centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1503

Procedimiento de empleo seguro McAfee Data Loss Prevention 11.1 con ePolicy Orchestrator 5.10

Febrero de 2021

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

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
2021.02.24 15:59:40 +01'00'

NIPO: 083-21-046-8

Fecha de Edición: febrero de 2021
McAfee ha participado en la realización y modificación del presente documento

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Febrero de 2021

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1 INTRODUCCIÓN

1. La fuga de datos se produce cuando sale información sensible o privada de una organización como resultado de comunicaciones no autorizadas a través de canales tales como aplicaciones, dispositivos físicos y protocolos de red.
2. McAfee Data Loss Prevention (McAfee DLP) es un paquete de productos que protege una red de 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 una red, cómo se accede a ellos, cómo se transmiten y si contiene información sensible. El uso de McAfee DLP favorece la creación e implementación de directivas de protección eficaces a la vez que se reduce la necesidad de un amplio proceso de ensayo y error.
3. McAfee DLP Endpoint proporciona protección integral para todos los posibles canales de fuga de datos, como dispositivos de almacenamiento extraíbles, la nube, correo electrónico, mensajería instantánea, Web, material impreso, portapapeles, capturas de pantalla, aplicaciones para compartir archivos, etc.
4. Sus principales características son:
    1) Integración con análisis de comportamientos de usuarios (UEBA) de terceros.
    2) Clasificación manual.
    3) Análisis y reparaciones iniciados por el usuario.
    4) Clasificación flexible, que ofrece diccionarios, expresiones regulares y algoritmos de validación.
    5) Una exclusiva tecnología de etiquetado para identificar los documentos según su origen, que impide que la información sensible que manejan las aplicaciones web, las aplicaciones de red y los recursos compartidos de red se duplique, renombre o salga de las instalaciones de la empresa.
    6) Compatibilidad con tecnologías de virtualización para proteger equipos de sobre mesa remotos y soluciones VDI.

2 OBJETO Y ALCANCE

5. La configuración evaluada del producto y por lo tanto incluida en la presente guía de empleo seguro consiste en una instancia única del sistema de gestión (con *ePolicy Orchestrator*, las extensiones para DLP y la extensión de *McAfee Agent*), *Discover, Prevent, Monitor,* y una o más instancias de sistemas gestionados (con *McAfee Agent, Endpoint client* y *Device Control*).
6. Los componentes que conforman el producto son los siguientes:
   1) McAfee Data Loss Prevention 11.1.x
   2) McAfee Data Loss Prevention Monitor 11.1.x
   3) McAfee Data Loss Prevention Prevent 11.1.x
   4) McAfee Data Loss Prevention Discover 11.1.x
   5) McAfee Data Loss Prevention Endpoint 11.1.x
   6) McAfee ePolicy Orchestrator 5.10.0
   7) McAfee Agent 5.5.1
7. Estos componentes quedan reflejados en el siguiente diagrama, donde se puede ver, delimitado en rojo, los componentes que forman el producto.

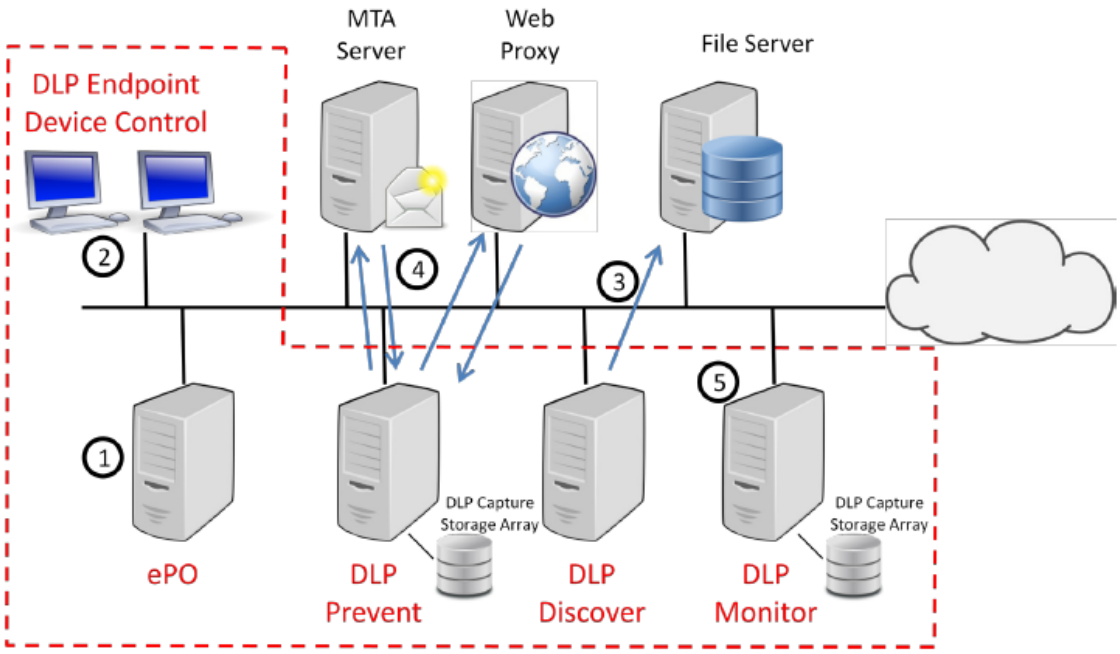

Ilustración 1. Componentes del producto.

8. Donde se puede distinguir las siguientes funcionalidades de cada una de las partes mencionadas:

1) **ePO**. ePolicy Orchestrator gestiona la configuración de la política y la gestión de incidentes de todos los componentes.
2) **DLP Endpoint Device Control.** Se encarga de monitorizar y restringir el uso de los datos de usuarios. También realiza un escaneo de los ficheros de los sistemas y correos electrónicos.
3) **DLP Discover.** Realiza un escaneo de los ficheros almacenados en local o en los repositorios de la nube para encontrar información sensible.
4) **DLP Prevent.** Recibe correos electrónicos procedentes de los servidores MTA (Mail Transfer Agent). Analiza los mensajes, añade cabeceras apropiadas de acuerdo a la política configurada y añade los correos electrónicos a un único servidor MTA, también conocido como *Smart Host.* DLP Prevent recibe tráfico web procedente de servidores web encapsulados en una petición ICAP (*Internet Content Adaptation Protocol)*. Analiza el tráfico web, determina si el tráfico debe de ser permitido o bloqueado y envía una respuesta ICAP de vuelta al servidor web proxy conectado. **DLP Capture** puede ser habilitado para almacenar contenido para el análisis posterior en un almacenamiento externo (*DLP Capture Storage Array*).
5) **DLP Monitor.** Es capaz de conectarse a un puerto *Switched Port Analyzer (SPAN)* o a un acceso de red para monitorizar de forma pasiva el tráfico. DLP Monitor captura, analiza y almacena el tráfico de red, pero no toma ninguna acción preventiva o bloqueante. Los datos recolectados por DLP Monitor son utilizados para determinar quién envía qué tipo de datos a través de la red y dónde es enviada dicha información. **DLP Capture** puede ser habilitado para almacenar contenido para el análisis posterior en un almacenamiento externo (*DLP Capture Storage Array*).

3 ORGANIZACIÓN DEL DOCUMENTO

9. El presente documento se estructura en las secciones indicadas a continuación, las cuales recopilan aquellas configuraciones y consideraciones a tener en cuenta para hacer uso del producto de forma segura durante todo su ciclo de vida:

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

   2) **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.

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

   4) **Apartado 7.** En este apartado se incluye una lista de tareas a revisar para verificar que se ha llevado a cabo cada una de las recomendaciones y configuraciones descritas en la presente guía de empleo seguro.

4 FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. En la presente sección se describe el procedimiento de recepción segura del producto. En este caso, el producto se trata de un producto *software* y, por lo tanto, no requiere la recepción de ningún tipo de paquete ni la comprobación de ningún tipo de embalaje.
11. Una vez adquirido el producto, su recepción consiste en un correo electrónico que incluye los siguientes datos:
    1) Account Number
    2) Grant Number
    3) Purchase order Number
12. Estos datos proporcionan un inicio de sesión al portal de descargas oficial (cuya URL será proporcionada en el mismo correo electrónico) donde será necesario introducir el correo electrónico utilizado para la adquisición del producto, así como el *Grant Number* del mismo. Una vez que se consigue el acceso al servidor de descargas, se podrán ver los productos disponibles para descargar en la sección *Products* de la página *My Products.* De este modo se puede proceder a la descarga del producto y de sus distintos componentes. Si se necesita una copia de la licencia, se puede obtener de la sección *License Keys*.
13. El producto se encuentra firmado digitalmente mediante un certificado de McAfee. Para verificar que los distintos ficheros descargados han sido firmados correctamente, el usuario puede extraer los ficheros incluidos dentro de los ficheros comprimidos y comprobar, haciendo clic derecho en el fichero y en la opción *Propiedades* seleccionar la sección *Digital Signature.* En el campo de *Signer Information* se podrá verificar la procedencia de dicho certificado.
14. Además, para cada descarga, se incluye un valor *hash* SHA-1 que permite verificar la integridad de la misma.
15. De este modo, se puede dar por concluido el proceso de obtención del producto y de sus componentes.

4.2 ENTORNO DE INSTALACIÓN SEGURO

16. El producto debe de desplegarse teniendo en cuenta las siguientes consideraciones:
    1) El componente ePO debe de instalarse en un equipo con visibilidad a los sistemas que se espera que se gestionen, como, por ejemplo, un controlador de dominio. De este modo será posible que el componente ePO también tenga visibilidad de red para la instalación del producto en múltiples equipos, facilitando su gestión centralizada.

2) Si se hace uso de un MTA, este debe de estar configurado de forma que se encamine el tráfico relacionado con el correo electrónico hacia el componente DLP Prevent.

3) El acceso a la base de datos que hace uso el producto debe de estar restringida exclusivamente a usuarios autorizados.

4) Los administradores autorizados deben de ser personal de confianza para la organización. Estos administradores seguirán y acatarán las instrucciones proporcionadas por la documentación del producto.

5) El hardware donde se encuentran instalado el producto y sus componentes debe de estar protegido de modificaciones físicas no autorizadas. Esto implica que, tanto el hardware como el sistema operativo, así como el software del que depende el producto, debe de operar correctamente.

4.3 REGISTRO Y LICENCIAS

17. Tal y como se ha explicado en la sección *4.1.ENTREGA SEGURA DEL PRODUCTO* el producto y sus componentes se descargan desde un servidor de descarga dedicado mediante el uso de unas credenciales de acceso proporcionadas por correo electrónico una vez que se ha adquirido el producto.

18. Una vez descargado e instalado el producto y sus componentes, puede ser necesaria una activación de la licencia (en el caso de que no se haya realizado durante la instalación del producto). Para ello es posible realizar la activación de la licencia del servidor ePO llevando a cabo los siguientes pasos:

    1) Seleccionar *Menú* → *Configuración* → *Configuración del servidor*, seleccionar Clave de licencia de Categorías de configuración y hacer clic en Editar.

    2) Introducir la Clave de licencia y hacer clic en Guardar.

19. De este modo, se actualizará el catálogo del servidor ePO con las versiones correspondientes a la licencia introducida.

4.4 CONSIDERACIONES PREVIAS

20. Es necesario tener en cuenta una serie de consideraciones previas a la propia instalación del producto. Además, es necesario que el administrador del producto se plantee las siguientes cuestiones con la finalidad de llevar a cabo el despliegue teniendo en cuenta la complejidad de la red de destino:

    1) ¿Cuántos sistemas se pretende gestionar con el servidor ePO?

    2) ¿Los sistemas se encuentran en una única red o en múltiples áreas geográficas?

    3) ¿Existen soluciones de seguridad, como un cortafuegos?

4) ¿Se hace uso del protocolo NAT (Network Address Translation) en una red externa?

5) ¿Existen restricciones de ancho de banda en los segmentos remotos de la red?

6) ¿Se realiza la gestión de equipos portátiles conectados a Internet fuera de la red corporativa?

7) ¿Hay distintos administradores con distintos permisos a través de productos diferentes, grupos de sistemas o funciones diferentes dentro de una consola de gestión?

