripción
	cambiada sin su conocimiento • Archivos creados o cambiados en un endpoint (revisar Reglas de protección de acceso).
Revisar la página de *McAfee Global Threat Intelligence (McAfee GTI)* en el sitio de amenazas de McAfee Labs **al menos una vez al día**	Para acceder al sitio de amenazas de McAfee Labs, seleccionar *Menú* → *Informes* → *Paneles*. Seleccionar el panel Resumen de ePO y, en Vínculos de McAfee, hacer clic en *Global Threat Intelligence.*
Examinar los informes de tipo "*top 10*" en busca de infecciones en el nivel de sitio, grupo, sistema y usuario	*McAfee ePO* proporciona informes preconfigurados de tipo "*top 10*" que muestran estadísticas sobre las infecciones en el entorno. Determinar qué usuarios, sistemas y partes de la red tienen más infecciones o vulnerabilidades. Estos informes podrían revelar debilidades en la red que impliquen ajustar las directivas.
Tareas de mantenimiento diarias de seguridad	
Examinar los informes de despliegue de archivos DAT	Es importante que exista un despliegue del 100 % de los archivos DAT más recientes en todos los sistemas gestionados. Es necesario asegurarse que los clientes dispongan de una tarea de actualización configurada para que se ejecute varias veces al día a fin de mantener actualizados los archivos DAT. Ejecutar la consulta Prevención de amenazas de *Endpoint Security*: Estado de conformidad de *AMCore Content* con frecuencia a lo largo del día para asegurarse de que los sistemas están ejecutando los archivos DAT más recientes.
Comprobar las consultas y los informes de conformidad	En '*Consultas e informes*', localizar las consultas de conformidad que identifican los sistemas que no han actualizado la versión de un producto gestionado con un motor, un *hotfix* o una actualización. Crear un proceso para asegurarse de que los sistemas están actualizados. Por ejemplo, ejecutar una tarea de actualización o despliegue para garantizar la conformidad.
Revisar el registro de agentes inactivos para determinar qué	En *'Tareas servidor'*, ejecutar la tarea de '*limpieza de agentes inactivos'*. Esta tarea identifica los sistemas

Tarea	Descripción
sistemas no se están comunicando con McAfee ePO	que no se han conectado con el servidor de *McAfee ePO* durante un número concreto de días, semanas o meses. Se puede utilizar esta tarea para mover los sistemas inactivos a un grupo nuevo en el Árbol de sistemas, etiquetar los sistemas, eliminar los sistemas o enviar un informe por correo electrónico. Si los sistemas están en la red, pero hay algún problema al incorporarlos en el servidor de *McAfee ePO*, llevar a cabo una de estas acciones: • Utilizar un Agente de *ping* o una Llamada de activación del agente para comprobar si un sistema está en línea y llevar a cabo una comunicación agente-servidor con el servidor de *McAfee ePO*. • Volver a instalar *McAfee Agent* para asegurarse de que el sistema se comunica con el servidor de *McAfee ePO*.
Asegurarse de que la sincronización con *Active Directory* o NT funciona	La sincronización con *Active Directory* o Dominio NT inserta una lista de nuevos sistemas y contenedores que *McAfee ePO* debe administrar. Si se utilizan, confirmar que la tarea de sincronización esté configurada para ejecutarse al menos una vez al día y asegurarse de que funcione. **ATENCIÓN:** Si la sincronización falla, los sistemas son vulnerables en la red y representan un riesgo importante de infección.
Confirmar que hay al menos un Análisis de procesos de memoria **a diario**	Mediante el *Panel de amenazas*, confirmar que los resultados de estos análisis no indican un aumento de las amenazas. **SUGERENCIA:** Ejecutar análisis de procesos de memoria con frecuencia, ya que son rápidos y discretos.
Comprobar Rogue System Detection	*Rogue System Detection* indica qué dispositivos están conectados a la red. Informa de los sistemas no gestionados, por lo que pueden encontrarse y desconectarse de la red rápidamente.
Tareas de bases de datos SQL diarias	

Tarea	Descripción
Crear una copia de seguridad incremental de la base de datos de *McAfee ePO*	Utilizar el Administrador corporativo de SQL Server de *Microsoft* para crear la copia de seguridad de la base de datos de *McAfee ePO*. Verificar que la copia de seguridad se haya creado correctamente una vez finalizada. **NOTA:** Se puede utilizar la función *'Recuperación de desastres'* de *McAfee ePO* para crear una instantánea de los registros en la base de datos de *McAfee ePO* a fin de recuperar o reinstalar el *software* con rapidez, si procede.

77. **Tareas semanales** que deben ser realizadas para asegurar el uso seguro del producto:

Tarea	Descripción
Tareas semanales de *McAfee ePO*	
Comprobar la existencia de actualizaciones, extensiones y *hotfixes* de los productos de McAfee en el sitio web de McAfee o a través del Catálogo de *software*	McAfee publica periódicamente actualizaciones y *hotfixes*, así como actualizaciones de archivos DAT y del motor. Comprobar el sitio web de McAfee y el *Catálogo de software* de *McAfee ePO* con frecuencia en busca de nuevas actualizaciones que incorporar a la consola de *McAfee ePO* para pruebas en el entorno local. También se puede utilizar el *Catálogo de software* para descargar e incorporar estas actualizaciones. **NOTA:** Los archivos DAT y del motor no se actualizan con el *Catálogo de software*.
Ejecutar una replicación completa en todos los repositorios distribuidos	Los repositorios distribuidos se pueden dañar debido a una tarea de replicación incompleta. Eliminar los archivos dañados de los repositorios mediante la ejecución de una replicación completa en todos los repositorios distribuidos una vez por semana. Las tareas de replicación completa eliminan el contenido existente en el repositorio y lo sustituyen por archivos nuevos. **NOTA:** Las tareas de replicación incremental solo copian los archivos nuevos o no existentes, pero

Tarea	Descripción
	no corrigen los archivos dañados.
Ejecutar *'Estado de repositorios distribuidos'*	Seleccionar *Menú* → *Informes* → *Consultas e informes*. Localizar y ejecutar el informe Estado de repositorios distribuidos para determinar si se han producido fallos en la actualización de los repositorios distribuidos. Si existen fallos, ejecutar de nuevo la replicación y asegurarse de que no vuelva a fallar.
Planificar un análisis bajo demanda de todos los sistemas del entorno	Planificar un análisis bajo demanda de todos los sistemas del entorno que se ejecute durante las horas no laborables. Véanse estos documentos para obtener más información: • Para ver los procedimientos recomendados para el análisis bajo demanda *en McAfee Endpoint Security*, consultar *https://kc.mcafee.com/corporate/index?page=content&id=KB74059*. • Para averiguar cómo crear un informe de *McAfee ePO* del evento 1203 (análisis bajo demanda completado), consultar *https://kc.mcafee.com/corporate/index?page=content&id=KB69428*.
Tareas de bases de datos SQL semanales	
Crear una copia de seguridad de la base de datos SQL de *McAfee ePO*	Utilizar el Administrador corporativo de *SQL Server* de Microsoft para crear la copia de seguridad de la base de datos de *McAfee ePO*. Verificar que la copia de seguridad se haya creado correctamente una vez finalizada. **NOTA:** Se puede utilizar la función Recuperación de desastres de *McAfee ePO* para crear una instantánea de los registros en la base de datos de *McAfee ePO* a fin de recuperar o reinstalar el software con rapidez, si procede.

Tarea	Descripción
Tareas semanales del sistema operativo *Windows Server*	
Eliminar los sistemas inactivos de *Active Directory*	*Active Directory* inserta una lista de nuevos sistemas y contenedores que *McAfee ePO* debe administrar. Confirmar que la tarea de sincronización esté configurada para ejecutarse al menos una vez al día y asegúrese de que funcione. **ATENCIÓN:** Si la sincronización falla, los sistemas son vulnerables en la red y representan un riesgo importante de infección.

78. **Tareas mensuales** que deben ser realizadas para asegurar el uso seguro del producto:

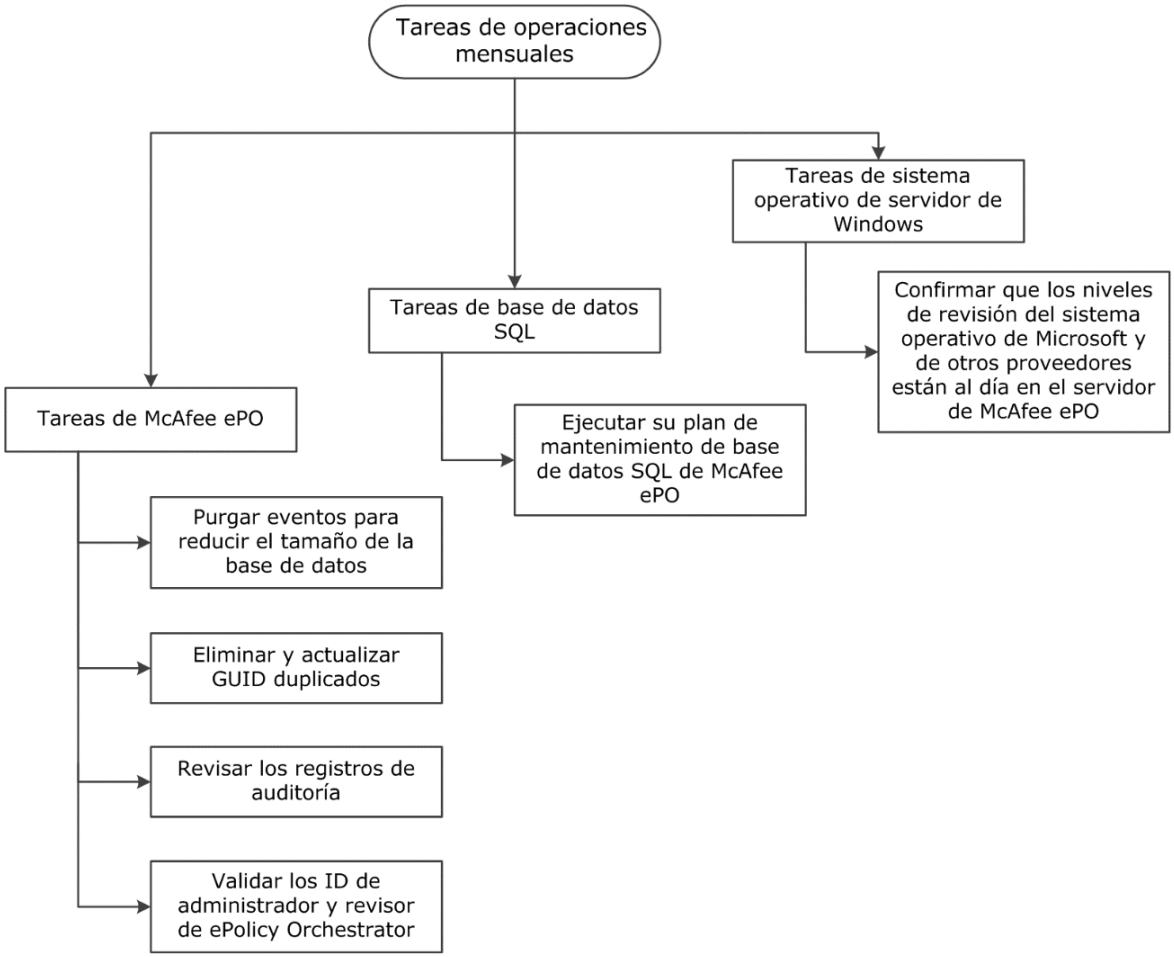

Ilustración 11. Tareas mensuales

Tarea	Descripción
Tareas mensuales de McAfee ePO	
Purgar los eventos para reducir el tamaño de la base de datos	Purgar los eventos automáticamente.
Eliminar y actualizar los GUID duplicados	Ejecutar las tareas de servidor de GUID de agente duplicado para localizar y corregir los GUID duplicados en el entorno. Además, ejecutar estas tareas servidor en función del resultado: • GUID de agente duplicado: borrar el recuento de errores • GUID de agente duplicado: eliminar los sistemas con posibles GUID duplicados
Revisar los registros de auditoría	Revisar los registros de auditoría de *McAfee ePO* para asegurarse de que las personas con privilegios de administración solo realicen cambios aprobados en configuraciones, tareas y directivas del sistema.
Validar el administrador de *McAfee ePO* y los identificadores de revisor	Confirmar que solo los empleados autorizados para tener acceso administrativo tienen identificadores configurados correctamente, con los conjuntos de permisos adecuados en el sistema de *McAfee ePO*.
Tareas de bases de datos SQL	
Ejecutar el plan de mantenimiento de la base de datos SQL de *McAfee ePO*	Configurar y ejecutar el plan de mantenimiento mensual de SQL: *https://kc.mcafee.com/corporate/index?page=content&id=KB67184*
Tareas mensuales del sistema operativo Windows Server	
Confirmar que el sistema operativo de	Revisar e implementar todas las actualizaciones de *Microsoft* para eliminar vulnerabilidades y mitigar los

Tarea	Descripción
Microsoft y otros niveles de actualización de proveedores en el servidor de McAfee ePO están actualizados.	riesgos. **NOTA:** También podrían publicarse otras actualizaciones de proveedores. Esta actualización es necesaria para reducir las vulnerabilidades en el entorno.