21. Además, es necesario tener en cuenta una serie de consideraciones relacionadas con la escalabilidad de la red y del propio servidor ePO. A continuación, se listan las versiones de Windows soportadas por el producto:

    1) Para los equipos que tengan instalados el **servidor McAfee** se recomienda el uso de algunos de los siguientes sistemas operativos de 64-bit:

        - Windows Server 2008 R2 Service Pack 1
        - Windows Server 2012
        - Windows Server 2012 Service Pack 1
        - Windows Server 2012 R2
        - Windows Server 2016
        - Windows Server 2019

    2) Para los equipos cliente que instalen los **componentes de McAfee** se recomienda el uso de sistemas operativos Windows 8.1 o posterior.

22. Antes de llevar a cabo la instalación del producto, hay que tener en consideración los siguientes pasos relacionados con la configuración del entorno en el que se ejecutará el producto:

    1) Se debe de establecer una dirección IP estática para las máquinas donde el producto sea instalado, siguiendo las recomendaciones del fabricante.

    2) Se ha realizado la instalación de las últimas actualizaciones disponibles de los sistemas operativos Windows.

    3) Se ha instalado en la máquina servidor (Windows Server), el rol Network 3.25 para realizar la instalación de SQL Server.

    4) Se ha realizado la instalación de SQL Server en la máquina servidora. McAfee ePO puede solo comunicarse con SQL utilizando una conexión TCP/IP. Antes de realizar la instalación de McAfee ePO, se debe de verificar que el servidor SQL que hospede la base de datos de McAfee ePO debe de tener TCP/IP habilitado. Para configurar el protocolo TCP/IP para el servidor SQL hay que seguir los siguientes pasos:

    5) Configurar el protocolo TCP/IP para el servidor SQL:

- Iniciar Gestor de configuración del servidor SQL.
- Desde el panel, expandir la opción *Configuración de red del servidor SQL* y seleccionar los protocolos para la instancia SQL. Si, por ejemplo, se usa una instancia por defecto (MSQLSERVER), seleccionar la opción *Protocolos para MSSQLSERVER*.
- En el panel de detalles, localizar la entrada para *TCP/IP* y comprobar la columna de estado. Si está establecida como *Activada*, seguir por el paso 2 para determinar el puerto que está siendo utilizado.
- Si la opción TCP/IP está establecida como deshabilitada, hacer doble clic en la opción TCP/IP para abrir la ventana de propiedades TCP/IP.
- Seleccionar la sección *Protocolo*, clic en *Habilitar*, y seleccionar *Si.*
- Clic *Aplicar* y después *OK* para cerrar el dialogo de *Advertencia.* TCP/IP está habilitado. Ahora se puede reiniciar el servicio para asegurar que los cambios han surtido efecto.
- En el panel principal, clic en *Servicios del servidor SQL.*
- En el panel de detalles, clic con el botón derecho en el servicio del servidor SQL y clic en *Reiniciar.*

6) Determinar el puerto utilizado por SQL:
   - Si se necesita, iniciar el *Gestor de configuración del servidor SQL,* expandir la opción *Configuración de red de servidor SQL,* y seleccionar la opción de *Protocolos* para la instancia SQL.
   - Doble clic en *TCP/IP* para abrir la ventana *Propiedades TCP/IP.*
   - Seleccionar opción *Direcciones IP.* Asegurarse que la opción *Activado* tiene el valor *Si* para cada dirección IP activa.
   - Bajo el campo *IPAll,* tomar nota del valor de *Puertos dinámicos TCP.* Si es un valor especifico, como por ejemplo 57482, el servidor SQL está utilizando puertos dinámicos. Tomar nota del valor ya que esta información puede ser necesitada más tarde en la instalación.

   Nota: Si se están utilizando puertos dinámicos, el servicio *SQL Browser* debe de estar en ejecución en el servidor SQL. Si el valor del campo *Puertos dinámicos TCP* está vacío, significa que el servidor SQL está utilizando un puerto estático y que el valor para este puerto puede ser mostrado en el campo *Puerto TCP.*

7) Si se hace uso de puertos dinámicos, tomar nota del nombre de la instancia SQL que hospedará la base de datos de McAfee ePO. La instancia por defecto es *MSSQLSERVER*.

8) Creación de una cuenta de usuario en SQL Server con los roles *sysadmin, dbcreator y public (Server Roles).* Además, se le ha asignado al usuario creado

el rol *db_owner (User Mapping)* de las bases de datos definidas por el propio SQL Server.

9) Configuración de SQL Server para permitir la autenticación mediante usuario SQL (*SQL Server Athentication*).

10) Configuración de SQL Server para habilitar el puerto 1433, definido por defecto, siguiendo las indicaciones del fabricante en sus manuales de instalación. Se debe de activar, además, la opción desencadenadores anidados siguiendo la recomendación del manual del fabricante.

11) Instalación de la utilidad SQL Server Management Studio para la gestión de los servicios asociados a SQL Server.

23. El instalador de McAfee ePO incluye un *Auditor de Pre-Instalación* para reducir o prevenir posibles problemas de instalación o actualización. Esta funcionalidad del instalador comprueba los siguientes parámetros:

    1) Licencia del producto.

    2) Credenciales que se utilizarán con Microsoft SQL:

    3) Credenciales de autenticación de Windows (Credenciales del dominio que tiene permisos de responsable de base de datos (*Database Owner (dbo))* en el servidor SQL).

    4) Credenciales de autenticación SQL.

    5) Directorio de destino de la instalación del producto.

    6) Servidor SQL instalado, incluyendo nombre del servidor o nombre de servidor con nombre de instancia y puerto utilizado por el propio servidor.

24. A la hora de llevar a cabo la instalación del componente *DLP Prevent* y del componente *DLP Monitor,* también es necesario tener en cuenta una serie de consideraciones previas (incluyendo los requisitos software y sistemas operativos compatibles) a la propia instalación y puesta en marcha:

    1) Deshabilitar todos los servicios que no se utilicen, como ICAP en el correo electrónico.

    2) Restringir las direcciones IP que pueden utilizar los servicios.

    3) Controlar quien tiene acceso físico al producto o a su consola de gestión.

    4) Uso de gestión externa a la red que permita a McAfee ePO aislar la gestión y el tráfico de red.

    5) El tráfico LAN debe de no ser accesible desde fuera de la organización.

    6) Conectar cualquier interfaz de *Baseboard Management Controller*, controlador de administración de placa base, (BMC) a una red de administración segura específica.

25. Por otra parte, para lleva a cabo la instalación del componente DLP Endpoint, hay que tener en cuenta las siguientes consideraciones previas:

1) *McAfee ePO.* El servidor ePO debe de estar instalado para gestionar este componente.

2) Para instalar el componente en un entorno virtual, es necesario preparar la plataforma virtual con los requisitos necesarios.

26. Antes de realizar la instalación del producto es necesario tener en cuenta la necesidad de disponer de:

    1) Una instalación del servidor McAfee ePO.

    2) Usuarios y grupos creados para asignaciones administrativas.

    3) Despliegue de McAfee Agent en los equipos en los que se requiera instalar este componente.

27. Teniendo en cuenta estas consideraciones, hay que descargar las extensiones del producto y los ficheros de instalación. Para ello, es posible descargarse el paquete correspondiente desde el repositorio de descarga o a través del catálogo software del propio servidor McAfee ePO (*Menú – Software – Catálogo de software*).

28. Finalmente, se recomienda la creación de usuarios a través del menú de McAfee ePO y la asignación de permisos para visualizar y guardar políticas, visualizar campos y también asignar un control de acceso basado en roles (*Role-Based Access Control-RBAC*).

29. Para el caso del componente DLP Discover, los pasos no son distintos que para el resto de componentes. Hay que tener en cuenta que, para la instalación de este componente, solamente hay que disponer del servidor McAfee ePO instalado previamente.

30. Además, se debe de realizar la descarga de las extensiones y el despliegue del producto a través del catálogo de software dl servidor McAfee ePO (*Menú – Software – Catálogo de Software*).

31. Finalmente, es necesario preparar la red donde se instalará el componente DLP Discover. Para ello, se deben de llevar a cabo los siguientes pasos:

    1) Es necesario configurar el cortafuegos que se encuentre desplegado para permitir una serie de puertos necesarios para el correcto funcionamiento del componente DLP Discover. Los puertos a tener en cuenta son los siguientes:

- Puerto 443. Puerto TCP que el servidor McAfee ePO utiliza para recibir peticiones de los agentes y de los controladores de agentes remotos de forma de que la comunicación entre el servidor y los componentes sea segura.
- Puerto 8081. Puerto TCP que los agentes utilizan para recibir peticiones de *wake-up* del servidor ePO o de los controladores de agentes.
- Puerto 8082. Puerto UDP que los agentes utilizan para enviar mensajes procedentes del servidor ePO o controlador de agente.
- Puerto 8443. Puerto TCP que el servidor McAfee ePO utiliza para permitir el acceso a la interfaz web.

- Puerto 8444. Puerto TCP que el controlador de agente utiliza para comunicarse con el servidor McAfee ePO para obtener la información requerida (como los servidores LDAP).
- Puerto 1433. Puerto TCP utilizado para comunicarse con el servidor SQL.
- Puerto 1434. Puerto UDP utilizado para solicitar el puerto TCP que utiliza la instancia de SQL que aloja la base de datos del servidor ePO.
- Puerto 389. Puerto TCP utilizado para obtener información LDAP de servidores Active Directory.
- Puerto 636. Puerto TCP utilizado para obtener información LDAP de servidores de Active Directory mediante el uso de SSL.
- Puerto 445. Puerto TCP utilizado para el inicio de sesión de la consola ePO cuando se autentica a un usuario de un Active Directory.
- Puerto 6514 (Opcional). Puerto utilizado para la comunicación con syslog (si se encuentra habilitado) utilizando TLS.

2) Crear usuarios y grupos para asignaciones administrativas.

3) Desplegar el agente (McAfee Agent) en los servidores.

4) Instalar el rol de servidor Microsoft Internet Information Services (IIS) en los servidores DLP.

4.5 INSTALACIÓN

32. La instalación del producto y de sus componentes se llevará a cabo siguiendo las siguientes guías de instalación y despliegue:

    1) McAfee Data Loss Prevention 11.1.x Installation Guide.

    2) McAfee Data Loss Prevention Endpoint 11.1.x Installation Guide.

    3) McAfee Data Loss Prevention Monitor 11.1.x Installation Guide.

    4) McAfee Data Loss Prevention Prevent 11.1.x Installation Guide.

    5) McAfee ePolicy Orchestrator 5.10.0 Installation Guide.

    6) McAfee Agent 5.5.1 Product Guide (McAfee ePolicy Orchestrator).

    7) McAfee Data Loss Prevention 11.1 Common Criteria Evaluated Configuration Guide.

33. Para llevar a cabo la instalación del producto de forma segura, es necesario seguir los siguientes pasos:

    1) Uso de **FIPS *mode***. La configuración segura requiere que el producto se instale utilizando el modo FIPS. Los pasos para realizar la instalación del producto haciendo uso de este modo son los siguientes:

    2) Desde la línea de comandos, hay que moverse entre los distintos directorios hasta llegar al directorio que contiene el instalador de McAfee ePO.

3) Introducir el siguiente comando: *setup.exe ENABLEFIPSMODE=1.* Debe de realizarse la ejecución con permisos de administrador.

4) Continuar los pasos de la instalación de forma habitual, siguiendo los pasos indicados en el asistente de instalación. Estos pasos se resumen a continuación:

5) Una vez iniciado el asistente de instalación, clic en *Siguiente* para continuar con la instalación. Monitorizar el proceso de instalación cuando se hace uso del asistente ya que, durante el proceso de instalación puede ser necesario reiniciar el sistema.

6) Elegir el *Directorio de destino* de la instalación. Es posible cambiarlo o dejar el directorio por defecto. Hacer clic en *Siguiente.*

7) El instalador buscará un Servidor SQL. Si la instalación encuentra varios servidores, automáticamente se moverá a la siguiente fase del proceso y se mostrará una lista de selección para elegir el servidor. Si no es posible encontrar ningún servidor, un diálogo consultará si se quiere buscar de nuevo. Si se hace clic en *No* se avanzará hacia el siguiente paso donde la información del servidor SQL puede ser introducida manualmente.

8) En el paso de *Información de base de datos,* especificar la información para la base de datos y hacer clic en *Siguiente*.

9) Especificar el servidor de base de datos y el nombre de la base de datos. Estos valores se rellenarán automáticamente si el paso anterior de descubrimiento automático ha funcionado correctamente. Si no ha funcionado o se utiliza puertos SQL dinámicos, hay que introducir el nombre del servidor SQL y el nombre de la instancia SQL separado una barra invertida "\".