79. Se deben realizar también **periódicamente** las siguientes tareas:

Tarea	Descripción
Evaluar el entorno, las directivas y las asignaciones de directivas de forma periódica para confirmar que sigan siendo aplicables	Las necesidades de la organización pueden cambiar, por lo que es necesario revisar periódicamente tanto las directivas existentes como las asignaciones de directivas para garantizar que sigan teniendo sentido en el entorno. Un menor número de directivas simplifica la administración del servidor.
Revisar las tareas cliente y las asignaciones de tareas existentes de forma periódica para confirmar que siguen siendo necesarias	Las tareas cliente ejecutan análisis, despliegan actualizaciones de productos, parches de productos y *hotfixes*, etc. en los sistemas gestionados por *McAfee ePO*. Eliminar las tareas no utilizadas para reducir la complejidad del sistema, lo cual puede afectar en última instancia al tamaño de la base de datos.
Revisar las etiquetas y los criterios de etiquetado existentes para garantizar que sigan siendo relevantes en el entorno	Usar las etiquetas como alternativa a los grupos del Árbol de sistemas a fin de combinar o seleccionar un grupo de sistemas sobre el que operar. Por ejemplo, para enviar actualizaciones, desplegar productos gestionados de McAfee o ejecutar análisis. El etiquetado resulta útil, pero es necesario supervisar las etiquetas para asegurarse de que tengan utilidad y el efecto necesario.
Revisar las exclusiones de productos (por ejemplo, *Endpoint Security*) y las inclusiones/exclusiones (por ejemplo, las reglas de	Las exclusiones deben ser lo más específicas posible dentro del entorno. Los cambios de productos pueden afectar a las exclusiones configuradas. Revisar las exclusiones

Tarea	Descripción
protección de acceso) periódicamente para validar su relevancia	periódicamente para asegurarse de que sigan ofreciendo el resultado necesario. Además, se pueden utilizar las configuraciones de riesgo alto y bajo de los análisis en tiempo real para potenciar las exclusiones. Estructurar el Árbol de sistemas o bien emplear las etiquetas como método alternativo para controlar las exclusiones.
Realizar cambios de *hardware* o eliminar repositorios que es necesario retirar del servicio	A medida que cambien la red y la organización, es posible que cambiar la ubicación y el tipo de los repositorios utilizados ofrezca una cobertura más eficiente y efectiva.
Validar que se dispone del *software* necesario, como puede ser la versión más reciente de *McAfee Agent*	Utilizar siempre la versión más reciente de los productos gestionados de McAfee para garantizar que exista disponible soporte técnico para dichos productos. Además, se dispondrá de las funciones y correcciones más recientes.
Eliminar el *software* no admitido o el *software* correspondiente a productos que no se utilizan del Repositorio principal y los repositorios distribuidos	Limitar el uso de espacio en el disco y descongestionar el servidor de *McAfee ePO* y los repositorios distribuidos. Conservar solo los productos utilizados actualmente en el entorno en el Repositorio principal.
Validar el Árbol de sistemas y eliminar los agentes que no se hayan comunicado con el servidor de *McAfee ePO* en 30 días o que se hayan retirado del servicio	Mantener el Árbol de sistemas organizado y eliminar los sistemas que ya no se utilicen o no se comuniquen con *McAfee ePO*. Un Árbol de sistemas limpio garantiza que los informes no incluyan información no pertinente. Configurar una tarea servidor para eliminar los sistemas inactivos.
Eliminar las tareas servidor que ya no se utilizan	Conservar solo las tareas servidor que se pretenda utilizar en la lista de tareas. Siempre se puede desactivar una tarea no utilizada que se desee conservar pero que no se emplee de forma

Tarea	Descripción
	regular. Limitar al mínimo la lista de tareas que se usan regularmente reduce la complejidad de *McAfee ePO*.
Eliminar las Respuestas automáticas que ya no son relevantes	Las respuestas automáticas se configuran para alertar a personas, especialmente a los administradores de sistemas, cuando es necesario resolver amenazas provocadas por eventos de malware, amenazas de clientes o problemas de conformidad.
Eliminar sistemas de *shell* que empleen una tarea servidor de McAfee ePO	Eliminar los sistemas con propiedades de sistema y producto incompletas o ausentes del Árbol de sistemas. Estos sistemas distorsionan los informes y las consultas, además de desperdiciar espacio en la base de datos de *McAfee ePO*.
Supervisar el tamaño de la base de datos	Comprobar el tamaño de la base de datos de *McAfee ePO* y determinar si es necesario purgar los eventos enviados a *McAfee ePO* y con qué frecuencia. Para purgar los eventos de la base de datos, véase *https://kc.mcafee.com/corporate/index?page=content&id=KB68961* y el procedimiento de purga del *Registro de auditoría*, el *Registro de tareas servidor* y el *Registro de eventos de amenazas*.