10) Especificar el tipo de credenciales de base de datos a utilizar. Es posible elegir entre la autenticación de Windows y la autenticación de SQL.

11) Clic en *Siguiente*. El instalador intentará conectarse al servidor SQL utilizando las credenciales proporcionadas. Si el instalador no puede determinar automáticamente el puerto, este mensaje aparecerá: *El programa de instalación no pudo acceder al puerto UDP 1434 de SQL.* Clic en *OK* para volver a la página de *Información de la base de datos*. Ahora, el campo del puerto TCP del servidor SQL está disponible. Introducir el puerto y hacer clic en *Siguiente*.

12) A continuación, se iniciará el *Pre-installation Auditor* el cual comenzará automáticamente. Es necesario revisar los resultados y corregir cualquier fallo que aparezca. Después hacer clic en *Ejecutar de nuevo.* Una vez que todas las comprobaciones hayan sido validadas, hacer clic en *Finalizar*.

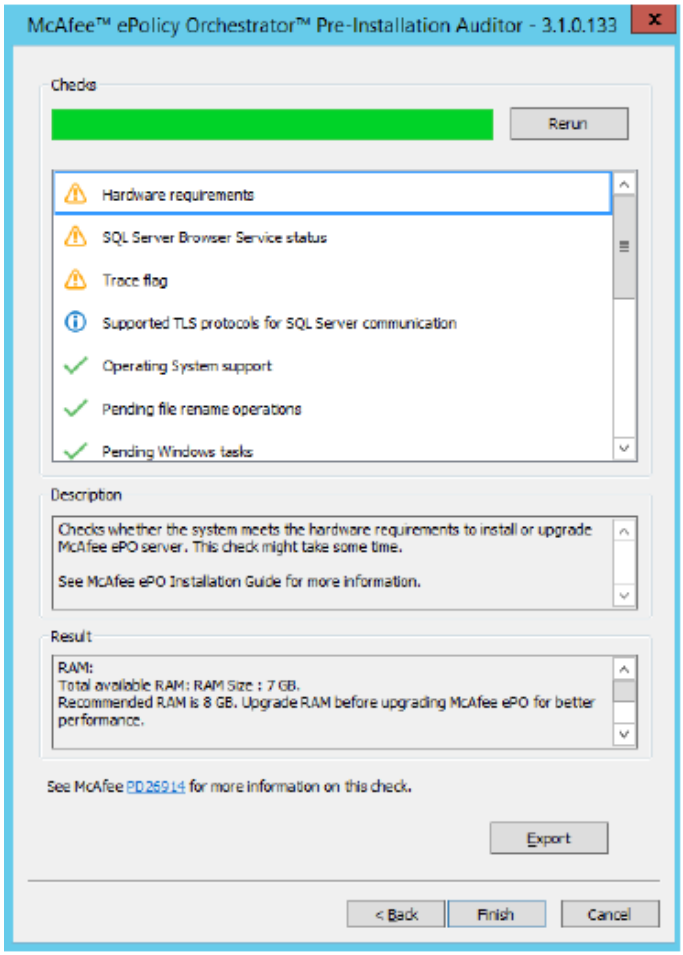

Ilustración 2. Comprobaciones realizadas por el instalador.

13) En el paso de *Información del puerto HTTP,* revisar el puerto por defecto asignado, hacer clic en *Siguiente* para verificar que los puertos no están en uso en el sistema. **Importante**: se puede cambiar alguno de esos puertos durante la instalación. Cuando la instalación esté completada, se puede cambiar solamente los puertos *Agent wake-up communication* y *Agent broadcast communication port*.

14) En el paso de *Información del administrador,* incluir esta información, después hacer clic en *Siguiente*.

15) Escribir el nombre de usuario y contraseña que se quiere utilizar para la cuenta de administrador principal. La contraseña debe de cumplir unos requisitos de complejidad suficientes y estar compuesto por: una longitud mínima o igual a 12 caracteres, estar formado por letras mayúsculas, letras minúsculas, números y por caracteres especiales [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “].

16) Incluir la frase de contraseña de recuperación. Esta frase de contraseña debe de estar compuesta de entre 14 a 200 caracteres, no debe de contener barras invertidas, espacios, comillas dobles, o caracteres por debajo de ASCII 32 o por encima de ASCII 65535.

Importante esta frase de contraseña debe de estar almacenada en un lugar seguro ya que es necesaria para descifrar la instantánea de recuperación de desastres y McAfee no puede recuperar dicha frase de contraseña.

17) En el paso de *Tipo de clave de licencia,* incluir la clave de licencia y después hacer clic en *Siguiente.* Si no se dispone de una licencia, es posible seleccionar el modo de *Evaluación* para continuar con la instalación del software en modo de evaluación. El periodo de evaluación está limitado a 90 días. Es posible introducir una clave de licencia después de completar la instalación a través de la configuración de McAfee ePO o del Catálogo Software. Opcionalmente, si se desea también es posible que McAfee ePO descargue automáticamente los productos de los cuales se dispone licencia después de que la instalación se complete. Para ello, seleccionar la opción *Habilitar instalación automática de producto.*

18) Aceptar el Acuerdo de licencia de usuario final de McAfee y hacer clic en OK.

19) Desde el diálogo de *Preparado para instalar el programa,* decidir si se quiere permitir a McAfee a recopilar datos de telemetría del propio software y del sistema y después hacer clic en *Instalar* para iniciar la instalación del software.

20) Cuando la instalación se ha completado, hacer clic en *Finalizar* para salir del programa de instalación.

21) Una vez finalizada la instalación, es conveniente llevar a cabo las siguientes tareas:

22) Definición de configuración de proxy. Si se hace uso de un servidor proxy, se debe de especificar su configuración en la página de *Configuración del servidor.* Para ello, es necesario seguir los siguientes pasos:

23) Seleccionar Menú → Configuración → Configuración del servidor, seleccionar Configuración de Proxy de Categorías de configuración y hacer clic en Editar.

24) Seleccionar *Configurar manualmente las configuraciones del proxy,* proporcionar la información específica de configuración del proxy y guardar los cambios.

25) Prueba para verificar que el producto es capaz de detectar y parar una amenaza de muestra. Para ello es necesario acceder al sistema de prueba, con permisos de administrador, y realizar los siguientes pasos:

26) Conectar con la web de EICAR: http://www.eicar.org/86-0-Intended-use.html

27) Seguir las instrucciones para descargar y ejecutar el fichero de test *68-Byte eicar.com*.

28) En Windows, clic en Inicio → Todos los programas → McAfee → McAfee Endpoint Security y hacer clic en Estado.

29) Hacer clic en *Registro de eventos* para mostrar los eventos de amenaza en la tabla de eventos y eliminar la amenaza de ejemplo.

30) Verificar la respuesta a la amenaza. Para verificar la respuesta, es necesario acceder a *Menú → Informes → Registro de eventos de amenaza* y comprobar el registro asociado a la prueba realizada.

31) Una vez instalado el producto, el siguiente paso es ejecutarlo y activar la licencia utilizando *Menú |Software | Configuración Servidor.* Posteriormente, es necesario proceder a la instalación de las extensiones *McAfee DLP Management extensions* y *McAfee Data Loss Prevention Appliance Management ePO Extension Bundle.*

32) El siguiente paso consiste en la instalación del agente a través del menú *Menú |Software | Repositorio Principal.* Desde este menú es posible realizar el despliegue del agente a los equipos detectados por McAfee ePO o descargar el instalador para desplegarlo de forma manual en los equipos.

33) El siguiente paso consiste en la instalación de los componentes *DLP Monitor* y *DLP Prevent*.

34) A continuación, se debe de realizar la instalación del componente *DLP Discover*.

35) Instalación de DLP server, el cual necesita seguir los mismos pasos que para el paso anterior y, además, los pasos para habilitar la característica de Windows Server IIS (*Web Server Role*).

36) Finalmente, es necesario llevar a cabo la instalación del componente *DLP Endpoint* en el equipo cliente y su correspondiente *McAfee Agent.* En primer lugar, se debe de realizar el despliegue del agente a través de la interfaz del servidor McAfee ePO y posteriormente el despliegue del componente *DLP Endpoint.*

34. Es necesario hacer mención a los pasos necesarios para realizar la instalación de los componentes del producto (*DLP Monitor, DLP Prevent, etc.*). Estos pasos se realizan desde la interfaz de McAfee ePO:

1) Seleccionar Menú → Software → Catálogo software.

2) En el panel izquierdo, expandir *Software (por etiqueta)* y seleccionar *Data Loss Prevention.*

3) Seleccionar el componente DLP a instalar:

- McAfee DLP Discover 11.1,
- McAfee Data Loss Prevention and Device Control 11.1
- McAfee DLP,
- Common UI,
- Appliance Management Extension,

- McAfee DLP Appliance Management.

4) Para instalar todo el software disponible, clic en *Incorporar todos*.

5) Seleccionar el *checkbox* para aceptar el acuerdo de licencia, después clic en *OK.*

5 FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

35. Tal y como se menciona en los manuales de instalación, el producto dispone de un modo de criptografía compatible con FIPS 140-2 denominado modo FIPS o *FIPS mode*. Para activar este modo, es necesario llevar a cabo la instalación del servidor McAfee ePO tal y como se ha descrito en la sección *4.5.INSTALACIÓN.* Además, una vez instalados los componentes de McAfee DLP, es necesario llevar a cabo algunos cambios en su configuración para que hagan uso de este modo de operación:

    1) Una vez instalados el resto de componentes, es necesario realizar un cambio en su configuración a través de la propia interfaz gráfica del producto:

    2) **Prevent/Monitor.** Desde la interfaz de McAfee ePO, en la sección *Catálogo de Directivas → Administración de appliances de DLP → General* aparece la lista de políticas definidas. Cada política puede editarse para activar el modo FIPS en *Modo de Seguridad → Activar modo FIPS 140-2.*

    3) **Discover/Endpoint.** Estos componentes realizan operaciones criptográficas de forma que sean conformes con FIPS 140-2 sin necesidad de una configuración adicional.

36. Por último, una vez realizada la instalación del producto es recomendable realizar los siguientes pasos para verificar que la configuración se ha realizado correctamente:

    1) **McAfee ePO.** Hay que llevar a cabo tres verificaciones:

- **Verificar *el controlador del Agente*.** Para ello, hay que editar el fichero *server.ini* situado en el directorio *DB* del directorio de instalación de McAfee ePO y buscar el valor *FipsMode.* Este valor debe de tener un valor "1". Si el valor es "0", será necesario llevar a cabo una reinstalación de McAfee ePO.
- ***Verificar servidor Apache.*** En el directorio *apache2\conf* del directorio de instalación de McAfee ePO hay que cambiar la configuración del fichero *httpd.conf* y buscar el valor *SSLFIPS.* Este valor debe de estar habilitado ("on"). Además, se puede verificar en el directorio *apache2\bin* las propiedades de los ficheros *libeay32.dll* y *ssleay32.dll* los cuales deben de incluir los siguientes valores:
- File version: 1.0.2.16
- Product version: 1.0.2.p
- **Verificar el servidor de aplicaciones.** Para ello, hay que verificar que en el menú Menú-> Configuración -> Configuración del servidor -> Claves de seguridad la opción Modo de seguridad indica "FIPS 140-2".

    2) **Componente cliente.** Para verificar que la instalación del componente cliente se ha establecido correctamente, hay que acceder al directorio de instalación del agente (por defecto *C:\Program Files\McAfee\Agent* y hacer clic derecho

en el fichero *cryptocme.dll* y seleccionar *Propiedades*. En la versión del fichero debe de aparecer el valor *4.0.1.0* el cual corresponde con la versión FIPS validada para la evaluación.

5.2 AUTENTICACIÓN

37. El servidor McAfee ePO soporta tres tipos de autenticación para los usuarios:
    1) Autenticación con usuario y contraseña a través de McAfee ePO.
    2) Autenticación de Windows. El dominio de Windows y los detalles del nombre de usuario están almacenados en McAfee ePO (una vez que se prepare el servidor para ello). De este modo, el usuario podrá hacer uso de sus credenciales de dominio para acceder a la interfaz del servidor McAfee ePO. Los usuarios de Windows que no pueden autenticarse con el dominio padre pueden habilitar la característica de autenticación de Windows y especificar los detalles de los dominios no confiables.
    3) Autenticación basada en certificado. Esto permite a los usuarios acceder a McAfee ePO con un certificado cliente válido en lugar de un nombre de usuario y una contraseña.
38. Durante la instalación del producto, es necesario llevar a cabo la creación de dos contraseñas. Estas contraseñas son la asociada a la interfaz del servidor McAfee ePO y la contraseña asociada a la base de datos asociada a Microsoft SQL Server.
39. Es recomendable que todas las contraseñas cumplan los siguientes requisitos de complejidad:
    1) Al menos 8 caracteres de longitud.
    2) Contener al menos un carácter en mayúsculas y otro en minúsculas.
    3) Contener al menos, un carácter numérico y otro alfanumérico.
40. Además, el producto soporta la autenticación a partir de las credenciales de usuario tanto las del sistema operativo Windows como las del propio servidor McAfee ePO. Con la finalidad de garantizar el empleo de contraseñas seguras, el producto dispone de la funcionalidad de establecer una política de contraseñas para los usuarios, la cual es recomendable configurar. Para realizar la configuración de esta política de contraseñas, es necesario llevar a cabo los siguientes pasos:
    1) En la interfaz del servidor McAfee ePO, seleccionar *Configuraciones del servidor* → *Política de contraseñas* y hacer clic en *Editar*. Definir los criterios para editar las contraseñas:
    2) *Criterio para fortaleza de contraseña.* En esta opción es posible definir la fortaleza de la contraseña (configurando su longitud entre 7 y 30 caracteres) así como restringir el uso de contraseñas (entre 3 y 24 contraseñas anteriores).

3) *Criterio de expiración de contraseña.* En esta opción es posible introducir el número de días antes de que la contraseña expire (de 30 a 365 días).

4) Una vez que se ha habilitado el criterio de fortaleza de contraseñas, automáticamente se requiere que las contraseñas contengan lo siguiente:

5) Una letra mayúscula (A-Z).

6) Una letra minúscula (a-z).

7) Un carácter numérico (0-9).

8) Un carácter especial (#?!@$%^&*-).

41. Finalmente cabe indicar que la comunicación entre los distintos componentes del producto se lleva a cabo mediante certificados para establecer un canal de comunicación seguro y confiable. De este modo se realiza una autenticación entre los componentes del producto.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

42. El producto permite a un usuario privilegiado realizar funciones de administración del propio producto. Estas funciones modificarán el comportamiento del producto desde un punto de vista funcional y desde el punto de vista de la seguridad, modificando varios atributos para ello.

43. Para llevar a cabo esta administración, el producto dispone de una interfaz web que permite realizar una administración remota. El producto utiliza el protocolo HTTPS para establecer un canal de comunicaciones seguro.

44. Por defecto, el producto permite el uso de protocolos de comunicaciones no seguros, con la finalidad de permitir compatibilidad en algunos entornos si es necesario. Sin embargo, para llevar a cabo una configuración segura del mismo, es necesario deshabilitar dichos protocolos para forzar que las comunicaciones se realicen de forma segura.

45. Para ello, es necesario incluir algunas modificaciones en las siguientes líneas de los ficheros, situados en la máquina donde se encuentra instalado el servidor McAfee ePO, mencionados a continuación:

    1) En el fichero situado en *C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Apache2\conf\httpd.conf* se debe de comentar (haciendo uso del carácter "#") la línea en la que se permite el uso del puerto 80 de comunicaciones, es decir, *Listen 80.* De este modo, se fuerza el uso de HTTPS.

    2) En el fichero situado en *C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Apache2\conf\ssl.conf* se debe de modificar la línea 106 para que quede de la siguiente forma:

SSLProtocol +TLSv1.2.

De este modo se fuerza el uso del protocolo de comunicaciones TLSv1.2 para establecer comunicaciones seguras.

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

46. El producto permite mantener los siguientes roles de usuarios: *Administrador y Usuario con permisos seleccionados.*
47. Para configurar cada uno de estos roles, es necesario llevar a cabo la creación de un usuario a través de la interfaz del servidor McAfee ePO. Las opciones de configuración de cuentas de usuarios se encuentran en *Gestión de usuarios -> Usuarios.*
48. Desde este panel es posible realizar la creación de un nuevo usuario, elegir un tipo de autenticación (*Autenticación desde McAfee ePO, Autenticación de Windows,* o *Autenticación basada en certificado*) y proporcionar las credenciales requeridas.
49. Finalmente, es posible elegir el rol de usuario entre administrador (*administrator*) o elegir un conjunto de permisos apropiado para el usuario.
50. El producto dispone de la posibilidad de personalizar el mensaje de inicio de sesión. De este modo, se puede configurar un mensaje de aviso y consentimiento antes de que un usuario haga el inicio de sesión con sus credenciales de usuario. Este mensaje se puede configurar desde la interfaz del servidor McAfee ePO a través del panel *Menú -> Configuración -> Configuración del servidor,* seleccionar *Mensaje de inicio de sesión* de la opción *Categorías de configuración* y hacer clic en la opción *Editar.* A continuación, hacer clic en la opción *Mostrar mensaje de inicio de sesión personalizado,* editar el mensaje y hacer clic en *Guardar* para guardar los cambios realizados.
51. El producto requiere un proceso de autenticación positivo previo a la realización de cualquier tipo de tarea, tanto para los usuarios con permisos cómo para los usuarios de tipo administrador.

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

52. El producto, una vez instalado de acuerdo a los pasos indicados en la sección *4.5.INSTALACIÓN* dispone de una configuración segura de los interfaces, puertos y servicios de modo que hace uso de aquellos que necesita para llevar a cabo de forma eficiente su funcionalidad.

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

53. El producto permite una modificación en su configuración con la finalidad de hacer uso de protocolos seguros. De acuerdo con esto, es recomendable llevar a cabo los siguientes cambios para forzar el uso del protocolo HTTPS y TLS1.2:

    1) **HTTPS.** Para que el producto no permita comunicaciones haciendo uso del protocolo HTTP y, por tanto, del puerto 80, es necesario comentar o eliminar la siguiente línea del fichero *http.conf* (situado en la ruta por defecto *C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Apache2\conf*): "*Listen 80*". De este modo, el producto no habilitará el puerto 80, manteniéndolo cerrado.

    2) **TLS.** Para que el producto no permita comunicaciones con versiones anteriores a TLSv1.2, es necesario modificar la línea *SSLProtocol* del fichero *ssl.conf* (situado en la ruta por defecto *C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Apache2\conf*) de modo que quede de la siguiente forma: *SSLProtocol +TLSv1.2*.

54. Siguiendo las indicaciones anteriores, el producto hará uso de protocolos seguros, exigiendo su utilización para las comunicaciones.

5.6 GESTIÓN DE CERTIFICADOS

55. El producto hace uso de certificados para llevar a cabo sus comunicaciones de forma confiable. Se pueden distinguir dos tipos de certificados en función del uso para el cual se requiere: certificados utilizados para la comunicación cliente-producto a través de un navegador web y certificados utilizados para la comunicación entre los componentes que forman el producto.

5.6.1 CASO 1. CERTIFICADOS UTILIZADOS POR UN NAVEGADOR WEB

56. Un navegador web mostrará un mensaje de advertencia cuando el certificado utilizado para acceder a través de la interfaz web del servidor McAfee ePO no sea válido. Es posible integrar un certificado firmado por una autoridad confiable o crear un certificado autofirmado si se prefiere optar por dicha vía. La creación de un certificado autofirmado puede proporcionar una seguridad básica y la funcionalidad necesaria para sistemas utilizados en redes internas.

57. Para la creación de un certificado autofirmado, es posible hacer uso de varias herramientas como por ejemplo OpenSSL. El primer paso, por lo tanto, consiste en la instalación de OpenSSL para Windows y la creación de la siguiente estructura de directorios:

    1) C:\ssl\: carpeta de instalación de OpenSSL.

    2) C:\ssl\certs\: utilizada para almacenar los certificados creados.

3) C:\ssl\keys\: utilizada para almacenar las claves creadas.

4) C:\ssl\requests\: utilizada para almacenar las solicitudes de certificación creadas.

58. Los pasos a seguir son los siguientes:

1) Para generar la clave de certificado inicial, escriba el siguiente comando en la línea de comandos:

2) C:\ssl\bin>openssl genrsa -des3 -out C:/ssl/keys/ca.key 2048

3) Introduzca una frase de contraseña en el símbolo del sistema inicial y verifíquela en el segundo. Se generará el archivo con el nombre *ca.key* y se almacenará en la ruta *C:\ssl\keys*.

4) Para autofirmar la clave de certificado que ha creado, escriba el siguiente comando den la línea de comandos:

5) openssl req -new -x509 -days 365 -key C:/ssl/keys/ca.key -out C:/ssl/certs/ca.cer

6) Escribir la información necesaria conforme que vaya solicitándolo el proceso (Nombre del país, nombre de estado o provincia, nombre del municipio, etc.).

7) Se generará el archivo con el nombre ca.cer y se almacenará en la ruta *C:\ssl\certs*.

59. Una vez generado el certificado, puede cargarse e integrarse en McAfee ePO:

1) Abra la página Editar certificado del servidor.

2) Seleccione Menú → Configuración → Configuración del servidor.

3) En la lista Categorías de configuración, seleccione Certificado de servidor y haga clic en Editar.

4) Navegue hasta el archivo del certificado de servidor y haga clic en *Abrir.* En este ejemplo, navegue hasta *C:\ssl\certs* y seleccione ca.cer.

5) Si fuera necesario, escriba la contraseña del certificado PKCS12.

6) Si fuera necesario, escriba el alias del certificado.

7) Navegue hasta el archivo de la clave privada y haga clic en *Abrir.* En este ejemplo, navegue hasta *C:\ssl\keys* y seleccione *ca.key*.

8) Si fuera necesario, escriba la contraseña de la clave privada y haga clic en *Guardar.*

9) Reinicie McAfee ePO para que el cambio surta efecto.

60. Cabe destacar también, la existencia de una sección orientada a la de mostrar otros comandos de la herramienta OpenSSL que pueden ser de utilidad para el usuario. No obstante, se recomienda el uso de certificados emitidos por una Autoridad de Certificación (CA), en lugar de certificados autofirmados.

61. Por otra parte, es necesario tener en cuenta que, los certificados hagan uso de algoritmos y funciones criptográficas admitidos por la guía CCN-STIC-807 [CCN-STIC-807]. Con el uso de la versión de OpenSSL v1.0.2p se generan certificados que cumplen con dichos algoritmos y funciones criptográficas. Sin embargo, se recomienda realizar una comprobación de los algoritmos que sean utilizados por los certificados que se instalen en el producto antes de hacer uso de ellos. Los algoritmos y funciones recomendados son los siguientes:

    1) RSA con claves de, al menos, 2048 bits de longitud.
    2) ECDSA con curvas P-256 o superior.
    3) DSA con claves de, al menos, 2048 bits de longitud.
    4) Funciones Hash SHA-256 o superior

62. Para verificar las funciones y algoritmos utilizados por un certificado, es necesario comprobar la pestaña de propiedades del mismo, basta con ver sus propiedades y en la sección *Detalles* se puede verificar los algoritmos utilizados. A continuación, se puede observar un ejemplo de un certificado:

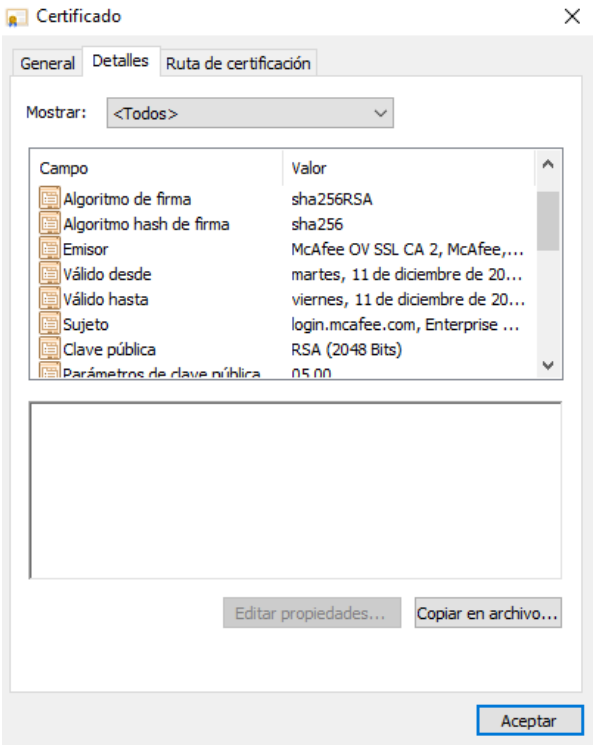

Ilustración 3. Propiedades de un certificado de ejemplo

63. Por lo tanto, es necesario tener en cuenta que aquellos certificados que se instalen con la finalidad de ser utilizados para interactuar con el producto deben de cumplir con los algoritmos y funciones mencionados.

64. Manteniendo el propósito de esta guía, en el caso de que los algoritmos hagan uso de algoritmos y funciones que no cumplan con lo referido, se recomienda la generación de un nuevo certificado. Si, por ejemplo, solamente es necesario llevar

a cabo una migración de SHA-1 a SHA-2 o superior, es posible realizarlo mediante la ejecución de los siguientes pasos:

1) Inicie sesión como administrador en la interfaz gráfica del componente McAfee ePO y seleccione *Menú* → *Configuración* → *Administrador de certificados.* La página del Administrador de certificados proporciona información sobre el certificado raíz instalado, los certificados de los controladores de agentes, los certificados de servidor y otros certificados derivados de la autoridad de certificación (CA) raíz de McAfee ePO.

2) Haga clic en *Regenerar certificado* y, a continuación, haga clic en *Aceptar* para confirmar. La CA raíz de McAfee ePO y otros certificados derivados de la CA raíz se regeneran y se almacenan en una ubicación temporal del servidor. El tiempo necesario para completar el proceso depende del número de controladores de agentes y de extensiones que derivan certificados de la CA raíz de McAfee ePO.

3) Una vez regenerados los certificados, espere a que se produzca una propagación suficiente de los certificados nuevos en su entorno. A medida que los agentes se comuniquen con el servidor de McAfee ePO, recibirán el nuevo certificado. El porcentaje de agentes que han recibido los certificados regenerados se indica en el *Administrador de certificados,* debajo de *Producto: Controlador de agentes* → *Estado*.

   Importante: Asegúrese de que el porcentaje de distribución sea lo más próximo posible al 100% antes de continuar. De lo contrario, cualquier sistema pendiente no recibirá los certificados recién regenerados y no podrá comunicarse con McAfee ePO una vez activados los certificados. Puede permanecer en este estado tanto tiempo como sea necesario para alcanzar una propagación suficiente.

4) Una vez logrado un porcentaje de distribución cercano al 100%, haga clic en *Activar certificados* para llevar a cabo el resto de operaciones futuras con los certificados nuevos. Se crea una copia de seguridad de los certificados originales y aparece un mensaje.

5) Haga clic en *Aceptar.*

6) Detenga e inicie estos servicios:

7) Detenga los servicios de los controladores de agentes.

8) Reinicie los servicios de McAfee ePO.

9) Inicie los servicios de los controladores de agentes.

10) Supervise su entorno y asegúrese de que sus agentes se comuniquen de forma correcta. Puede cancelar la migración en este punto para revertir los certificados y restaurar la comunicación agente-servidor; sin embargo, esto no es posible una vez completado el paso siguiente.

11) Haga clic en *Finalizar migración* para completar la migración de certificados. Si se produce algún problema durante la migración, haga clic en *Cancelar migración* para revertir a los certificados anteriores. Si cancela la migración, detenga los servicios de los controladores de agentes, reinicie el servicio de McAfee ePO e inicie de nuevo los servicios de los controladores de agentes. Puede iniciar de nuevo la migración de certificados tras solucionar los problemas.

12) Reinstale los agentes que utilicen los certificados antiguos a fin de restaurar la comunicación agente-servidor.

65. El producto también permite el uso de un certificado SSL personalizado firmado por un tercero como Verisign. Hay que tener en cuenta que el producto proporciona los mecanismos necesarios para soportar la integración de un certificado, pero no la generación, validación y solución de problemas que conlleva un certificado de terceros. Para obtener un certificado personalizado SSL para utilizar en McAfee ePO es necesario llevar a cabo la siguiente lista de pasos:

1) Crear una nueva clave privada utilizando OpenSSL haciendo uso de una longitud de 2048 bits y cifrarla haciendo uso de aes128:

```
openssl> genrsa -aes128 -out c:\ssl\keys\mcafee.key 2048
```

2) Crear una CSR con los nombres *subj alt*, ejecutando el siguiente comando, sustituyendo los valores correctos cuando sea necesario.

NOTA: el valor CN corresponde con lo que se emite el certificado, ya sea el nombre FQDN o NETBIOS del servidor. Si ePO está agrupado, use el nombre del clúster virtual. Esos valores se introducen en el campo de asunto del certificado:

```
openssl req -key c:\ssl\keys\mcafee.key -config sancert.cnf -new -subj "/C=US/ST=state/L=city/O=OrgName/OU=domain.com/CN=servername.domain.com" -out c:\ssl\keys\mcafee.csr
```

3) Para obtener el certificado del servidor, proporcionar el CSR al CA de la empresa encargada del certificado personalizado. Un certificado SSL personalizado puede ser certificado utilizando:

4) Un ECA (un dominio CA de Windows): en el controlador de dominio, se debe de ejecutar el siguiente comando. Este comando fuerza el uso de una plantilla del servidor web que genera el certificado del servidor:

```
certreq -submit -attrib "CertificateTemplate: WebServerV2" c:\ssl\keys\mcafee.csr
```

5) Una CA procedente de un tercero, como Verisign o Entrust: Una CA de terceros puede proporcionar un fichero de certificado único (*en formato .cer*) o a veces proporciona más de un fichero de certificado (*formato .crt*), como, por ejemplo:

- Un certificado raíz representado el certificado raíz.

- Un certificado para un certificado intermedio.
- El certificado del servidor en sí mismo.
  Estos tres ficheros de certificados están combinados en un formato propio para ePO para utilizarlos en los siguientes pasos. Pero, si la CA puede proporcionar el certificado en formato PKCS#7, no es necesario convertirlo. Puede proporcionarse el archivo resultante a ePO (con formato .cer). Es posible que sea necesario modificar el nombre del archivo a *.p7b*.

6) Para utilizar un certificado personalizado SSL con ePO y tener presente la cadena de certificados entera, es necesario seguir los siguientes pasos:

i. Combinar los ficheros en formato *.crt*.

ii. Exportarlos como un fichero con formato *.pb7.*

iii. Utilizar el asistente de exportado de certificados de Windows o utilizar OpenSSL para utilizar el siguiente comando:

```
openssl> crl2pkcs7 -nocrl -certfile cert1.crt -certfile cert2.crt -certfile cert3.crt -out outfile.p7b
```

7) Crear una versión sin cifrar de la clave privada para ser utilizada como entrada en ePO:

```
openssl> rsa -in c:\ssl\keys\mcafee.key -out c:\ssl\keys\unsecured.mcafee.pem
```

8) Utilizar el nuevo certificado y la clave privada para ser utilizada como entrada en ePO:

i. Iniciar sesión en la consola ePO.

ii. Clic en Menú → Configuración → Configuración del servidor.

iii. Clic en Certificado de servidor bajo la opción Categorías de configuración, después hacer clic en Editar.

iv. Seleccionar Utilizar el certificado proporcionado y la clave privada.

v. Clic *Navegar* en el campo del certificado (P7B, PEM), localizar y seleccionar el fichero del certificado (en formato *.pb7* o *.cer*), después hacer clic en *Abrir.*

vi. Clic Guardar.

vii. Reiniciar los servicios ePO del sistema Windows en *services.msc*.

- McAfee ePolicy Orchestrator 5.10.0 Application Server.
- McAfee ePolicy Orchestrator 5.10.0 Event Parser.
- McAfee ePolicy Orchestrator 5.10.0 Server.

5.6.2 CASO 2. CERTIFICADOS UTILIZADOS PARA LA COMUNICACIÓN ENTRE COMPONENTES

66. El producto utiliza certificados para realizar la comunicación entre el componente DLP y el componente McAfee ePO. Para garantizar que la comunicación es confiable y evitar que un componente sea suplantado, el producto realiza lo que se conoce como *CA pinning* y, por tanto, para que un cliente establezca una comunicación segura con un servidor, debe de disponer de un certificado firmado por la CA de confianza de McAfee, independientemente de los certificados que tenga instalados el equipo. Esta CA se genera durante la instalación del servidor ePO de forma automática y a su vez, a través de esta CA, se genera otro certificado de agente para el instalador de la máquina cliente. Esta medida, además, serviría como un mecanismo de protección frente a ataques *TLS Downgrade* y así se garantiza el uso del protocolo de comunicaciones TLSv1.2 al realizar la comunicación entre los componentes que conforman al producto.

5.7 SERVIDORES DE AUTENTICACIÓN

67. El producto permite el registro de servidores para permitir la integración de software con otros servidores externos así como para dar soporte a los tres tipos de autenticación mencionados en *5.2.AUTENTICACIÓN*. Uno de los servidores que permite registrar es un servidor LDAP para llevar a cabo la autenticación de usuarios.
68. Además, el producto también permite la autenticación mediante certificado, posibilitando así una adaptación al entorno donde se realice el despliegue.

5.7.1 AUTENTICACIÓN MEDIANTE ACTIVE DIRECTORY

69. El producto permite llevar a cabo el despliegue de servidores LDAP de varias formas. Una vez que los servidores se registren y la autenticación de Windows esté configurada, no sería necesario modificar la configuración.
70. El esfuerzo requerido para configurar completamente la plataforma depende de la topología de red y la distribución de las cuentas de usuario a través de la red:

    1) Si las credenciales para los usuarios están contenidas en un pequeño conjunto de dominios o servidores en un único árbol de dominio, hay que registrar la raíz del árbol.

    2) Si las cuentas de usuario están más dispersas, registrar un número de servidores o dominios. Determinar un número mínimo de sub árboles de dominio o servidores y registrar las raíces de esos árboles. Se deben de registrar en orden de uso. Situar los dominios más utilizados en lo alto de esta lista mejorará el rendimiento medio del proceso de autenticación.

71. Para que los usuarios puedan iniciar sesión en un servidor McAfee ePO utilizando la autenticación de Windows, es necesario adjuntar un conjunto de permisos al grupo de Active Directory en el dominio al que pertenece su cuenta. Al determinar cómo se asignan los conjuntos de permisos, es necesario considerar las siguientes capacidades:

    1) Los conjuntos de permisos pueden asignarse a múltiples grupos de Active Directory.

    2) Los conjuntos de permisos pueden asignarse dinámicamente sólo a un grupo completo del Active Directory. No pueden ser asignados a sólo algunos usuarios en un grupo.

72. Si es necesario asignar permisos especiales a un usuario individual, es posible hacerlo creando un grupo de Active Directory que contenga sólo ese usuario.

73. McAfee ePO puede simplificar el proceso de gestionar usuarios creando automáticamente usuarios en Windows basados en su grupo del Active Directory. Para habilitar esta característica, se deben de realizar los siguientes pasos:

    1) La característica *Inicio de sesión de Active Directory* debe de estar habilitada. Esta característica se puede habilitar mediante el menú *Configuración de servidor* el cual permite al usuario registrado generar automáticamente cuando las siguientes condiciones se cumplen:

- Los usuarios proporcionan credenciales válidas, utilizando el formato *dominio**nombre*.
- Un servidor de Active Directory que contiene información sobre este usuario que ha sido registrado con McAfee ePO.
- El usuario es un miembro de al menos un grupo dominio local o un dominio global que mapea aun conjunto de permisos de McAfee ePO.
- Al menos un permiso debe de estar mapeado al grupo de usuario de Active Directory.

    2) Un servidor LDAP registrado debe de estar configurado para el dominio, por lo que McAfee ePO puede determinar que los miembros del grupo pertenecen verdaderamente al domino.

74. Para habilitar la autenticación mediante credenciales de Windows en el servidor McAfee ePO hay que realizar los siguientes pasos:

    1) Parar el servicio McAfee ePO antes de comenzar la activación del menú de *Autenticación de Windows* en la configuración del servidor.

    2) Desde la consola del servidor, seleccionar Inicio -> Configuración -> Panel de control -> Herramientas administrativas

    3) Seleccionar *Servicios*.

    4) En la ventana anterior, hacer clic derecho en *McAfee ePolicy Orchestrator Servidor de aplicaciones* y seleccionar *Parar.*

5) Renombrar el fichero *Winauth.dll* a *Winauth.bak.* En una instalación por defecto, este fichero se encuentra situado en *C:\Program Files\McAfee\ePolicy Orchestrator\Server\bin*.

6) Reiniciar el servidor. La siguiente vez que se abra la página de *Configuración del servidor*, la opción *Autenticación de Windows* aparecerá.

75. Para configurar la autenticación avanzada de Windows, es posible hacerlo mediante varias vías. No obstante, en primer lugar, hay que tener en cuenta los siguientes puntos:

1) ¿Se quieren utilizar varios controladores de dominio?

2) ¿Hay muchos usuarios dispersos a través de múltiples dominios?

3) ¿Se quiere hacer uso de un servidor WINS para comprobar a través de qué servidores se autentican los usuarios?

76. Los pasos para realizar la configuración de autenticación avanzada de Windows son los siguientes:

1) Seleccionar Menú → Configuración → Configuración del servidor, después seleccionar Autenticación de Windows de la lista de Categorías de configuración.

2) Hacer clic en *Editar*.

3) Especificar si se quiere hacer uso de uno o más dominios, uno o más controladores de dominios o un servidor WINS. Los dominios deben de proporcionarse en un formato DNS y los controladores de dominio y los servidores WINS deben de tener nombre de dominios completamente cualificados.

NOTA: es posible especificar múltiples dominios o controladores de dominio, pero solamente un servidor WINS.

4) Hacer clic en guardar para finalizar la adición de servidores.

77. Como resultado, el servidor McAfee ePO intentará autenticar a usuarios con servidores del modo en el que se ha configurado. Al seguir una lista de preferencia, el producto comenzará con el primer servidor de la lista y continuará recorriendo la lista hasta que el usuario se autentique correctamente.

5.7.2 AUTENTICACIÓN MEDIANTE CERTIFICADO

78. Por último, es necesario tener en cuenta la autenticación mediante el uso de certificados. Esto permitirá a los usuarios acceder a la interfaz de configuración de McAfee ePO con un certificado válido en lugar de usuario y contraseña.

79. Antes de comenzar con el uso de este tipo de autenticación, hay que habilitar el método de autenticación y cargar un certificado CA firmado. También es necesario tener en cuenta que se debe de tener un certificado firmado en los formatos

soportados: P7B, PKCS12, DER, o PEM. Los pasos a seguir para llevar a cabo la configuración del producto a través de la interfaz de McAfee ePO, para utilizar este tipo de autenticación son los siguientes:

1) Abrir la página Editar autenticación basada en certificado.
2) Seleccionar Menú → Configuración → Configuración del servidor.
3) En la lista incluida en Categorías de configuración, seleccionar Autenticación basada en certificado, y hacer clic en Editar.
4) Seleccionar Habilitar autenticación basada en certificado.
5) En la sección *Certificado CA para certificado cliente*, hacer clic en *Navegar,* navegar y seleccionar el fichero del certificado y hacer clic en *OK.* Cuando el fichero sea aplicado, el mensaje mostrado cambia a *Reemplazar certificado CA actual.*

   NOTA: Reemplazar el certificado cuando expira, o si los requisitos de seguridad de la organización cambian.

6) (Opcional) Si se proporciona un certificado PKCS12, hay que introducir la contraseña asociada.
7) Configurar cualquier opción adicional necesaria.
8) Si se tiene una lista de revocación de certificados (CRL), hacer clic en *Navegar,* navegar y seleccionar el fichero CRL, después hacer clic en OK.

   NOTA: El fichero CRL debe de tener formato PEM.

9) (Opcional) Como alternativa o método adicional de comprobar la autenticidad del certificado, hay que configurar el *Online Certificate Status Protocol (OCSP)*. Para ello:

- Clic en Habilitar comprobación OCSP.
- Introducir la dirección URL en el servidor OCSP.
- (Opcional) Seleccionar *Activar comprobaciones de puntos de distribución de CRL cuando el servidor de McAfee ePO no reciba respuesta de OSCP.* Si la conexión a la URL de OCSP predeterminada falla, McAfee ePO intentará conectarse a la lista CRL incluida anteriormente.
- (Opcional) Seleccionar Convertir la URL de OCSP predeterminada en la URL de OCSP principal. Si la conexión falla, McAfee ePO recurrirá a otro operador OCSP si se ha mencionado en Acceso a la información de entidad emisora.

10) Para requerir autenticación basada en certificado para todos los usuarios remotos, hacer clic en *Los usuarios remotos utilizan el certificado para iniciar sesión*.

11) Para hacer que el nombre de usuario sea igual que el del sujeto del *nombre distintivo (Distinguised Name (DN))* especificado en el certificado, hacer clic en *El nombre de usuario del certificado predeterminado es el DN del sujeto*.

12) Configurar la opción *Integración con Active Directory*.

Importante: Para que esta configuración funcione, se debe de habilitar el inicio de sesión a través de *Active Directory* y el grupo de usuario añadido al conjunto de permisos.

13) Para asignar los usuarios de Active Directory automáticamente al conjunto de permisos, hay que seleccionar la opción *Asignar automáticamente permiso para el inicio de sesión de usuario con un certificado de Active Directory.*

14) Para crear automáticamente una cuenta de usuario de McAfee ePO a cualquier usuario que acceda a McAfee ePO con el certificado AD válido, seleccionar *Crear automáticamente usuarios para propietarios de certificados de Active Directory.*

15) Guardar la configuración mediante *Guardar*.

16) Reiniciar McAfee ePO para activar la autenticación mediante certificado.

5.8 SINCRONIZACIÓN HORARIA

80. El producto permite llevar a cabo una sincronización segura de sí mismo y de sus componentes mediante el uso del protocolo NTP (*Network Time Protocol*). Es posible hacer uso de este protocolo realizando los siguientes pasos desde la interfaz de gestión de McAfee ePO (desde el panel *Catálogo de directivas* → *Gestión de appliance común* → *General* → *<nombre de directiva>,* configurar *Fecha y tiempo*:

    1) Seleccionar la zona horaria requerida de la lista.
    2) Habilitar el protocolo NTP seleccionando *Habilitar NTP*.
    3) Para definir un servidor NTP, hay que hacer clic en el icono "+".
    4) Introducir los detalles del servidor.
    5) Hacer clic en "Actualizar".

5.9 ACTUALIZACIONES

81. El producto y sus componentes pueden ser actualizados de forma automática a través de la interfaz de McAfee ePO. Para ello, es necesario seguir los siguientes pasos:

    1) Hacer clic en Menú → Software → Catálogo Software.
    2) En la página *Catálogo Software,* en la lista incluida en *Categoría,* seleccionar una de las siguientes categorías o utilizar el cuadro de búsqueda para encontrar el software que se quiere actualizar:

- *Actualizaciones disponibles.* Lista cualquier actualización disponible de los componentes software que cubre la licencia instalado y comprueba su estado en el servidor McAfee ePO.
- *Evaluación*. Muestra el software de evaluación instalado o incorporado en este servidor.
- *Categorías de producto:* Muestra el software instalado y con licencia.

3) Una vez decidido cuál es el software a actualizar, hay que seleccionar una acción que aplique a todos los componentes software o a los componentes de forma individual.

4) Para todos los componentes en el software, hacer clic:

- *Incorporar todos* para incorporar todos los componentes del producto nuevo en el servidor.
- *Actualizar todos* para actualizar todos los componentes del producto existente en el servidor.
- *Quitar todos* para borrar todos los componentes del producto existente en este servidor.

5) Para componentes individuales en el software, hacer clic en:

6) *Descargar* para descargar el software o la documentación del producto en una localización de la red.

- *Incorporar (rama)* para incorporar un paquete de producto nuevo en este servidor.
- *Incorporar* para incorporar una extensión de producto nueva en este servidor.
- *Actualizar* para actualizar un paquete o extensión existentes ya instalados o incorporados en este servidor.
- *Eliminar* para desinstalar un paquete o extensión ya instalado o incorporado en este servidor.

7) Bajo la opción *Incorporar,* se debe revisar y aceptar los detalles del producto y el Acuerdo de licencia de usuario final (EULA), seleccionar la *Rama del paquete cliente,* y hacer clic en *Incorporar* para finalizar la operación.

82. Con carácter adicional, es posible habilitar la actualización global en los servidores para desplegar de forma automática los paquetes de actualización software. Para ello, se pueden seguir los siguientes pasos:

1) Hacer clic en *Menú* → *Configuración* → *Configuración del servidor,* seleccionar *Actualización global,* después hacer clic en *Editar* en la parte inferior de la página.

2) En la página siguiente de *Estado* hacer clic en *Editar actualización global* y seleccionar *Activado.*

3) Si se desea, modificar el intervalo *Intervalo de ejecución aleatoria*. Cada actualización de cliente se realizará en un tiempo aleatorio en función del intervalo seleccionado, el cual ayuda a distribuir la carga de red. El tiempo por defecto es de 20 minutos.

4) La siguiente página es *Tipos de paquetes* dónde hay que seleccionar los paquetes a iniciar por la actualización. La actualización global inicia una actualización solamente si hay nuevos paquetes para los componentes especificados en el *Repositorio principal y* o los que se han movido en otra rama. Hay que seleccionar estos componentes con cuidado.

5) *Firmas y motores* – Seleccionar *Contenido de Host Intrusion Prevention,* si es necesario.

Nota: La selección de un tipo de paquete determina qué inicia una actualización global (no qué se actualiza durante el proceso de actualización global). Los agentes reciben una lista de paquetes a actualizar durante el proceso de actualización global. Los agentes utilizan esta lista para instalar solamente las actualizaciones que se necesiten.

6) Cuando se finalice el proceso, hay que hacer clic en *Guardar* para guardar los cambios. Una vez habilitados, la actualización global inicia una actualización la siguiente vez que se compruebe alguno de los paquetes actualizados o aquellos que se han movido a otra rama.

Nota: Es necesario asegurarse de ejecutar una tarea *Extraer ahora* y hacer una programación de una tarea recurrente *Extracción del repositorio* cuando se esté preparado para iniciar una actualización automática.

5.10 SNMP

83. Antes de realizar la configuración del protocolo SNMP es necesario llevar a cabo el registro del servidor SNMP de forma previa. Para ello es necesario seguir los siguientes pasos:

1) En la interfaz web de McAfee ePO, seleccionar el menú Menú → Configuración –> Servidores registrados, después hacer clic en Nuevo servidor.

2) Desde el menú *Tipo de servidor* de la página de *Descripción*, seleccionar *Servidor SNMP,* proporcionar el nombre y cualquier información adicional sobre el servidor y después hacer clic en *Siguiente.*

3) Desde el desplegable *URL,* seleccionar uno de los siguientes tipos de dirección de servidor, después introducir las direcciones:

- Nombre DNS – Especifica el nombre DNS del servidor registrado.
- IPv4 – Especifica la dirección IPv4 del servidor registrado.
- IPv6 – Especifica el nombre DNS del servidor registrado el cuál dispone de una dirección IPv6.

4) Seleccionar la versión SNMP que utilizará el servidor. Se recomienda el uso de la versión 3 del protocolo, para el cuál será necesario rellenar los detalles incluidos en *Seguridad SNMPv3.*

5) Hacer clic en *Enviar captura de prueba* para probar la configuración.

6) Hacer clic en *Guardar* para guardar los cambios.

84. Una vez registrado el servidor SNMP, es necesario llevar a cabo la configuración de forma segura del protocolo SNMP a través los siguientes pasos:

1) Desde el menú Catálogo de directivas → Ajustes generales de Administración de Appliances → General → <nombre de directiva> → SNMP se realiza la configuración de las alertas SNMP:

- Habilitar alertas SNMP.
- Introducir la dirección o el nombre del equipo como *Destino de la captura*.
- Introducir el *Nombre de la comunidad* que se ha establecido para el sistema de gestión SNMP.
- Seleccionar la versión requerida del protocolo SNMP. Se recomienda el uso de la versión 3 del protocolo (SNMP v3).
- (Opcional) Hacer clic en el símbolo "+" y repetir los pasos *ii* a *iv* para añadir más de una captura de destino.

2) Configurar SNMP Monitor:

- Habilitar *Monitor* SNMP.
- Seleccionar la versión del protocolo SNMP utilizado por el sistema de gestión SNMP. Se recomienda el uso de la versión 3 del protocolo SNMP.

3) Para la versión v3 de SNMP, hay que llevar a cabo los siguientes pasos:

- Introducir un nombre de usuario que se ha configurado para el sistema de gestión SNMP.
- Introducir el protocolo de autenticación, es posible seleccionar MD5 o SHA. Se recomienda el uso del protocolo SHA.
- Introducir el protocolo de privacidad. Se puede seleccionar entre el protocolo DES o AES. Se recomienda el uso del protocolo AES.
- Introducir la frase de contraseña de autenticación.
- Introducir la frase de contraseña de privacidad.

4) Seleccionar Permitir la supervisión de SNMP para todos los hosts o Permitir la supervisión SNMP de estos hosts únicamente. Si se ha seleccionado Permitir la supervisión SNMP de estos hosts únicamente, es necesario configurar al menos un host antes de poder guardar los ajustes de SNMP.

5) Hacer clic *Guardar* para guardar estos cambios, o en *Duplicar* para crear una directiva utilizando estos ajustes.

85. Es posible llevar a cabo la descarga de los ficheros *MIB* y *SMI* para visualizar las capturas de SNMP y los contadores que están disponibles para los componentes desplegados.

5.11 ALTA DISPONIBILIDAD

86. En el caso de que sea necesario, el producto puede ser configurado para equilibrar la carga del tráfico entrante y asegurar una alta disponibilidad de las

funcionalidades ofrecidas por el producto. Es posible configurar dos o más componentes McAfee DLP Prevent siempre y cuando se configure una red local LAN 1 conectada al mismo segmento de red. Todos los componentes de un *clúster* deben de estar en la misma subred o red. Para ello, es necesario seguir los siguientes pasos:

1) En el servidor McAfee ePO, abrir el catálogo *Catálogo de directivas.*
2) Seleccionar el producto *Administración de appliances de DLP,* elegir la categoría *General,* y abrir la directiva que se desea editar.
3) Habilitar la opción *Equilibrio de carga*.
4) En el identificador del clúster *ID de clúster*, hacer uso de las flechas de dirección para seleccionar el número que servirá de identificador del clúster.
5) En el campo *Dirección IP virtual*, introducir una dirección IP para que los paquetes de la dirección IP virtual sean enviados al *clúster* principal. Los componentes del clúster utilizan la máscara de red asignada a la dirección IP física. La dirección IP virtual debe de estar creada en la misma subred o red como los otros dispositivos McAfee DLP Prevent, y no puede ser la misma dirección IP que cualquier otro dispositivo que forme parte del clúster.

87. Como resultado, McAfee ePO transmitirá la configuración realizada a todos los componentes del clúster cuando se apliquen los cambios. Será necesario esperar un tiempo de cinco minutos para que clúster se estabilice e identifique el clúster principal y los escáneres del clúster. Las descripciones de los componentes cambiarán en consecuencia en *Administración de appliances*.
88. Con carácter adicional, será necesario llevar a cabo un procedimiento similar para balancear la carga del análisis del tráfico entrante y por lo tanto se puede establecer un clúster de componentes *McAfee DLP Monitor*.
89. Antes de proceder a la configuración de este clúster hay que tener en cuenta las siguientes consideraciones:
    1) Configurar el componente McAfee DLP Monitor para el rol de clúster mediante el asistente de instalación.
    2) Configurar dos o más componentes McAfee DLP Monitor en una LAN 1 conectados al mismo segmento de la red.
    3) Todos los componentes deben de estar desplegados en la misma subred o red.
90. Los pasos para llevar a cabo la configuración de este clúster son los siguientes:
    1) En el servidor McAfee ePO, abrir el *Catálogo de directivas.*
    2) Seleccionar el producto *Administración de appliances de DLP <Versión>,* elegir la categoría *General,* y abrir la política que se desea editar.
    3) Habilitar la opción *Equilibrio de carga*.

4) En el identificador del clúster *ID de clúster*, hacer uso de las flechas de dirección para seleccionar el número que servirá de identificador del clúster.

5) En el campo *Dirección IP virtual*, introducir una dirección IP para que los paquetes de la dirección IP virtual sean enviados al *clúster* principal. Los appliances del clúster utilizan la máscara de red asignada a la dirección IP física. La dirección IP virtual debe de estar creada en la misma subred o red como los otros dispositivos McAfee DLP Monitor, y no puede ser la misma dirección IP que cualquier otro appliance que forme parte del clúster.

Precaución: El identificador del clúster y la dirección IP virtual deben de ser la misma para todos los miembros que conforman un clúster.

91. Como resultado, McAfee ePO transmitirá la configuración realizada a todos los componentes del clúster cuando se apliquen los cambios. Será necesario esperar un tiempo de cinco minutos para que clúster se estabilice e identifique el clúster principal y los escáneres del clúster. Las descripciones de los componentes cambiarán en consecuencia en *Administración de appliances*.

5.12 AUDITORÍA

5.12.1 REGISTRO DE EVENTOS

92. El registro de auditoría registra todas las acciones de usuario del producto. Estos registros se incluyen en el *Registro de auditoría* del producto y consisten en una lista de información que crecerá de acuerdo al funcionamiento del producto y de sus componentes.

93. Estas entradas podrán ser consultadas mediante el *Generador de consultas* para realizar búsquedas en base a parámetros o bien es posible utilizar las consultas predeterminadas aplicables a esos datos.

5.12.2 ALMACENAMIENTO LOCAL

94. El producto almacena de forma local en el equipo donde se encuentra desplegado el servidor McAfee ePO toda la información referente a los registros de auditoría. Por defecto, este es el comportamiento del producto y es posible visualizar dichos registros de auditoría, posible hacerlo desde la interfaz de McAfee ePO en *Menú → Informes → Registro de auditoría.*

95. Es importante tener en cuenta que es posible borrar de forma periódica las acciones del log de auditoría para mejorar el rendimiento de la base de datos, al tratarse de un registro en continuo crecimiento. Para ello, es necesario llevar a cabo los siguientes pasos:

1) Abrir el menú Menú → Informes → Registros de auditoría.

2) Hacer clic en *Purgar.*

3) En el diálogo emergente, seleccionar una unidad de tiempo.

4) Hacer clic en *OK.*

96. Con carácter adicional, es posible crear una tarea en el servidor para que automáticamente se eliminen los registros de auditoría antiguos. Para ello, hay que llevar a cabo los siguientes:

1) Abrir el menú Generador de tareas de servidor, seleccionar Menú → Automatización → Tareas servidor, después hacer clic en Acciones → Nueva tarea.

2) Escribir un nombre para la tarea, como por ejemplo *Borrar eventos*, añadir una descripción y después hacer clic en *Siguiente*.

3) En la sección de *Acciones,* se pueden configurar entre las siguientes opciones (es posible incluir todas las acciones en una misma tarea):

4) *Purgar Registro auditoría* – Eliminar registros más antiguos de 6 meses.

5) *Purgar eventos de cliente* – Eliminar registros más antiguos de 6 meses.

6) *Purgar log de tareas del servidor* – Eliminar registros más antiguos de 6 meses.

7) Purgar log de eventos de amenaza – Eliminar registros cada día.

8) *Purgar eventos SiteAdvisor Enterprise* – Eliminar registros después de 10 días.

9) Hacer clic en *Siguiente* y programar la tarea para que sea ejecutada cada día fuera del horario de trabajo.

10) Hacer clic en la sección *Resumen,* para confirmar que la tarea de servidor es correcta y está bien configurado acorde a lo requerido, después hacer clic en *Guardar* para guardar los cambios.

5.12.3 ALMACENAMIENTO REMOTO

97. El producto permite llevar a cabo el registro de servidores *syslog* para exportar la información de auditoría a un servidor externo. Para realizar el registro de un servidor, es necesario seguir los siguientes pasos:

1) Seleccionar Menú –> Configuración → Servidores registrados, hacer clic en Nuevo servidor.

2) Desde el menú *Tipo de servidor* de la página de *Descripción*, seleccionar *Servidor Syslog,* para especificar un nombre único y cualquier otro detalle. Después, hacer clic en *Siguiente.*

3) Desde la página *Generador de servidores registrados*, modificar lo siguiente:

4) *Nombre de servidor* – Utilizar el nombre de dominio y un nombre de dominio completo o una dirección IP para el servidor.

5) *Número de puerto TCP* – Incluir el puerto TCP del servidor syslog. El puerto por defecto es 6514.

6) *Habilitar reenvío de eventos* – permite activar el reenvío de eventos desde el *controlador de agentes* a este servidor de Syslog.

7) *Prueba* – Probar la conexión con el servidor syslog.

8) Guardar los cambios mediante *Guardar.*

5.13 BACKUP

98. El producto dispone de un modo de recuperación frente a desastres que permite una rápida recuperación y reinstalación del servidor McAfee ePO.

99. Para recuperar el entorno del servidor McAfee ePO, es necesario tener una copia de respaldo de los datos que permita hacer posible dicha recuperación. Los datos que hacen el entorno del servidor único, consisten en dos elementos principales: la base de datos y las secciones del sistema de ficheros del servidor. Para ello se hará uso de una *instantánea* de recuperación para poder restaurarlo. Por motivos de seguridad, los ficheros almacenados en dicha *instantánea* estarán cifrados utilizando la frase de contraseña de cifrado del almacén de claves. Esta clave no puede ser recuperada y por tanto es necesario almacenarla debidamente.

100. Una consideración importante es la de disponer de una copia sincronizada con la información de la base de datos para que la recuperación sea exitosa. El monitor del panel instantánea de servidor indica si la instantánea está actualizada.

101. El contenido de esta *instantánea* de recuperación ante desastres incluye los directorios configurados para los ejecutables registrados, pero no los ficheros asociados, los cuales deberán de ser restaurados en el entorno de McAfee ePO. Después de restaurar este entorno, cualquier ejecutable registrado será notificado en caso de que el directorio se encuentre roto o no disponible. Para almacenar una *instantánea* a través del panel de control de McAfee ePO es necesario seguir los siguientes pasos:

    1) Seleccionar Menú → Informes → Paneles y seleccionar Instantánea del servidor de ePO.

    2) Hacer clic en *Tomar instantánea* para comenzar a almacenar la *instantánea* en la base de datos. Durante el proceso, aparecerá una barra del título del *Monitor de instantáneas* cambia para indicar el estado del proceso. El tiempo necesario para realizar la copia dependerá de varios factores, como, por ejemplo, las extensiones de producto instaladas.

    3) (Opcional) Después de que el proceso de instantánea finalice, hacer clic en Ver detalles de la ejecución actual para abrir el Detalles del registro de tareas del servidor.

5.14 SERVICIOS DE SEGURIDAD

102. El propósito del producto y de sus componentes es el de monitorizar la red donde se encuentran desplegados con la finalidad de detectar cualquier posible fuga de información que se produzca. Para ello, es necesario establecer una serie de reglas y opciones de configuración para aumentar su efectividad en base a las necesidades de la red y/o de la organización. Las opciones de configuración del cliente determinan cómo funciona el software. La mayor parte de las opciones de configuración del cliente DLP tienen valores predeterminados razonables que se pueden utilizar para la configuración y las pruebas iniciales sin alteración. Para su configuración, es necesario seguir los siguientes pasos:

1) En McAfee ePO, seleccionar Menú → Directiva → Catálogo de directivas
2) En la lista desplegable *Producto,* seleccionar *Data Loss Prevention 11.*
3) (Opcional) En la lista desplegable *Categoría*, seleccionar *Configuración del servidor.*
4) Seguir uno de los siguientes procedimientos:

- Seleccionar una configuración del servidor para editarla.
- Hacer clic en *Duplicar* para la configuración de *McAfee Default*.

5) (Opcional, solo para McAfee DLP Discover) En la página de *Box*, comprobar las opciones del historial de versiones y de la papelera.
6) En la página Servicio de copia de pruebas:

- Introducir el recurso compartido de almacenamiento y las credenciales. En el caso de McAfee DLP Prevent o McAfee DLP Monitor, especificar un nombre de usuario y una contraseña. No seleccionar la opción de la cuenta de sistema local.
- Introducir la configuración del servidor o aceptar las opciones predeterminadas.
- Si la directiva debe cumplir con regulaciones de privacidad como RGPD, eliminar la selección de la casilla de verificación de información de cadenas coincidentes breves.

7) (Opcional, solo para McAfee DLP Discover) En la página *Registro*, hay que definir el tipo de resultado del registro y el nivel de registro. **Sugerencia:** Hacer uso de los valores predeterminados.
8) (Solo para el servidor de McAfee DLP para dispositivos móviles) En la página del *Proxy ActiveSync*, introducir el nombre DNS del servidor de ActiveSync.
9) En la página Documentos registrados:

- (Solo para McAfee DLP Discover) Comprobar el Recurso compartido de almacenamiento del Servicio de copia de pruebas (establecido en la página Configuración de DLP → General).
- (McAfee DLP Discover y McAfee Network DLP) Comprobar que el Motor de documentos está activado y escribir la dirección IP de DLP Server. El motor de documentos utiliza la API REST para hacer coincidir las huellas digitales

almacenadas en el DLP Server especificado. Si no se hace uso de documentos registrados, es posible desactivar el motor de documentos.

- (Solo para DLP Server) Introducir el nombre, el recurso compartido de almacenamiento UNC y el nombre de usuario para que los recursos compartidos de pruebas puedan cargar los paquetes de documentos registrados en DLP Server.

10) (Solo para McAfee DLP Discover) En la página *Gestión de derechos*, definir las credenciales del servicio de gestión de derechos.

11) (Solo McAfee DLP Discover) En la página *SharePoint*, seleccionar *Utilizar papelera de reciclaje al eliminar un archivo* o anular su selección.

Atención: Si se activa esta opción y el servidor de SharePoint no utiliza la papelera de reciclaje, cualquier acción de tipo *Mover* llevada a cabo en los archivos fallará y se aplicará de forma predeterminada el valor *Copiar*. El valor predeterminado en SharePoint es activar la papelera de reciclaje.

12) (Opcional, solo para McAfee DLP Discover) En la página *Extractor de texto*, hay que establecer las opciones de configuración del extractor de texto. **Sugerencia:** Hacer uso de los valores predeterminados.

- Definir la página de códigos de respaldo ANSI. El valor predeterminado utiliza el idioma predeterminado del servidor de descubrimiento.
- Establecer el tamaño de archivo máximo de entrada y de salida y el tiempo de espera.
- Seleccionar la casilla de verificación *Utilizar OCR* si desea extraer texto de archivos de imagen.

Nota: El reconocimiento óptico de caracteres consume muchos recursos. Si se está analizando una gran cantidad de imágenes puede aumentar significativamente el tiempo de análisis. Anular esta selección de la casilla de verificación cuando no sea necesario analizar el reconocimiento óptico de caracteres.

13) Hacer clic en Aplicar directiva.

14) Una vez aplicada la directiva, la interfaz informará de su correcta puesta en marcha:

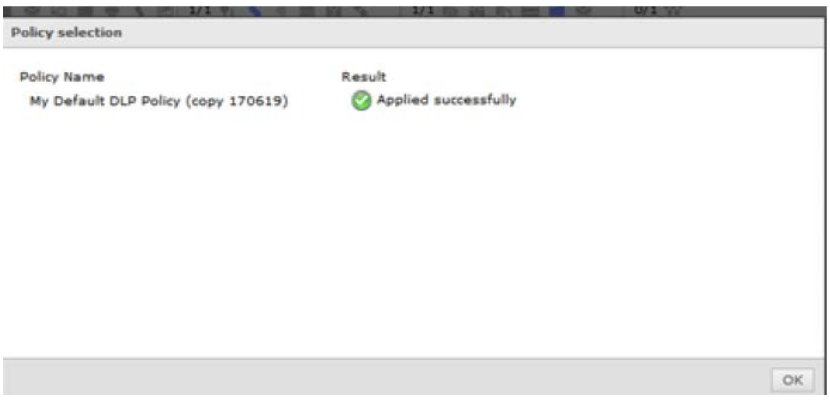

Ilustración 4. Cuadro de política aplicada correctamente

103. Por otra parte, los conjuntos de reglas definen las directivas de McAfee DLP. Un conjunto de reglas puede contener una combinación de reglas de protección de datos, control de dispositivos, descubrimiento y control de aplicaciones. Las definiciones de reglas se aplican a todos los conjuntos de reglas.

104. La página *Conjuntos de reglas* muestra una lista de conjuntos de reglas definidas y el estado de cada una. También figura el número de incidentes registrados para cada uno de los conjuntos de reglas, el número de reglas definidas y el número de reglas activadas. Es posible crear las siguientes definiciones de reglas:

1) **Crear un nuevo intervalo de puertos de red**. Los intervalos de puertos de red funcionan como criterios de filtrado en las reglas de protección de comunicaciones de la red. El procedimiento para la creación de esta regla es el siguiente:

   a) En McAfee ePO, seleccionar Menú → Protección de datos → Administrador de directivas de DLP → Definiciones.
   b) En el panel de la izquierda, seleccionar *Puerto de red* y, a continuación, hacer clic en *Acciones* → *Nuevo.* También es posible editar las definiciones integradas.
   c) Introducir un nombre único y, si se desea, una descripción.
   d) Introducir los números de puerto, separados por comas y, si se desea, una descripción; después, hacer clic en *Agregar.*
   e) Cuando se haya agregado todos los puertos necesarios, hacer clic en *Guardar.*

2) **Creación de un intervalo de direcciones de red.** Los intervalos de direcciones de red funcionan como criterios de filtrado en las reglas de protección de comunicaciones de la red. Para cada definición requerida, llevar a cabo los pasos del 1 al 4. El procedimiento para llevar a cabo la creación de esta regla es el siguiente:

   a) En McAfee ePO, seleccionar Menú → Protección de datos → Administrador de directivas de DLP → Definiciones.
   b) En el panel de la izquierda, seleccionar *Dirección de red (dirección IP)* y, a continuación, hacer clic en *Acciones* → *Nuevo.*
   c) Introducir un nombre único y, si se desea, una descripción.
   d) En el cuadro de texto, introducir una dirección, un intervalo o una subred. Hacer clic en *Agregar.* En la página se mostrarán ejemplos con el formato correcto.

   Nota. Se admiten únicamente direcciones IPv4. Si se introduce una dirección IPv6, aparecerá el mensaje *La dirección IP no es válida* en lugar de indicarse que no se admite.

   e) Cuando se haya agregado todas las direcciones necesarias, hacer clic en Guardar.

3) **Crear** una **definición de lista de direcciones de correo electrónico.** Las definiciones de lista de direcciones de correo electrónico son dominios de correo electrónico predefinidos o direcciones de correo electrónico

específicas que pueden incluirse en las reglas de protección de correo electrónico. Para crear este tipo de regla, hay que seguir los siguientes pasos:

a) En McAfee ePO, seleccionar Menú → Protección de datos → Administrador de directivas de DLP → Definiciones.
b) En el panel de la izquierda, seleccionar Lista de direcciones de correo electrónico y, a continuación, hacer clic en Acciones → Nuevo.
c) Introducir un Nombre y se desea una Descripción.
d) Seleccionar un Operador de la lista desplegable. Los operadores definidos con la opción Direcciones de correo electrónico admiten caracteres comodines en el campo Valor.

Nota: Las reglas de protección de correo electrónico que se implementan en McAfee DLP Prevent o McAfee DLP Monitor no coinciden con los operadores *Nombre para mostrar.*

e) Introducir un valor y, a continuación, hacer clic en *Agregar.*
f) Hacer clic en *Guardar* cuando se haya acabado de agregar direcciones de correo electrónico.

4) **Crear una definición de la impresora de red.** Hacer uso de definiciones de la impresora de red para crear reglas específicas de protección contra impresión. Las impresoras definidas pueden incluirse en reglas o excluirse de estas. Antes de comenzar, es necesario disponer de una ruta UNC de la impresora de red. El procedimiento a seguir es el siguiente:

a) En McAfee ePO, seleccionar Menú → Protección de datos → Administrador de directivas de DLP → Definiciones.
b) En el panel de la izquierda, seleccionar *Impresora de red* y, a continuación, hacer clic en *Acciones → Nuevo.*
c) Introducir un *Nombre* único y, si se desea, una *Descripción*.
d) Introducir la ruta *UNC*. Todos los demás campos son opcionales.
e) Hacer clic en *Guardar.*

5) **Crear una definición de lista de URL.** Las definiciones de listas de URL se utilizan para definir las reglas de protección web y los criterios de clasificación de identificación de huellas digitales de contenido web. Se añaden a las reglas y clasificaciones como condiciones de *Dirección web (URL)*. El procedimiento para llevar a cabo la creación de la regla es el siguiente:

a) En McAfee ePO, seleccionar Menú → Protección de datos → Administrador de directivas de DLP → Definiciones.
b) En el panel de la izquierda, seleccionar *Lista de URL* y¸ a continuación, selecciona *Acciones → Nuevo.*
c) Introducir un *Nombre* único y una *definición* opcional.
d) Seguir uno de estos procedimientos:

e) Introducir información de *Protocolo, Host, Puerto y Ruta* en los cuadros de texto y, a continuación, haga clic en *Agregar.*

Nota: También es posible agregar una cadena de consulta opcional.

f) Pegar una URL en el cuadro de texto *Pegar URL,* hacer clic en *Analizar* y, a continuación, en *Agregar.* El software rellena los campos de URL.

g) Una vez agregadas a la definición todas las URL requeridas, haga clic en *Guardar.*

6 FASE DE OPERACIÓN

105. Una vez que el producto está configurado de forma segura y se encuentra en un modo de funcionamiento normal, el usuario *administrador* es el encargado de llevar a cabo las siguientes tareas de mantenimiento:

- Comprobaciones periódicas del hardware y software para asegurar que no se ha introducido hardware o software no autorizado.
- Aplicación regular de los parches de seguridad, con objeto de mantener una configuración segura.
- Actualizaciones periódicas del software de los equipos, para garantizar que están al día, tanto en las capacidades de reconocimiento de aplicaciones, como en la prevención de amenazas.
- Mantenimiento de los registros de auditoria. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
- La información de auditoria se guardará en las condiciones y por el periodo establecido en la normativa de seguridad.
- Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

7 CHECKLIST

La siguiente *checklist* contiene todas las recomendaciones sobre la configuración relativas al producto:

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Consideraciones previas	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro de las licencias	☐	☐	
Actualización de firmware	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado	☐	☐	
Elegir mecanismo de autenticación.	☐	☐	
Configuración de administradores	☐	☐	
Configuración de interfaces puertos y servicios	☐	☐	
Configuración de protocolos seguros	☐	☐	
Gestión de certificados	☐	☐	
Asignar servidor de autenticación (si es necesario)	☐	☐	
Sincronización horaria (servidor NTP)	☐	☐	
Configuración de actualizaciones automáticas	☐	☐	
Configuración protocolo SNMP	☐	☐	
Configurar Alta Disponibilidad	☐	☐	
Auditoría. Almacenamiento remoto (si aplica)	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Servicios de seguridad. Configuración reglas DLP.	☐	☐	

8 REFERENCIAS

CCN-STIC-807	Criptología de empleo en el Esquema Nacional de Seguridad, abril 2017
DLP_IG	McAfee Data Loss Prevention 11.1.x Installation Guide.
DLP_END_IG	McAfee Data Loss Prevention Endpoint 11.1.x Installation Guide.
DLP_MON_IG	McAfee Data Loss Prevention Monitor 11.1.x Installation Guide.
DLP_PREV_IG	McAfee Data Loss Prevention Prevent 11.1.x Installation Guide.
ePO_IG	McAfee ePolicy Orchestrator 5.10.0 Installation Guide.
AG_IG	McAfee Agent 5.5.1 Product Guide (McAfee ePolicy Orchestrator).
MA_CC	McAfee Data Loss Prevention 11.1 Common Criteria Evaluated Configuration Guide.
AG_PG	McAfee Agent 5.5.1 Product Guide
ePO_PG	McAfee ePolicy Orchestrator 5.10.0 Product Guide
DLP_PG	McAfee Data Loss Prevention 11.1.x Product Guide

9 ABREVIATURAS

ENS	Esquema Nacional de Seguridad.
API	Application Programming Interface
BMC	Baseboard Management Controller, Controlador de administración de placa base
CA c	Certification Authority
CRL	Certificate 'Revocation List
DLP	Data Loss Prevention
DN D	Dintinguised Name
DNS	Domain Name System
EICA	European Institute for Computer Antivirus Research
ePO	ePolicy Orchestator
EULA	End-User License Agreement
HTTP	HyperText Transfer Protocol Secure
ICAP	Internet Content Adaptation Protocol
IIS	Internet Information Services
LAN	Local Area Network, Red de Area Local
LDAP	Lightweight Directory Access Protocol, Protocolo ligero de acceso a directorios
MTA	Mail Transfer Agent
NAT	Network Address Translation
NTP	Network Time Protocol
OCSP	Online Certificate Protocol
RBAC	Role-Based Access Control, Control de acceso basado en roles
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer (SPAN)
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
UDP	User Datagram Protocol
UEBA	User and Entity Behavior Analytics
VDI	Virtual Desktop Infrastructure
WINS	Windows Internet Naming Service