7. CHECKLIST

1. A continuación, se presenta una *checklist* que contiene todas las recomendaciones sobre la configuración de seguridad del producto.

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Recepción del *Grant Letter*	☐	☐	Carta en la que aparece el número de concesión y los productos adquiridos
Validar acceso a zona de descargas	☐	☐	Acceder a *https://www.mcafee.com/enterprise/en-us/downloads/my-products.html* con el número de concesión y un email válido
Descarga de extensiones y paquetes de instalación	☐	☐	Desde la zona de descargas obtener los elementos indicados en el párrafo 13
Ubicación de servidores	☐	☐	Confirmar que los servidores de la arquitectura se ubican en lugar seguro
Se requieren *Agent Handlers*	☐	☐	Determinar el uso de *Agent Handlers* adicionales, bien en DMZ, bien en red interna
Se cumplen los requisitos de ePO	☐	☐	Validar requisitos *hardware*, *software* y de la base de datos
Se cumplen los de Endpoint Security	☐	☐	Validar requisitos *hardware* y *software* según plataforma
Definir método de distribución del agente	☐	☐	Elegir el método o métodos más adecuados entre los disponibles
Seleccionar módulos de *Endpoint Security* a desplegar	☐	☐	En función de las características de cada máquina se puede elegir que módulos de Endpoint Security desplegar
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado (FIPS-CC)	☐	☐	Activar el despliegue en modo FIPS
Modificar certificado SSL de consola ePO	☐	☐	Seguir el procedimiento definido para usar un certificado SSL propio
Método de autenticación de usuarios	☐	☐	Determinar si los usuarios autenticarán mediante db local, LDAP o certificado
Control de acceso a consola	☐	☐	Definir los controles de acceso a la consola ePO
Definición de usuarios	☐	☐	Crear usuarios con el rol adecuado manteniendo la lista siempre actualizada

ACCIONES	SÍ	NO	OBSERVACIONES
Uso de TLS v1.2	□	□	Confirmar que v1.0 y v1.1 de TLS están desactivados
Arquitectura de actualizaciones	□	□	Definir si es necesario el despliegue de repositorios distribuidos o es suficiente con la funcionalidad *peer-to-peer* de *McAfee Agent*
Backup	□	□	Confirmar la configuración del plan de mantenimiento de la base de datos de ePO

8. REFERENCIAS

KB51569	Plataformas compatibles con *ePolicy Orchestrator*
KB91326	Plataformas compatibles con *Endpoint Security* for *Linux Firewall*
KB87073	Plataformas compatibles con *Endpoint Security for* Linux Prevención de amenazas
KB84934	Plataformas compatibles con *Endpoint Security* para Mac
KB66797	Requisitos de puerto de *ePolicy Orchestrator* para tráfico firewall
KB72477	Cómo generar un certificado SSL personalizado para su uso con ePO mediante *OpenSSL Toolkit*
ePO WebAPI	https://docs.mcafee.com/es-ES/bundle/epolicy-orchestrator-web-api-reference-guide/page/GUID-D87A6839-AED2-47B0-BE93-5BF83F710278.html#
KB86318	Declaración de mantenimiento de *ePolicy Orchestrator* (SSC1512011)-compatibilidad con *Transport Layer Security 1.2*
KB67184	Plan de mantenimiento recomendado para las bases de datos de *ePolicy Orchestrator* con *SQL Server Management Studio*
KB53094	Solución de problemas para encontrar los posibles archivos infectados si no se detecta un virus
KB74059	Prácticas recomendadas para los análisis bajo demanda
KB69428	Create an ePolicy Orchestrator report for the event: 1203 (*on-demand scan completed*)
KB68961	Cómo encontrar los diez principales eventos de amenazas y Purgar eventos

9. ABREVIATURAS

CRL	*Certificate Revoation List*
EDR	*Endpoint Detection Response*
ePO	*ePolicy Orchestrator*
EPP	*Endpoint Protection Platform*
GTI	*Global Threat Intelligence*
LDAP	*Light Directory Access Protocol*
OCSP	*Online Certificate Status Protoco*
SIEM	*Security Information and Event Management*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL