centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1507

Procedimiento de empleo seguro
Forcepoint On-Premise Security 8.5

Noviembre 2021

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.01.27 13:11:59 +01'00'

NIPO: 083-21-211-1
Fecha de Edición: noviembre de 2021.

ÍNDICE

1. INTRODUCCIÓN

1. **On-Premise Security 8.5** proporciona una solución agregada de protección de la navegación de usuarios y prevención de robo de datos, dentro y fuera de la red de la organización. La protección proporcionada por *On-Premise Security* se entrega mediante tres (3) componentes principales, que se gestionan de forma centralizada y unificada desde la plataforma de gestión *Forcepoint Security Manager (FSM)*. Estos son:

    a) ***Forcepoint Web Security.*** Solución para protección de la navegación de los usuarios mediante el filtrado, análisis de aplicaciones cloud, categorización y defensa ante amenazas avanzadas en tiempo real. Solución basada en *proxies*, *appliances* físicos o virtuales, o de forma híbrida, contando con equipos en local y servicios en nube, para acompañar al usuario en todo momento, integrándose de forma nativa con la solución Forcepoint DLP para evitar la fuga de información incluso cuando el usuario se encuentra fuera de la organización.

    b) ***Forcepoint DLP.*** Forcepoint DLP es una solución unificada de protección contra amenazas y prevención de pérdida de datos que identifica y protege datos sensibles en *endpoints*, redes y servicios en la nube. Facilita el cumplimiento, de manera eficiente, de los requerimientos normativos y protege la propiedad intelectual.

    c) ***Forcepoint Email Security.*** Plataforma de protección contra el spam y el phishing en los mensajes de correo electrónico, protegiendo a su vez contra posibles ransomware y otras amenazas persistentes avanzadas antes de que puedan infectar los sistemas. Integrado de forma nativa con la solución Forcepoint DLP para prevenir la fuga de información por correo electrónico. Incluye, entre otras, características de cifrado del email, mensajes de concienciación y educación a usuarios ante cómo evitar ataques por técnicas como phishing. Forcepoint Email Security opera también en infraestructura en nube con las más altas certificaciones de seguridad de la industria para brindar protección en los sistemas cloud más populares como Microsoft Office 365 y Gsuite.

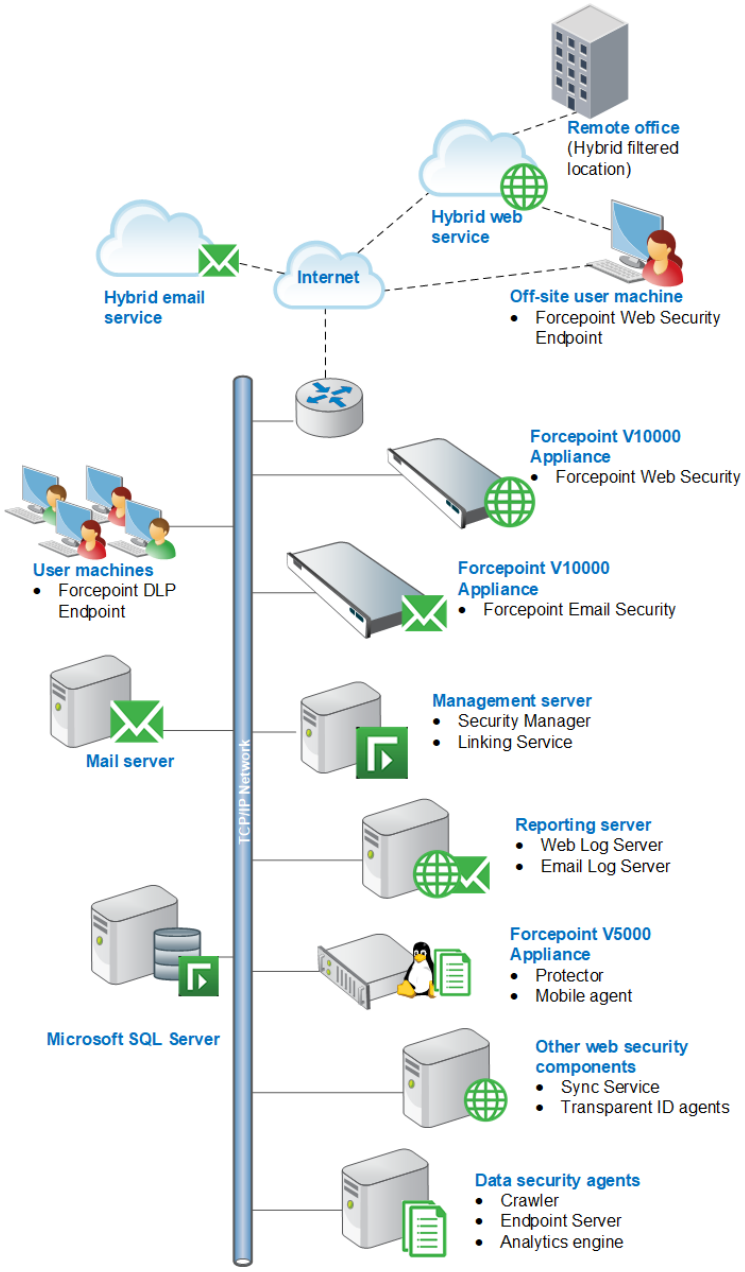

Figura 1 – Diagrama a alto nivel de las soluciones *Forcepoint On-Prem Security*

2. Estos componentes trabajan juntos para evitar infracciones de seguridad, pérdida de productividad y problemas legales que puedan surgir debido a hábitos de navegación, mensajes de correo electrónico y uso de red inapropiado.
3. Los componentes se administran utilizando ***Forcepoint Security Manager (FSM).***
4. La solución de seguridad local es altamente escalable y configurable de acuerdo con las necesidades específicas de cada organización.
5. Estas soluciones pueden estar desplegadas en las instalaciones del cliente, despliegues híbridos o implementaciones basadas en la nube. Sin embargo, **la cualificación de este producto abarca únicamente la solución *on-premise*.**

6. Cada uno de los componentes que integran esta solución puede ser adquirido y licenciado de forma independiente, según las necesidades del cliente y el entorno concreto.

2. OBJETO Y ALCANCE

7. Este Procedimiento de Empleo Seguro tiene como alcance la solución **Forcepoint On-Premise Security 8.5,** ejecutada en *appliances* físicos *Forcepoint V-Series Security Appliances*. Detalla sus principales características de seguridad para la protección ante exfiltración de información sensible.

8. El modelo de *appliance* V10000 G4 es el incluido en el alcance de la cualificación. Estos dispositivos presentan las siguientes especificaciones:

    - *Dell Platform Name: R430*
    - *CPU: Intel E5-2620 v3 X2*
    - *Memory: 32 GB*
    - *Ports:*
        - *4x onboard NICs*
        - *1 x 2 port addon NIC*
        - *VGA display connector*
        - *Serial port connector*
        - *Power supply connector*
    - *On-board NIC: Broadcom 4P 5720*
    - *Addon NIC: Broadcom 2P 5720 or Intel 10G 2P X520 or Intel 10G 2P X520 + Intel 10G 2P X710*
    - *Hard drive: 300GB SAS X4*
    - *RAID controller: PERC H730 Mini*

9. **Este producto ha sido cualificado e incluido en el CPSTIC (a fecha de publicación de esta guía) en las familias "*Sistemas de Prevención de Fuga de Datos*" y "*Proxies*".**

3. ORGANIZACIÓN DEL DOCUMENTO

10. A continuación, se expone en líneas generales el objetivo de cada uno de los diferentes apartados del presente procedimiento:

    1. **Introducción. -** Breve descripción de la solución *Forcepoint On-Prem Security* 8.5, los productos del porfolio de soluciones Forcepoint que la componen y una breve descripción del objetivo funcional de cada una de ellas.
    2. **Objeto y Alcance. -** Exposición del objeto por el que se desarrolla este procedimiento y qué componentes forman parte del alcance de la solución global evaluada.
    3. **Organización del documento.** Presentación de la estructura del presente documento para facilitar su comprensión.
    4. **Servicios de Seguridad.** Identifica las características y funciones de seguridad relevantes que proporcionan cada uno de los componentes de la solución.
    5. **Fase de despliegue e Instalación. -** Descripción de las fases que se cubrirían desde que se adquiere la solución:
        - 5.1. Cómo se suministra al cliente y procedimiento habitual de entrega de los productos hardware y software adquiridos,
        - 5.2. Dónde y cómo debe instalarse la solución para que se despliegue en un entorno con las mayores garantías de seguridad,
        - 5.3. Cómo deben registrarse los productos adquiridos en los sistemas Forcepoint para su correcto licenciamiento,
        - 5.4. Recomendaciones y requerimientos previos a tener en cuenta para el diseño y despliegue;
        - 5.5. Indicaciones a alto nivel que deben seguirse para la correcta instalación de la solución y los componentes *Forcepoint On-Premise* Security en un entorno seguro.
    6. **Fase de Configuración.** Se exponen los procedimientos necesarios para las fases de:
        - 6.1. **Modo de Empleo Seguro.** Incluye las actividades a realizar para disponer de la solución suministrada en el modo seguro requerido FIPS 140-2 y otras recomendaciones adicionales.
        - 6.2. **Autenticación.** Incluye la definición de los métodos de autenticación que se pueden utilizar, tanto para el acceso de la gestión de usuarios con permisos administrativos en la consola FSM y/o en los *appliances* Forcepoint, así como los métodos de autenticación disponibles para los usuarios clientes del servicio ofrecido por la solución.
        - 6.3. **Administración del Producto.** Describe las opciones que proporciona la plataforma en la creación de accesos administrativos mediante

cuentas locales o de red, así como los diferentes perfiles y roles administrativos disponibles.

6.4. **Configuración de interfaces, puertos y servicios.** Detalla cómo deben configurarse los interfaces de red de cada componente y los puertos de red necesarios para mantener una correcta comunicación entre los componentes del sistema. Además, se busca facilitar la identificación de servicios adicionales y la parametrización posterior a la instalación para garantizar un nivel de seguridad más avanzado, como, por ejemplo, cerrando puertos o eliminando servicios innecesarios.

6.5. **Configuración de Protocolos Seguros.** Presenta los protocolos seguros que utilizan los componentes de la solución, los autorizados por las buenas prácticas y guías del Centro Criptológico Nacional, así como, las configuraciones para garantizar su utilización.

6.6. **Gestión de Certificados.** Incluye indicaciones de cómo realizar las tareas más habituales en la gestión de los certificados.

6.7. **Servidores de Autenticación.** Referencia a los servicios que pueden utilizarse para la autenticación de usuarios y control de cuentas para uso administrativo.

6.8. **Sincronización Horaria.** Incluye los requisitos y recomendaciones habituales para la implementación global de sincronización de tiempos en los componentes de la solución.

6.9. **Actualizaciones.** Indica cómo y cuándo se deben realizar las diferentes actualizaciones en el *software* y *firmware*, aplicación de *Hotfix* y paquetes de políticas personalizadas suministradas por el servicio de Soporte Técnico Forcepoint.

6.10. **Auto-Chequeos. Detalla los métodos de los que dispone la solución para la comprobación del estado general de los componentes y los servicios que proporciona.**

6.11. **SNMP.** Especifica la necesidad de monitorización por SNMP y la utilización de protocolo más seguro, versión 3.

6.12. **Alta Disponibilidad.** Detalla cómo la arquitectura, diseño y despliegue de los componentes de la solución proporcionan alta disponibilidad del servicio en caso de fallo de alguno de sus componentes.

6.13. **Auditoría.** Incluye todos los aspectos asociados a los registros de eventos generados por la solución, su monitorización y auditoría. Incluye también los aspectos relativos al almacenamiento y gestión de registros.

6.14. **Backup.** Detalla la configuración de tareas programadas y manuales de copias de seguridad de los diferentes componentes.

7. **Operación.** Incluye la descripción a alto nivel de la operación de la plataforma en modo seguro.
8. ***Checklist*.** Contiene todas las recomendaciones de seguridad detalladas a lo largo del procedimiento.
9. **Referencias.** Recoge la documentación que se ha referenciado a lo largo de la elaboración de la guía.
10. **Abreviaturas**. Glosario de las abreviaturas que se pueden encontrar a lo largo del documento para mejor su entendimiento**.**
11. **Anexos**. Por su extensión en la descripción en el cuerpo del documento, se recoge información adicional organizada en anexos.

4. SERVICIOS DE SEGURIDAD

11. El entorno *Forcepoint Security On-Prem 8.5* se compone de tres (3) productos para dar cumplimiento a la protección de Email, Web y DLP. A continuación, se exponen estas soluciones y las características clave que proporcionan.

4.1.1 PROTECCIÓN DE ACCESO A INTERNET

12. El entorno aplica una política de filtrado de Internet sobre el tráfico. Dicha política permite a los administradores definir categorías de sitios web y protocolos a los que se debe impedir el acceso. Los administradores especifican las restricciones de categoría y protocolo a implementar para cada usuario o grupo de usuarios. El tráfico de usuarios se puede controlar de varias maneras:

    a) permitiendo el acceso al contenido (todo lo demás está bloqueado por defecto).

    b) bloqueando el acceso a ciertos contenidos.

    c) imponiendo cuotas y restricciones de ancho de banda.

13. Las políticas se basan en categorías de contenido web y protocolos no web. Los administradores pueden definir políticas con categorías predeterminadas o crear nuevas categorías para crear políticas más personalizadas.

14. Las categorías de protocolo predeterminadas incluyen mensajería instantánea, compartición de archivos como *Torrent* y muchos otros. Al igual que con las categorías de contenido, los administradores pueden definir categorías de protocolos para ayudar a aplicar políticas más personalizadas.

15. Las políticas detallan qué filtros se deben aplicar para la protección web. Cada filtro incluye:

    - El tipo de filtro (filtro de categoría, filtro de acceso limitado o filtro de protocolo).
    - El nombre y la descripción del filtro.
    - El contenido del filtro (categorías o protocolos con acciones aplicadas, o una lista de sitios permitidos).
    - El número de políticas que aplican el filtro seleccionado.
    - Las acciones para el filtro se especifican en su creación.

ACCIONES POR TIPO DE FILTRO	
TIPO DE FILTRO	**BOTONES DE ACCIÓN**
Category filter	Se puede utilizar el botón ***Permit***, ***Block***, ***Confirm*** o ***Quota*** para cambiar la acción aplicada a las categorías seleccionadas.

ACCIONES POR TIPO DE FILTRO	
TIPO DE FILTRO	**BOTONES DE ACCIÓN**
	Para cambiar la acción aplicada a una categoría principal y todas sus subcategorías, primero se debe cambiar la acción aplicada a la categoría principal y luego haga clic en **aplicar a subcategorías ("*Apply to Subcategories*")**. Para habilitar el bloqueo de palabras clave, el bloqueo de tipo de archivo o el bloqueo basado en el ancho de banda, haga clic en **Avanzado ("*Advanced*")**.
Limited Access filter	Se puede utilizar el botón **Agregar sitios y Agregar expresiones ("*Add Sites*" y "*Add Expressions*")** para agregar URL permitidas, direcciones IP o expresiones regulares al filtro. Para eliminar un sitio del filtro, se debe marcar la casilla de verificación junto a la URL, la dirección IP o la expresión, y luego clic en **Eliminar ("*Delete*")**.
Protocol filter	Se puede utilizar el botón **Permitir ("*Permit*")** o **Bloquear ("*Block*")** para cambiar la acción aplicada a los protocolos seleccionados. Para cambiar la acción aplicada a todos los protocolos en un grupo de protocolos, cambie la acción aplicada a cualquier protocolo en el grupo y luego clic en **Aplicar al grupo ("*Apply to Group*")**. Para registrar datos para el protocolo seleccionado o para habilitar el bloqueo en función del ancho de banda, clic en **Avanzado ("*Advanced*")**.

16. El escaneo realizado para aplicar las políticas de protección de Internet incluye el uso de Forcepoint ACE (*Advanced Classification Engine*) para identificar señuelos maliciosos, kits de explotación, amenazas emergentes, comunicaciones de *botnet* y otras actividades de amenazas avanzadas. Múltiples motores de contenido en tiempo real analizan el contenido completo de la página web, *scripts* activos, enlaces web, perfiles contextuales, archivos (incluidos los ejecutables).

4.1.2 DATA LOSS PREVENTION

17. El entorno proporciona una política de prevención de pérdida de datos para proteger de fugas de información y pérdida de datos, tanto en el perímetro como dentro de la organización. El componente *Forcepoint DLP* puede funcionar de

forma independiente o puede combinarse con *Forcepoint Web Security* o *Forcepoint Email Security* para proporcionar una solución integral de prevención de pérdida de datos. El módulo *DLP Forcepoint Web Security* evita la pérdida de datos a través de canales web como HTTP, HTTPS y FTP. El módulo Email DLP incluido en Forcepoint DLP evita la pérdida de datos a través del correo electrónico.

18. El motor de políticas de DLP es responsable de analizar los datos y usar análisis para compararlos con las reglas de las políticas configuradas. Las políticas se pueden utilizar para definir:
    - Quién puede mover y recibir datos.
    - Qué datos pueden y no pueden moverse.
    - Dónde se pueden enviar los datos.
    - Cómo se pueden enviar los datos.
    - Qué medidas tomar en caso de incumplimiento de la política.
19. Hay cuatro (4) tipos de políticas DLP:
    - **Política de correo electrónico (*Email Policy*)** - Se puede definir una sola política de correo electrónico DLP que contenga todos los atributos que se supervisarán en los mensajes entrantes y salientes. Para cada atributo (por ejemplo, la aparición de una frase clave definida), la política define si se debe permitir o poner en cuarentena el mensaje y si se debe enviar una notificación.
    - **Política web (*Web Policy*)** - Se puede habilitar una política web única de DLP que contenga todos los atributos que se deben monitorizar en los canales HTTP, HTTPS y FTP, y también permite especificar sitios web a los que no se pueden enviar datos confidenciales.
    - **Política predefinida (*Predefined Policy*)** - *Forcepoint On-Premise Security DLP* viene con un amplio conjunto de políticas predefinidas que cubren los requisitos de datos para una amplia variedad de organizaciones. Incluyen:
        - Políticas de uso aceptable, como ciberacoso, obscenidades e imágenes indecentes.
        - Políticas de protección de contenido, como difusión de contraseñas, tarjetas de crédito e información financiera.
        - Regulaciones, cumplimiento y políticas de estándares, como PCI y regulaciones federales.
        - Políticas de indicadores de robo de datos, tales como sospecha de diseminación maliciosa y empleado descontento.
    - **Política personalizada (*Custom Policy*)** - Proporciona a los administradores la capacidad de crear políticas personalizadas adaptadas a las necesidades de su organización.

20. El administrador puede gestionar la gravedad y las medidas que se deben tomar cuando coinciden las reglas de la política. Puede también definir si los incidentes deben activarse cada vez que una regla coincide o para la acumulación de coincidencias para una fuente en particular a lo largo del tiempo (*Drip* DLP), y también puede definir cómo se cuentan las coincidencias, el umbral para desencadenar el incidente, la gravedad de asignar infracciones y el plan de acción a aplicar.
21. El componente Forcepoint DLP tiene dos (2) bases de datos para incidentes y datos forenses:
    - La base de datos de incidentes contiene información sobre infracciones de políticas, como qué regla coincidió, cuántas veces, cuáles fueron los desencadenantes de infracciones, fecha, canal, origen, ID y más.
    - El repositorio forense contiene información sobre la transacción que resultó en el incidente, como el contenido de un cuerpo de correo electrónico, De:, Para :, CC: , archivos adjuntos, campos, nombre de archivo, etc.
22. En los *endpoints* Windows, el componente Forcepoint DLP también admite la integración con el sistema de etiquetado de clasificación de *Boldon James*. Esto permite aplicar etiquetas de datos personalizadas a archivos con la API apropiada instalada en los *endpoints*. Para información de referencia, consultar [REF39] *Enhancing Forcepoint DLP with Boldon James Data Classification*.

4.1.3 PROTECCIÓN EMAIL

23. El componente *Forcepoint Email Security* para DLP aplica una política de email para proporcionar protección a los sistemas de correo electrónico a fin de evitar la entrada de amenazas maliciosas en la red de una organización, así como la visibilidad y control del canal de correo electrónico como vía posible de exfiltración de información. Cada mensaje es procesado por un conjunto robusto de análisis antivirus y antispam para evitar que el correo electrónico infectado ingrese a la red. El enrutamiento de mensajes basado en el dominio y la dirección IP garantiza la entrega confiable y precisa del correo electrónico.
24. Hay tres (3) tipos de políticas disponibles, según la dirección del correo electrónico: entrante, saliente o interno. La dirección del mensaje se determina en función de los dominios protegidos de una organización:
    - Entrante: la dirección del remitente no proviene de un dominio protegido y la dirección del destinatario está en un dominio protegido.
    - Saliente: la dirección del remitente proviene de un dominio protegido y la dirección del destinatario no está en un dominio protegido.
    - Interno: tanto la dirección del remitente como la del destinatario están en un dominio protegido.
25. Las políticas también se pueden aplicar a las comunicaciones de correo electrónico salientes para proteger contra la pérdida de datos confidenciales. La

monitorización de correos electrónicos salientes incluye la monitorización de DLP por goteo, o Dr*ip DLP* para identificar dónde se filtran datos confidenciales en pequeñas cantidades con el tiempo.

26. Los mensajes de correo electrónico se pueden administrar en base a:

- **Propiedades del mensaje:** incluido el volumen, configuraciones de destinatario no válidas, opciones de mensajes de archivo, verificación del remitente del mensaje y la habilitación de la verificación de etiqueta de dirección de rebote (BATV).
- **Opciones de Conexión**: usar listas negras en tiempo real, verificación inversa de DNS, servicio de reputación, retrasar el saludo SMTP, habilitar el comando SMTP VRFY y cambiar el puerto SMTP).
- **Detección de IP de origen verdadera:** usar la información del encabezado del mensaje y el número de saltos de red a un dispositivo de correo electrónico para determinar la dirección IP del primer remitente fuera del perímetro de la red).
- **Conexiones TLS:** forzar conexiones hacia o desde una IP específica o grupo de dominio. Utiliza la seguridad de la capa de transporte (TLS) obligatoria y determina el nivel de seguridad utilizado por esa conexión.
- **Ataques de recolección de directorio*s (Directory harvest attacks*):** limitar el número máximo de mensajes y conexiones que provienen de una dirección IP durante un período de tiempo determinado.
- **Opciones de control de *relay*:** limitar los dominios y los grupos de direcciones IP para los que el servidor puede enviar correo.
- **Rutas de entrega (*Delivery Routes):*** cambiar el orden de una ruta de directorio de usuario o basada en dominio.
- **Reescritura de direcciones email y de dominio:** especificar la dirección del destinatario para reescribir las entradas de los mensajes para enmascarar los detalles de la dirección y redirigir la entrega de mensajes.
- ***Sandbox* de URL:** análisis en tiempo real de las URL que están incrustadas en el correo electrónico entrante.

5. FASE DE DESPLIEGUE E INSTALACIÓN

5.1 ENTREGA SEGURA DEL PRODUCTO

27. El despliegue de la herramienta consta de componentes *hardware* y *software*. Los componentes *Forcepoint Email Security* y *Web Security* están preinstalados en el dispositivo *Forcepoint V10000 G4* antes de que sea enviado al cliente.

28. El paquete que envía el fabricante contiene un *appliance*, con una imagen de *software* preinstalada, y con accesorios para su instalación física. El cliente puede acceder al *software* y a la documentación del producto iniciando sesión con su cuenta de usuario como cliente en: *https://support.forcepoint.com/MyAccount*.

29. Una vez iniciada sesión, se puede acceder a los apartados correspondientes: "*Downloads*" para acceso al *software*; y "*Documentation*" para la documentación técnica de instalación, despliegue, administración e información adicional de interés, para cada una de las soluciones de Forcepoint.

30. Forcepoint utiliza una empresa de terceros para realizar diversas actividades relacionadas con la entrega del producto al cliente, incluidas la gestión de existencias, la fabricación, las pruebas, el aseguramiento de la calidad, la integración, la logística y la entrega. Esta empresa se conoce como "empresa subcontratista".

31. Cuando el cliente compra el dispositivo de seguridad V10000 G4 v8.5, todo el *software* se preinstala durante la fabricación. La caja y todo el embalaje del producto lo realiza la empresa subcontratista en sus instalaciones de fábrica. La caja está etiquetada con un número de pieza y un número de serie que se pueden verificar con la lista de materiales (BOM).

32. En las fábricas, un grupo de empleados realiza inspecciones de control de calidad de cada unidad antes de colocarlas en el inventario. Además, el equipo de fabricación de Forcepoint realiza inspecciones a intervalos irregulares y, a nivel ejecutivo, trimestralmente para revisar el proceso de fabricación y el entorno. Las inspecciones aseguran que todas las cuestiones y problemas con los procesos de embalaje y envío son identificados y corregidos.

33. Forcepoint gestiona el envío del producto junto con las empresas contratistas en función de los plazos y la disponibilidad del transportista. Los transportistas comúnmente utilizados para realizar los envíos de productos a los clientes son *Federal Express (FedEx)* y *Crane Logistics (Crane)*. Forcepoint utiliza el sistema de seguimiento en línea de estos transportistas y proporciona la información al cliente comprador por correo electrónico. Cualquier envío que encuentre paradas se investigará de inmediato.

34. Forcepoint a menudo involucra a distribuidores y revendedores en compras. Esas organizaciones contactarán al cliente directamente con la información de entrega.

35. **Los clientes deben verificar que han recibido el producto *hardware* correcto.** Para ello, deben verificar el número de envío de la caja para asegurarse de que coincide con el número proporcionado por Forcepoint.

36. El cliente también debe **verificar la integridad del *software* descargado** a través del *hash* SHA256 de los archivos descargados. Este hash debe ser comparado con los valores de *hash* publicados en la página de descarga del archivo.

37. También se puede verificar la versión del *software* del servidor haciendo clic en la opción "*Acerca*", en el menú "*Ayuda*" del *Forcepoint Security Manager*.

5.2 ENTORNO DE INSTALACIÓN SEGURO

38. Por lo tanto, se recomienda instalar el producto en un Centro de Proceso de Datos (CPD) que deberá contar con un sistema de control de acceso limitado y restringido al conjunto de personas expresamente autorizadas.

5.3 REGISTRO Y LICENCIAS

39. Para la activación de las licencias, previamente suministradas desde Forcepoint, es necesario seguir el procedimiento de activación de las licencias en la consola de gestión *Forcepoint Security Manager*. Para realizar este registro será necesario seguir los pasos que se recogen en la ayuda de la versión *Forcepoint On-Prem 8.5* en el enlace: *[REF34] Entering a Subscription Key.*

5.4 CONSIDERACIONES PREVIAS

40. Antes de instalar cualquier componente de *Forcepoint On-Premise Security 8.5*, se deben haber completado todos los preparativos que se detallan a continuación:

5.4.1 CONSIDERACIONES ESPECÍFICAS PARA WINDOWS

41. Se debe haber aplicado todas las actualizaciones del sistema operativo subyacente Microsoft. No debe haber actualizaciones pendientes, especialmente las que requieren un reinicio del sistema operativo.

42. Dada la protección ofrecida por el sistema operativo Windows Server 2016 y posteriores, todos los procesos en ejecución poseen acceso exclusivo a la zona de memoria asignada. Por este motivo, se recomienda la instalación de Forcepoint Security Manager sobre Windows Server 2016 o versiones posteriores.

43. Además del espacio requerido por el propio instalador, se requieren aproximadamente 2 GB de espacio en disco en la unidad de instalación de Windows (generalmente C) para almacenar archivos temporales extraídos como parte del proceso de instalación. Para más información sobre requerimientos de espacio en disco, en el siguiente enlace se detallan los requerimientos *hardware:* [REF1] Forcepoint System requirements for this version.

44. El instalador requiere .NET Framework v3.5 y 4.5. Para Windows Server, en todos los casos aplicable a versiones Standard o Enterprise, 2012R2, 2016 y 2019, la v3.5 está desactivada de forma predeterminada mientras que la v4.5 está activada por defecto. **Ambas deben ser seleccionadas y activadas.**

5.4.2 OBTENER LOS INSTALADORES DEL SOFTWARE

45. El instalador de Forcepoint Security se utiliza para instalar o actualizar el servidor de administración de Forcepoint. Permite actualizar la configuración existente, instalar funcionalidades o servidores adicionales completos como servidores de logs, servidores de análisis de imágenes (OCR), servidores de gestión de políticas o de endpoints, para alta disponibilidad y redundancia.

46. El instalador también se utiliza para realizar instalaciones de soluciones de Forcepoint como *Web Security* o *Email Security* sobre plataformas existentes con Forcepoint DLP instalado y operativo, para disponer de una plataforma de gestión centralizada y unificada de las soluciones *Forcepoint OnPrem Security*.

47. Hasta la versión 8.5 se incluía con el instalador de Forcepoint una versión de *Microsoft SQL Express 2017*. Las nuevas versiones no la incorporan y se recomienda la instalación desde una fuente oficial de Microsoft.

48. Existen paquetes de instaladores específicos para instalar componentes de protección web en servidores Linux compatibles.

49. Los instaladores de Windows y Linux se descargan desde la sección "*My account*" en forcepoint.com. Se debe buscar la versión que se va a instalar (v8.5.x o consultar recomendación al fabricante) y se hacer doble clic para iniciar el proceso de instalación.

50. El ejecutable del instalador de *Forcepoint Web Security* para plataformas Windows, para versiones 8.x, está nombrado como ***Forcepoint8xxSetup.exe***. El instalador para plataformas Linux, para versiones 8.x, estará nombrado como ***Web85xSetup_Lnx.tar.gz***.

51. En plataformas *Windows Server*, cuando ya se ha ejecutado el instalador para algún otro producto *Forcepoint OnPrem Security* (como Web o Email) y al finalizar se ha seleccionado la opción conservar archivos de instalación ("*Keep installation files*"), se puede reiniciar el instalador sin extraer todos los archivos por segunda vez.

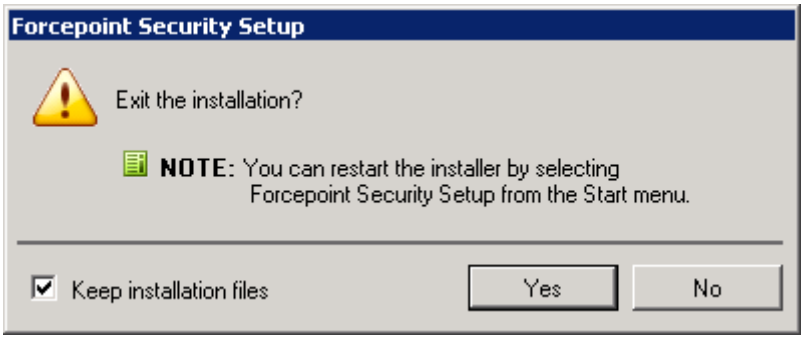

Figura 2 - *Pop-up* de aviso de cierre de instalador

52. Para iniciar el instalador por segunda vez y siguientes, si se ha hecho el punto anterior, no es necesario descomprimir y ejecutar de nuevo el archivo descargado de la web de soporte de Forcepoint. En plataformas Windows se puede encontrar

como aplicación ya instalada en el menú de inicio un icono de Forcepoint, llamado ***Forcepoint Security Setup***.

53. A modo informativo, los instaladores de *Forcepoint Management Server* pueden tener un tamaño entre 3 y 5 GB.

5.4.3 PRIVILEGIOS PARA LA INSTALACIÓN

54. Los componentes de Forcepoint generalmente se distribuyen en varias máquinas. Además, algunos componentes acceden a servicios de directorio de red o servidores de bases de datos. Para realizar la instalación, se recomienda iniciar sesión en la máquina como usuario con privilegios de administrador local. De lo contrario, es posible que los componentes no puedan acceder adecuadamente a los componentes o servicios remotos.

    Importante: Si se planea instalar *SQL Server Express* para almacenar y mantener datos para su solución de protección web, se debe iniciar sesión como usuario de dominio para ejecutar el instalador de *Forcepoint Security*. Esto garantiza que *Service Broker*, instalado como parte de SQL Server, pueda autenticarse contra un dominio (requerido).

55. En entornos superiores a 350 usuarios o en casos de entornos de producción con alta carga no se recomienda la utilización de la versión Express de SQL, siendo SQL Server la distribución recomendada.

5.4.4 SINCRONIZACIÓN DE TIEMPOS

56. Se deben sincronizar todas las máquinas donde está instalado un componente Forcepoint. Para ello, **se considera una buena práctica la utilización de un servidor de *Network Time Protocol* (NTP).**

    Importante: Si se instalan componentes sobre un *appliance* Forcepoint, se debe sincronizar la hora de la máquina con la hora del *appliance*.

5.4.5 ANTIVIRUS

57. Se debe deshabilitar cualquier antivirus en la máquina antes de instalar los componentes de Forcepoint. Cuando la instalación se ha realizado, se debe volver a habilitar. Algunos archivos deben excluirse de los análisis antivirus para evitar problemas de rendimiento; ver *[REF35] Excluding Forcepoint files from antivirus scans.*

5.4.6 SIN GUIONES BAJOS EN FQDN

58. No se deben instalar componentes Forcepoint en una máquina cuyo nombre de dominio completo (FQDN) contenga un guion bajo. El uso de este carácter en un FQDN es incompatible con los estándares del Grupo de Trabajo de Ingeniería de Internet (IETF). Se pueden encontrar más detalles de esta limitación en las especificaciones IETF RFC-952 y RFC-1123.

5.4.7 DESHABILITAR UAC Y DEP

59. Antes de comenzar el proceso de instalación, se debe desactivar la configuración de Control de Cuentas de Usuario (UAC), de Prevención de Ejecución de Datos (DEP), y cualquier política de restricción de *software* que pueda bloquear la instalación. La configuración de UAC se puede volver a habilitar después de la instalación. DEP debe estar seleccionado para sólo permitir servicios y programas Windows esenciales.

5.4.8 *FORCEPOINT SECURITY MANAGER*

60. Además de las recomendaciones de preparación general descritas en esta sección, se añaden las siguientes recomendaciones adicionales asociadas al FSM:

    - No se debe instalar en una máquina controladora de dominio.
    - Si se desea utilizar una versión Microsoft SQL Server en el servidor de administración Forcepoint, se puede utilizar SQL Server Express, cumpliendo los requerimientos de dimensionamiento de Forcepoint.
    - Si se utiliza una instancia SQL Server, puede usarse cualquiera de las versiones compatibles.
    - No está recomendada la instalación de FSM en el mismo servidor donde se encuentre instalado Microsoft SQL Server.

5.4.9 *SQL SERVER EXPRESS*

61. La instalación de *Microsoft SQL Server Express* requiere de componentes de terceros. Aunque algunas versiones del instalador de Forcepoint Security instalarán estos componentes automáticamente, es una buena práctica instalar los componentes primero, antes de ejecutar el instalador de Forcepoint Security.

62. Los componentes son los siguientes:

    - *.NET Framework 4.6*
    - La versión 8.5.x requiere .NET 4.5. En versiones superiores, según la documentación de requisitos de instalación, puede ser requerido .NET 4.6 o superior, sustituyendo ésta a la versión 4.5.
    - *Windows Installer 4.5*
    - *Windows PowerShell 1.0.*

5.4.10 COMPONENTES DE PROTECCIÓN WEB

63. Los componentes *Forcepoint Web Security* y *Forcepoint URL Filtering* requieren de una descarga completa inicial de la base de datos maestra o principal de categorías de sitios web (llamada *Master Database*), con la que se filtrará posteriormente a qué categorías de sitios web se permitirá navegar a los usuarios en la política de navegación. Esta base de datos será actualizada dinámicamente

desde Forcepoint por internet, una vez la solución esté configurada correctamente y ejecutándose.

64. Los sitios web solicitados por los usuarios durante la navegación, serán clasificados por esta base de datos Máster y, en tiempo real, por el motor de clasificación y análisis avanzado en nube de Forcepoint, llamado Forcepoint ACE (*Advanced Classification Engine*). Este motor es el encargado de analizar aspectos como la actualización de la categoría del sitio web, el análisis de la reputación del sitio como originador de ataques informáticos, el origen de contenido con códigos maliciosos, *malware* o envío de *spam*.

65. Para que el servicio de filtrado de navegación funcione correctamente, es requerido que, cada servidor *proxy* que ejecute el servicio *Filtering Service (*el servicio encargado de aplicar filtrado de la navegación en las soluciones *Forcepoint Web Security*) debe poder acceder al sitio web de descarga de Forcepoint en *download.forcepoint.com*. Esta dirección URL debe estar permitida en todos los *firewalls*, otros servidores *proxy*, enrutadores o archivos *host* existentes en la red, que puedan interferir en el acceso al sitio web de Forcepoint.

5.4.11 CORTAFUEGOS

66. Se debe deshabilitar cualquier *firewall* en la máquina antes de la instalación. Una vez la instalación se haya completado, se debe volver a habilitar.

67. El instalador de Forcepoint Security agrega dos (2) reglas de entrada al perfil público del *firewall* de *Windows*. Los puertos 9443 y 19448 se abren para la infraestructura de administración de Forcepoint por lo que estos puertos deben estar abiertos para permitir que los navegadores se conecten al FSM. Además, se pueden agregar reglas adicionales al Firewall de Windows al instalar los componentes *de Forcepoint On-Premise Security*. Por ejemplo, si en la arquitectura se incluyen servicios como *Forcepoint Protector*, para el análisis de tráfico web con soluciones de terceros. Este servicio utiliza el protocolo ICAP, por lo que además de los puertos anteriores, deberán añadirse los puertos estándar del protocolo (1344) o los que se utilicen de forma personalizada.

68. Para información detallada sobre los puertos necesarios para el correcto funcionamiento del entorno en función de los diferentes componentes desplegados, puede consultarse en la web de *Forcepoint* en *[REF36] Default ports for on-premises Forcepoint security solutions*.

5.4.12 SERVICIO *COMPUTER BROWSER*

69. Para disponer de la identificación de usuarios mediante consultas al controlador de dominio sobre usuarios o grupos de usuarios, es necesario disponer de servicios de la solución Forcepoint como *User Service, DC Agent o Logon Agent.* La selección de uno, otro o varios servicios de identificación de usuarios será determinado por las necesidades y características de cada entorno, cliente u organización. Al menos uno de estos servicios es requerido para la identificación del usuario. Para instalaciones sobre un servidor Windows, **el servicio *Computer***

Browser (Examinador de Equipos) **nativo de Windows debe estar ejecutándose**. En la mayoría de las máquinas, el servicio está deshabilitado de manera predeterminada.

70. Si se detiene el servicio, el instalador intentará habilitarlo e iniciarlo. Si esto falla, el componente se instala y se inicia, pero los usuarios no se identifican hasta que habilita e inicia el servicio *Computer Browser*.

5.4.13 *NETWORK AGENT*

71. El componente agente de red (*Network Agent*) es el encargado de habilitar el filtrado sobre protocolos no-HTTP a nivel de red. El Agente de red funciona supervisando el uso general de la red, incluidos los *bytes* transferidos. Registra resúmenes de uso, que incluyen la hora de inicio y la hora de finalización, los bytes generales utilizados y los bytes utilizados por protocolo, a intervalos predefinidos.

72. Cuando se usa, el agente de red generalmente se configura para ver todo el tráfico y puede distinguir entre solicitudes enviadas desde máquinas internas a máquinas internas (visitas a un servidor de intranet, por ejemplo) y solicitudes enviadas desde máquinas internas a máquinas externas como servidores web (solicitudes de internet de los usuarios, por ejemplo).

73. En las implementaciones de *Forcepoint Web Security* en las que el control de tráfico HTTP/HTTPS es realizado por los *appliances Content Gateway*, el agente de red es un componente opcional que se puede usar para:

    a) Administrar solicitudes que no son HTTP.

    b) Proporcionar mejoras en el registro de logs.

    c) Gestionar el acceso a Internet según el ancho de banda.

74. Si se está instalando el agente, es necesario asegurarse de que la máquina del agente esté en disposición de monitorizar y responder a las solicitudes de internet del cliente.

75. En instalaciones independientes (que no incluyen *Content Gateway* o un producto de integración de terceros), si se instala el agente de red en una máquina que no puede monitorizar las solicitudes de los clientes, la aplicación de políticas básicas y las funciones como la administración de protocolos y *Bandwidth Optimizer* no podrán funcionar correctamente.

    Importante: No se debe instalar el agente de red en una máquina que ejecute un *firewall* ya que el agente utiliza la captura de paquetes que puede entrar en conflicto con el *software* del *firewall*.

76. La tarjeta de interfaz de red (NIC) que designe para su uso por parte del agente de red durante la instalación debe admitir el modo promiscuo. El modo promiscuo permite que una NIC escuche direcciones IP que no sean las suyas. Si la NIC admite el modo promiscuo, se establece en ese modo durante la instalación. Se

debe consultar al administrador de red o al fabricante de la NIC para ver si la tarjeta admite el modo promiscuo.

77. En Linux, **no** se debe elegir una NIC sin una dirección IP (modo *Stealth*) para las comunicaciones del agente de red. Si se instala el agente en una máquina con múltiples NIC, después de la instalación, se puede configurar el agente para usar más de una NIC. Consulte [REF36] *Network Agent Quick Start* para obtener más información.

78. Si el agente está instalado en una máquina Linux, usando una tarjeta de red (NIC) para bloquear y otra NIC para monitorizar, se debe garantizar que:

    - La NIC de bloqueo y la NIC de monitorización tienen direcciones IP en diferentes segmentos de red (subredes). Si están asignadas a la misma subred, el sistema operativo Linux puede intentar enviar el bloqueo a través de la NIC de monitorización. Si esto sucede, la página solicitada o el protocolo utilizado no se bloquea y el usuario puede acceder al sitio web.
    - Se elimina la entrada de la tabla de enrutamiento para la NIC de monitorización.

5.4.14 INSTALACIÓN EN LINUX

79. La mayoría de los componentes de protección web se pueden instalar en Linux.

80. Antes de realizar la instalación:

    a) Si SELinux (*Security-Enhanced Linux*) está habilitado, se debe deshabilitar o configurar en modo permisivo.

    b) Si el *software* de protección web se está instalando en una máquina Linux en la que está activo un *firewall*, se debe deshabilitar el *firewall* antes de ejecutar la instalación. Después de la instalación, se debe reiniciar el *firewall* y asegurarse de que los puertos utilizados por los componentes instalados en esta máquina están abiertos.

    Importante: No instalar el agente de red en una máquina que ejecute un *firewall* ya que la captura de paquetes puede entrar en conflicto con el *software* del *firewall*.

81. Si, durante la instalación, se recibe un error con respecto al archivo */etc/hosts*, se debe, para conseguir corregir el problema, tener en cuenta lo siguiente:

    a) El archivo de hosts (por defecto, en */etc*) debe contener una entrada de nombre de host para la máquina, además de la dirección de *loopback*.

    Nota: se puede verificar si se ha especificado un nombre de *host* en el archivo de *hosts* utilizando el comando *hostname -f*.

    Para configurar el *hostname: hostname <host>,* donde *<host>* es el nombre que se asigna a esta máquina.

    b) También hay que actualizar la entrada *HOSTNAME* en el archivo */etc/sysconfig/network: HOSTNAME=<host>*

c) En el archivo */etc/hosts*, se debe especificar la dirección IP para asociar con el nombre de *host*. Esto debería ser estático y no ser atendido por DHCP. No se debe eliminar la segunda línea del archivo, la que comienza con 127.0.0.1 (la dirección de *loopback* IPv4), ni la tercera línea del archivo, la que comienza con *::1* (la dirección de *loopback* IPv6). Además, no se debe agregar el nombre de host a la segunda o tercera línea.

<IP address> <FQDN> <host>

127.0.0.1 localhost.localdomain localhost

::1 localhost6.localdomain6 localhost6

Aquí, <FQDN> es el nombre de dominio completo de esta máquina (es decir, *<host>. <subdomains>. <Dominio de nivel superior>*), por ejemplo, *myhost.example.com*, donde *<host>* es el nombre asignado a la máquina.

Importante: La entrada de nombre de *host* que se cree en el archivo de *hosts* debe ser la primera entrada en el archivo.

5.4.15 FORCEPOINT DLP

82. Los servidores que ejecutan Forcepoint DLP se pueden configurar como parte de un dominio o como un grupo de trabajo separado. Si hay desplegados varios servidores o se desea ejecutar comandos de ejecución en servidores de archivos en respuesta a tareas de descubrimiento de información sensible en repositorios compartidos (por ejemplo, eliminar o cifrar un fichero que contenga información sensible descubierto en una carpeta compartida de un servidor del dominio), se recomienda que el servidor o los servidores formen parte de un dominio.

83. Sin embargo, las GPO estrictas pueden interferir y afectar el rendimiento del sistema e incluso hacer que el sistema se detenga. Por lo tanto, al desplegar servidores Forcepoint DLP en un dominio, se recomienda que formen parte de las unidades organizativas que no imponen GPO estrictas. **Es por ello, que no se debe instalar el servidor Forcepoint DLP en una máquina controladora de dominio (DC).**

84. Ciertos escaneos de antivirus en tiempo real pueden degradar la eficiencia del sistema. Este aspecto puede mitigarse al excluir algunos directorios de los escaneos. Para más información, se recomienda consultar la guía de referencia [REF35] Forcepoint de escaneos antivirus.

5.5 INSTALACIÓN

85. Tras tener en cuenta los requerimientos y consideraciones previas, se debe proceder a la instalación de los diferentes componentes, según las necesidades concretas de cada entorno cliente.

86. La consola FSM es el componente de gestión del sistema *Forcepoint Security On-Prem* para los componentes *Web*, *Email* y *Data Security*, por lo que debe ser instalado en primer lugar, antes de desplegar ningún otro componente Forcepoint. FSM debe residir en un servidor Windows. Sus requerimientos de

sistema se encuentran descrito en la guía [REF 1] *Forcepoint System requirements for this versión.*

87. La configuración segura o *hardening* de la base de datos SQL Server debe realizarse antes de la instalación de cualquier componente Forcepoint.

88. La guía de referencia [REF4] *Guía completa de instalación Forcepoint On-Prem 8.5* proporciona información completa de instalación y configuración de las soluciones *Forcepoint On-Prem Security* objeto de este Procedimiento de Empleo Seguro.

89. Tras la instalación de los componentes y comprobaciones de su correcto funcionamiento y comunicación entre los mismos, se procederá a la securización adicional FIPS. Los *appliances* Forcepoint son entregados con una imagen de *firmware* preinstalada. Para poder proceder con la securización FIPS del mismo, se debe haber terminado la instalación inicial.

5.5.1 INSTALACIÓN *FORCEPOINT WEB SECURITY*

90. La instalación de FSM descrita anteriormente debe hacerse de forma previa al despliegue de la solución, integrando en este servidor los servicios de *Policy Broker* y *Policy Database*.

91. Posteriormente se despliegan los *appliances* realizándose la configuración inicial de red que permite la comunicación con el servidor FSM. Los *appliances* no requieren instalación adicional de ningún componente, y en su instalación se integran con el servidor FSM para su gestión, tal y como se explica más adelante en los apartados de operación y administración.

5.5.2 INSTALACIÓN FORCEPOINT DLP

92. Con la primera ejecución del *software Forcepoint DLP*, se instalarán por defecto otros componentes requeridos como *Endpoint Server*, Policy *Server*, *Fingerprint Repository*, *Crawler* y *Management Server*. La finalidad de estos componentes es la siguiente:

    a) *Endpoint Server*. Responsable de la comunicación y sincronización de configuración, políticas y logs con los diferentes agentes instalados en los *endpoints* de clientes.

    b) *Policy Server*. Responsable del análisis de los datos y la aplicación de políticas.

    c) *Fingerprint Repository*. Almacena la base de datos de huellas digitales que se crean cuando se utilizan clasificadores de información basados en huellas digitales o *fingerprints* sobre archivos y bases de datos.

    d) *Crawler*. Motor que realiza las tareas de búsqueda para la detección en información sensible existente en reposo.

    e) Management Server. Servicio que gestiona, coordina todos los servicios de gestión de los componentes de la solución y proporciona el interfaz de administración y gestión centralizada para interactuar con la solución.

93. Según las necesidades particulares de cada cliente y escenario, puede ser necesaria la instalación del agente *endpoint* Forcepoint. Este agente será el último componente a desplegar. El paquete de instalación del agente se genera en la consola de gestión FSM donde reside el *Endpoint Manager*.

6. FASE DE CONFIGURACIÓN

6.1 PERSONALIZACIÓN DEL *GUI* DE GESTIÓN FSM

94. Siguiendo las recomendaciones y estándares de seguridad, se puede personalizar la página de inicio de sesión en la consola FSM. Actualmente, se pueden modificar dos (2) aspectos de esta página de inicio: el logo corporativo y el contenido de la página de *login*.

95. Para modificar el logo que se muestra en la página de inicio de sesión, se puede reemplazar el archivo de imagen por defecto, que se encuentra alojado en el servidor en el que se despliega la consola de gestión FSM. Si se ha realizado la instalación de la consola utilizando la ruta por defecto sugerida durante el proceso de instalación, este archivo se puede encontrar en la siguiente ruta:

    *C:\Program Files (x86)\Websense\EIP Infra\tomcat\webapps\manager\login\images\login**emblem.png***

96. Para modificar el texto que se muestra en la página de inicio de sesión, se debe modificar el archivo .jsp que se encuentra también alojado en el servidor. Si se ha realizado la instalación de la consola de gestión FSM utilizando la ruta por defecto sugerida durante el proceso de instalación, este archivo se puede encontrar en la siguiente ruta:

    *C:\Program Files (x86)\Websense\EIP Infra\tomcat\webapps\manager\login\pages**loginPage.jsp***

97. Forcepoint tiene previsto que, en siguientes versiones de producto, se incorpore nuevas funcionalidades en este aspecto que permitan una configuración más flexible e intuitiva, incluyendo *banner* informativo al usuario posterior al inicio de sesión en la consola FSM. Se recomienda consultar las guías de instalación y administración disponibles en la página de soporte de Forcepoint, para conocer la versión correspondiente en el momento de la instalación de la solución.

98. Una sesión de consola FSM, por defecto, finaliza 22 minutos después de la última acción realizada en la interfaz de usuario (haciendo clic de página en página, introducir información, guardar en caché los cambios o salvar los cambios). Se muestra un mensaje de advertencia 5 minutos antes del cierre de la sesión.

99. A fecha de elaboración de este documento, no es posible modificar el tiempo de inactividad por defecto. Forcepoint tiene previsto incluir esta característica en próximas versiones de producto.

6.2 MODO DE OPERACIÓN SEGURO

100. **Se debe configurar el producto para que opere en un modo de operación seguro**. Para ello, los pasos generales que se deben seguir son los siguientes:

    a) **Habilitar el modo FIPS**, siguiendo las recomendaciones de operación recogidas en el *"Anexo IV.- Refuerzo de la seguridad en la operación"* y la guía de referencia *[REF33] Applying FIPS 140-2 Validated Cryptography in Forcepoint DLP v8.5.2.* Toda la funcionalidad criptográfica es realizada por uno de los módulos criptográficos con certificación FIPS. El Módulo criptográfico

Forcepoint C (Certificado *CMVP # 2875*) se utiliza para proteger las comunicaciones entre componentes, mientras que el Módulo criptográfico *Forcepoint Java (CMVP Certificate#3113)* se utiliza para proteger comunicaciones entre servidores y estaciones de trabajo de administración remota. Habilitar el modo FIPS en los componentes no es un proceso con vuelta atrás, por lo que, si los *test* de los componentes muestran errores y se desea deshabilitar el modo FIPS, será necesario, resetear el *appliance* a los valores de fábrica y, en caso de las plataformas servidor, su reinstalación desde cero.

b) Establecer las políticas y buenas prácticas de acceso seguro a la consola de gestión FSM. Se debe limitar el acceso a la consola para que solo pueda ser accedida mediante un navegador web. El **Anexo I "Configuración de Administración Segura" describe en detalle las configuraciones recomendadas y la forma de realizar dichas configuraciones sobre la plataforma Forcepoint On-Premise Security v8.5.x.**

c) Habilitar el navegador de la estación de trabajo autorizada para conectar a la interfaz de gestión para que negocie la utilización del modo *FIPS 140-2* y no se acepte negociar un algoritmo no autorizado por el Centro Criptológico Nacional, según la guía CCN-STIC-807.

d) Revisar los registros de auditoría generados.

6.3 AUTENTICACIÓN

101. Los *appliances Forcepoint Security On-Prem* requieren que los administradores se identifiquen y se autentiquen con el entorno antes de obtener acceso a cualquiera de las funciones de administración disponibles a través de la interfaz web o la CLI. La CLI de instalación solo está disponible cuando se configura el dispositivo antes de la puesta en marcha, a través del puerto serie o los puertos de monitor y teclado en el dispositivo y no requiere que los administradores sean identificados y autenticados al acceder a él. Esto se debe a que se supone que a un administrador ya se le ha otorgado acceso físico al dispositivo. La identificación y autenticación se aplica en la CLI una vez que se ha completado la instalación.

102. Los administradores se conectan a FSM y se les solicita que ingresen sus credenciales de autenticación antes de permitir el acceso a FSM. La autenticación exitosa proporciona un inicio de sesión único a todas las consolas de seguridad locales. El entorno mantiene una lista de nombres de usuario de administrador, membresía de grupo y contraseñas para cada cuenta administrativa, autenticando así el acceso a la consola de seguridad local para el administrador. La administración de la FSM a través de la GUI se realiza mediante la API del controlador de dispositivo.

103. **Se recomienda que los usuarios administrativos se autentiquen mediante un certificado X.509** para acceder a la administración de la FSM. Se pueden admitir varios certificados para cada usuario, así como múltiples Autoridades de Certificación (CA) para firmar certificados. El *Anexo I "Configuración de*

Administración Segura" describe en detalle los pasos de configuración de autenticación basada en certificado.

104. Los métodos de acceso y autenticación a la gestión de los *Content Gateways*, pueden consultarse en las guías de referencia Forcepoint para tal efecto, como [REF14] *Accessing the Content Gateway Manager*. En esta documentación, se puede ver cómo se configura la autenticación en base a SSO con la consola FSM, autenticación de doble factor con certificados, limitación de las direcciones IP origen permitidas para iniciar una sesión de gestión, etc. El *Anexo I "Configuración de Administración Segura"* describe en detalle los pasos de configuración requeridos en los *appliances Content* Gateway para limitar el acceso de administración a usuarios previamente autenticados en el servidor FSM con autenticación basada en certificado, deshabilitando el acceso basado en usuario y contraseña.

105. El acceso de administración a los appliances *Content Gateway* mediante protocolo **SSH se recomienda que sea deshabilitado**, evitando así un acceso de gestión basado en usuario y contraseña. En caso de ser necesario puede habilitarse mediante el acceso integrado con el servidor FSM. El Anexo I "Configuración de Administración Segura" describe en detalle los pasos para deshabilitar y habilitar este acceso de gestión vía SSH.

106. Para la autenticación de los usuarios a los que puedan dar servicio las soluciones *Forcepoint Security On-Prem*, se dispone de varios métodos para adaptarse a las necesidades de cada cliente y escenario. Para obtener información más detallada de cada uno de los métodos de autenticación soportados y su parametrización, se debe acceder a la guía de referencia [REF15] *Content Gateway user authentication*. En esta referencia, se encuentran detallados los siguientes métodos de autenticación de usuarios y su configuración:

    - *Integrated Windows Authentication*
    - *Legacy NTLM authentication*
    - *LDAP authentication*
    - *RADIUS authentication*
    - *Rule-Based Authentication*
    - *Mac and iPhone/iPad authentication*

107. Dicha referencia también incluye información sobre las opciones y parametrización global de autenticación o limitaciones de algunos navegadores.

6.4 ADMINISTRACIÓN DEL PRODUCTO

6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

108. Forcepoint exige la identificación y autenticación de los administradores antes de que puedan acceder a cualquier funcionalidad de administración a través de la CLI o GUI, según el tipo de componente a administrar.

109. El acceso por CLI a los componentes *gateways* podrá realizarse a través de un terminal directo, cable serie o por SSH. La referencia de cómo configurar este tipo de acceso se puede ver en la guía *[REF7] Accessing the CLI*. Según cada cliente y arquitectura de la red de gestión, se puede utilizar indistintamente uno u otro método. No obstante, lo más habitual en los clientes y por integración con herramientas de gestión de accesos, suele ser más utilizado el método por SSH. Como se ha indicado anteriormente, una vez concluida la instalación inicial se recomienda deshabilitar este acceso de administración forzando que toda la administración de los *appliances* se realice a través del acceso integrado con FSM.

110. Adicionalmente, se pueden establecer restricciones de acceso a usuarios concretos, por dirección IP de origen, etc., según se indica en la guía de referencia *[REF6] Content Gateway Security*.

111. La plataforma para la administración y gestión global de seguridad es FSM a la que se puede acceder local o remotamente utilizando TLS 1.2, mediante navegador accediendo a la URL de la IP del servidor de gestión y al puerto TCP 9443 (Por ejemplo: *https://192.168.0.1:9443)*. **Se debe configurar la plataforma para permitir únicamente el uso de TLS 1.2**, tal y como se describe más adelante.

112. Forcepoint también evita que los administradores accedan al contenido FSM antes de autenticarse. Se mantiene, para ello, una lista de atributos de seguridad (como credenciales de inicio de sesión).

113. Los usuarios de correo electrónico deben identificarse y autenticarse antes de que el entorno Forcepoint permita el acceso a su correo electrónico personal por el interfaz de usuario para gestionar mensajes de correo electrónico en cuarentena.

114. El entorno puede asignar un límite en el número de sesiones concurrentes que los usuarios administrativos pueden tener con FSM. Si se alcanza este límite, la plataforma evita que se creen nuevas sesiones. Para usuarios de administración con rol de *Super Administrador*, se limita a una única sesión.

6.4.2 CONFIGURACIÓN TLS V1.2 FORCEPOINT SECURITY ON-PREM

115. De cara a reforzar la seguridad en todas las comunicaciones, se recomienda configurar los distintos elementos de la solución para que únicamente soporte cifrado basado en TLS v1.2 y con los métodos de cifrados aprobados.

116. **Se deben seguir los pasos de configuración definidos en el *Anexo II "Empleo de mecanismos de cifrado robusto"* para forzar el uso de TLS v.1.2** y no usar versiones anteriores e inseguras del protocolo.

6.4.3 CONFIGURACIÓN DE ROLES DE ADMINISTRACIÓN

117. Se dispone de interfaces de administración robustas que los administradores autorizados pueden usar para administrar el entorno y configurar políticas para controlar el acceso al contenido. Por defecto, el filtrado de *proxy* está habilitado, pero todo el tráfico está permitido; por lo tanto, el entorno Forcepoint tiene una postura permisiva por defecto.

118. El entorno de Forcepoint define dos (2) roles de administrador:

    a) Administrador de seguridad: Puede tener acceso a uno o varios módulos de las soluciones *Forcepoint OnPrem* con nivel de super administrador. Adicionalmente, se le puede conceder la capacidad de crear otras cuentas con rol de administrador delegado.

    b) Administrador delegado. Son las cuentas de usuario creadas con rol de administrador por el administrador de seguridad, pero con permisos y roles específicos por cada módulo.

119. Los roles de administrador administran las operaciones de todo el sistema, como la configuración de dominios, la edición de perfiles de usuario, permisos, configuración de rutas y preferencias en todos los componentes web, de correo electrónico y de datos. La lista completa de roles y descripción de estos se puede ver en la presente documentación en [REF37] Roles de Administración.

120. Desde la consola FSM se pueden asignar usuarios a los roles configurados, así como la creación de roles personalizados granulares según las necesidades concretas del cliente y entorno.

121. Durante la instalación, se crea un rol predeterminado de Administrador de seguridad global a la que se asigna el usuario predeterminado, **admin**. Cuando se inicia sesión por primera vez en FSM con la contraseña establecida durante la instalación, se dispone de acceso administrativo total a todos los ajustes de configuración y a los siguientes permisos en los módulos que forman parte de su suscripción.

122. **Las contraseñas por defecto deben ser actualizadas tras su primer uso. Posteriormente, deben ser actualizadas periódicamente y cumplir con parámetros míninos de fortaleza que establezca cada organización.** FSM exige por defecto las siguientes condiciones para establecimiento de contraseñas (no modificables):

    - Longitud de 8 caracteres como mínimo.
    - Inclusión de al menos una letra en mayúscula y otra en minúscula, un número, y un carácter especial (como “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“ y “)”).

123. Adicionalmente a las medidas que exige la solución descritas anteriormente, como norma general de buenas prácticas, **se sugiere que adicionalmente las contraseñas sigan las siguientes directrices**:

    - Una longitud mínima de 12 caracteres, aunque se recomienda una longitud de 15 caracteres.
    - No deberán repetirse al menos las 5 últimas contraseñas utilizadas.
    - No deberá realizarse un nuevo cambio de contraseña en los 4 días posteriores al último cambio.

- El valor recomendado para la vigencia y expiración de contraseñas no debe ser superior a 180 días.
- Las cuentas creadas y no utilizadas deben eliminarse o inhabilitarse.

124. De acuerdo a las recomendaciones recogidas en el *Anexo I "Configuración de Administración Segura"* **se debe utilizar un doble factor de autenticación para el acceso administrador**, mediante token RSA o certificado de usuario, deshabilitando el acceso basado en contraseña.

125. Los administradores se pueden identificar utilizando credenciales de inicio de sesión de red o cuentas locales utilizadas solo para FSM. Las cuentas de red (*Network Accounts*) son cuentas del servicio de directorio existente en la red. Por ejemplo, se puede utilizar una cuenta del Directorio Activo corporativo para garantizar acceso administrativo a la gestión del FSM utilizando las credenciales de inicio de sesión del usuario en el dominio. Las cuentas locales (*Local Accounts*) son cuentas creadas específicamente para utilizarse en la FSM.

126. Para añadir una cuenta de red para la administración en la FSM consultar la guía de referencia [REF8] *Adding a network account*.

127. Para añadir una cuenta de administrador local, a través del entorno de administración de la consola FSM, se accederá al menú *Global Settings > General > Administrators,* haciendo *click* en el botón "*Add Local Account*". Para obtener información más detallada de cómo agregar una cuenta local de administración, consulte la guía de referencia [REF9] *Adding a local account.*

128. Los parámetros que definen la robustez de las contraseñas locales no son configurables, por lo que, si los requerimientos de contraseña no son suficientes para cumplir los requerimientos de la política corporativa, se sugiere la creación de administradores delegados basados en cuentas de red, o del servicio de directorio utilizado, las cuales cumplan los requerimientos necesarios.

129. En los entornos en los que se dispone de *appliances físicos*, el usuario admin local es independiente en cada plataforma física. De acuerdo a las recomendaciones recogidas en el *Anexo I "Configuración de Administración Segura"* estas cuentas de administración local no serán accesibles, siendo la única forma de acceso a la gestión de los *appliances* a través de la integración con FSM con autenticación robusta basada en certificados de cliente X.509

6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

130. Una vez cubiertas las consideraciones previas del apartado 5.4 (CONSIDERACIONES PREVIAS), se seleccionará el interfaz de red que se utilizará para acceder a la FSM vía web. En el caso de que el servidor tenga más de un interfaz de red, se dispondrá de un desplegable para seleccionar qué dirección IP se utilizará para la gestión. Esta dirección IP será la dirección que usarán el resto de componentes para la comunicación con el FSM.

131. En caso de configuración de *Content Gateways* en clúster, el interfaz de red de comunicación será un interfaz dedicado. En el caso de ser *appliances* físicos de

Forcepoint, la recomendación es que se utilice el puerto P1. Para más información sobre configuración de red del Content Gateway, consulte la guía de referencia Forcepoint, *[REF10] Content Gateway Manager Help.*

132. La comunicación entre los componentes *Forcepoint Security On-Prem* requiere una serie de puertos abiertos para su correcto funcionamiento. El listado completo de puertos y dirección del tráfico entre componentes puede encontrarse en *[REF11] Default ports for on-premises Forcepoint security solutions*.

    Importante: Para cumplir con las mejores prácticas de seguridad recomendadas, **se deben deshabilitar los puertos innecesarios y / o inseguros en sus redes y / o dispositivos**.

133. Para realizar el procedimiento de *hardening* o securización avanzada de las plataformas y componentes Forcepoint Security On-Prem, , es requerido seguir los procedimientos documentados en las guías de referencia *[REF12] Security Enhancements for Forcepoint On-Premises Products*. Esta información requiere de acceso registrado a Forcepoint como cliente o *partner*.

6.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

134. El entorno *Forcepoint Security On-Prem* incluye algoritmos criptográficos validados por NIST que proporcionan funciones criptográficas compatibles.

135. El módulo criptográfico C (versión 2.0.5) de Forcepoint, usado en todas las plataformas y sistemas operativos, posee el certificado del Programa de Validación del Módulo Criptográfico (CMVP) # 2875.

136. Los servicios de generación de claves criptográficas, cifrado, *hash* y firma se realizan con criptografía validada por el Programa de Validación de Algoritmo Criptográfico (CAVP). El módulo criptográfico C tiene los siguientes certificados CAVP:

    - *AES: #2234, #3264 y #4401*
    - *CVL: #36, #472 y #1110*
    - *DRBG: #264, #723 y #1419*
    - *DSA: #693, #933 y #1176*
    - *ECDSA: #347, #620 y #1058*
    - *HMAC: #1363, #2063 y #2925*
    - *RSA: #1145, #1664 y #2381*
    - *SHS: #1923, #2702 y #3628*
    - *3DES: #1398, #1853 y #2373*

137. Además, el entorno utiliza el Módulo criptográfico *Forcepoint Java Cryptographic Module* (versión 3.0.1) en servidores basados en Windows, como FSM. Dicho módulo recibió el Certificado CMVP # 3113. Los servicios de generación de claves

criptográficas, cifrado, *hash* y firma se realizan con criptografía validada por el Cryptographic Algorithm Validation Program (CAVP). El módulo criptográfico de Java tiene los siguientes certificados CAVP:

- *AES: #4702*
- *CVL: #1342, #1343, #1344 y #1345*
- *DRBG: #1600*
- *DSA: #1244*
- *ECDSA: #1160*
- *HMAC: #3114*
- *KAS: #130*
- *RSA: #2562*
- *SHA-3: #24*
- *SHS: #3849*
- *3DES: #2494*

138. El módulo criptográfico de Java se usa en el lado del servidor para proteger las comunicaciones entre FSM y las estaciones de trabajo del operador. Las diferentes configuraciones permiten al FSM utilizar los algoritmos aprobados por FIPS 140-2.

139. Dado que los protocolos SSL ya no se consideran seguros debido a diversas vulnerabilidades, y lo mismo ocurre con los protocolos TLS inferiores a 1.2, existe la necesidad de permitir que los clientes tengan un sistema que funcione solo con TLS 1.2. Todos los servidores (*Secure Listener*) son configurables para que puedan restringir TLS 1.2 solamente. Para ello, como se ha mencionado previamente, se deben seguir los pasos indicados en el *Anexo II "Empleo de mecanismos de cifrado robusto"* para forzar el uso de TLS v.1.2.

140. El acceso por SSH a los *appliances* Forcepoint se realiza por defecto con SSHv2. No se requiere configuración adicional para usar esta versión de protocolo. Se puede cambiar la versión a utilizar de SSH en la propia configuración del *appliance*, pero no se recomienda este cambio por motivos de seguridad. Además, como ya se ha indicado en el apartado 6.3 AUTENTICACIÓN punto el acceso vía SSH a los *appliances* se recomienda que sea deshabilitado una vez realizada la configuración inicial.

141. La comunicación entre los diferentes servicios de la solución está protegida mediante cifra. Sin embargo, existe una excepción: la comunicación entre los servicios *Filtering Service* de los *appliances* y el *Log Service del Forcepoint Security Manager* en la solución *Forcepoint Web Security On-Premise*. **Dicho canal no está cifrado. Para asegurar que está transmisión de datos está protegida, se debe seguir lo indicado en el *Anexo III – "Comunicación Segura entre FSM y Web Content Gateway"***. Dicho anexo detalla los pasos de configuración necesarios para el establecimiento de un canal de comunicación cifrado entre los *appliances*

y el servidor FSM de modo que la comunicación entre *Filtering Service* y *Logs Server* se realice de forma segura a través de un canal cifrado.

6.7 GESTIÓN DE CERTIFICADOS

142. En la solución *Forcepoint Security On-Prem*, se utilizan certificados para la comunicación entre la consola de gestión FSM y los componentes Forcepoint desplegados en red (servidores o *appliances*) y los agentes de los *endpoints*.

6.7.1 GESTIÓN DE CERTIFICADOS EN *FORCEPOINT WEB SECURITY*

143. Con objeto de mejorar la seguridad en la conexión entre los administradores y el interfaz de gestión, **se recomienda cambiar el certificado de la interfaz de gestión para garantizar que el tamaño mínimo de clave privada es de 3072 bits**. Este cambio se realizará en el servidor FSM y en los *appliances* Web Content Gateway, tal y como se describe a continuación. Los pasos para la realización de dicho cambio están recogidos en el *Anexo II - Empleo de mecanismos de cifrado robusto*.

6.7.2 GESTIÓN DE CERTIFICADOS EN *FORCEPOINT DLP*

144. Los componentes de *Forcepoint DLP* que utilizan certificados para la comunicación con la consola de gestión FSM son:

    a) Los agentes *Forcepoint DLP* desplegados en los equipos de usuarios.

    b) *Forcepoint Email DLP gateways*. La solución Forcepoint DLP incluye Forcepoint Protector, un *appliance* en distintos formatos (*HW* y *SW Content Gateway appliance*) que intercepta y analiza el tráfico de correo electrónico actuando como una MTA SMTP.

    c) *Forcepoint Web DLP gateways*.

    d) Servidores suplementales o redundantes. Los que se utilizan para distribuir, si se necesita, componentes en la red, disponer de equipos redundantes o de respaldo; o con funcionalidades específicas como pueden ser los OCRs.

145. Estos certificados son creados automáticamente durante la instalación de la consola de gestión Forcepoint FSM. Son propios de la infraestructura Forcepoint, por lo que no se pueden cargar certificados de terceros para esta comunicación entre componentes.

146. La duración por defecto de estos certificados es de 5 años. Pasado ese tiempo, **se deberá ejecutar el procedimiento de renovación de dichos certificados**, y volver a registrar los componentes con la consola FSM para que utilicen el nuevo certificado. Las guías de referencia para realizar estos procedimientos son:

    a) *[REF40] How to create and install a new server certificate in the TRITON EIP infrastructure*

    b) *[REF41] Rebuilding the Connection Between Forcepoint DLP Endpoint Clients and Endpoint Servers*

c) *[REF42] Re-registering Forcepoint DLP components.*

6.8 SERVIDORES DE AUTENTICACIÓN

147. En el proceso de autenticación de los usuarios para las tareas de administración, FSM puede conectarse con los siguientes servicios LDAP para identificación de los usuarios:
    - *Windows Active Directory (Native Mode)*
    - *Novell eDirectory*
    - *Oracle Directory Service*
    - *Lotus Notes/Domino*
    - Otros directorios genéricos basados en LDAP
148. Los usuarios de administración pueden ser autenticados por doble factor de autenticación en base a certificado o RSA SecureID. Ver información de referencia en el *Anexo I – Configuración de Administración Segura* y en la guía *[REF16] Configuring two-factor authentication*. **Se recomienda, siempre que sea posible, la configuración de autenticación multifactor para el acceso de administración**.
149. En cuanto a la autenticación de los usuarios como clientes del servicio que proporciona *Forcepoint Security On-Prem* en los *appliances*, los servicios de autenticación pueden ser:
    - *Integrated Windows Authentication - IWA (Kerberos con SPNEGO a NTLM)*
    - *Legacy NTLM authentication (NTLMSSP)*
    - *LDAP authentication*
    - *RADIUS authentication*
    - En los *Content Gateway* también es soportada la combinación de *Integrated Windows Authentication (IWA), Legacy NTLM, y LDAP utilizando Rule-Based Authentication.*
150. Además de encontrar información detallada de la configuración específica de cada método en las guías de instalación y configuración del producto, para este apartado concreto se puede consultar la siguiente guía de referencia: *[REF15] Content Gateway user authentication*.

6.9 SINCRONIZACIÓN HORARIA

151. La sincronización horaria es una de las consideraciones previas a tener en cuenta a la hora de comenzar la implantación de la solución *Forcepoint Security On-Prem.* Se trata de un servicio crítico para el correcto funcionamiento de la solución.
152. Independientemente del tipo de despliegue, **es recomendable la utilización de servicio NTP.**

153. Aunque la configuración NTP en la red es una tarea sencilla, se puede consultar la guía de referencia *[REF17] Time and date* para obtener más información sobre los diferentes comandos disponibles para su configuración.

6.10 ACTUALIZACIONES

154. La actualización del *software* y *firmware* de los componentes de *Forcepoint Security On-Prem* debe realizarse manualmente. Dependiendo de la versión de la que se parta y a la que se desee actualizar la plataforma, podría ser requerida la actualización en fases, a la versión inmediatamente superior o la recomendada según la documentación Forcepoint.

155. No existe una periodicidad concreta de publicación de actualizaciones mayores o menores del *firmware* de los productos, pero, habitualmente, **suele ser cada 6 meses y se recomienda leer detenidamente las *Release Notes*** para determinar las ventajas de su aplicación. Estas actualizaciones de *firmware* pueden incorporar indistintamente parches o solución de problemas identificados, o nuevas funcionalidades de producto.

156. Para poder hacer uso, en caso de necesidad, del servicio de soporte técnico de Forcepoint, es necesario que la plataforma tenga una versión instalada que se encuentre dentro del ciclo de vida de soporte. Se deben seguir las publicaciones de nuevas versiones de producto y obsolescencia de las versiones existentes.

157. Se debe garantizar que las **versiones de *software* y *firmware* desplegadas en el producto disponen de soporte de seguridad** por parte del fabricante para así disponer de parches de seguridad en caso de detectarse nuevas vulnerabilidades.

158. La publicación de *hotfixes* o parches no guarda ninguna periodicidad. Dependiendo del nivel de severidad de la corrección de funcionalidad o vulnerabilidad que pueda resolver el *hotfix*, se recomendará su aplicación e instrucciones concretas, en la documentación del parche y se deben seguir las indicaciones y recomendaciones de Forcepoint. Para obtener más información sobre la actualización de las soluciones se puede consultar la guía *[REF18] Upgrading Forcepoint Security Solutions to 8.5.x*.

159. El software y *firmware* para las actualizaciones debe ser descargado desde la web de Forcepoint, y **seguir las comprobaciones de integridad** del archivo a descargar mediante la comprobación SHA256 que se muestran para cada versión de archivo disponible para su descarga.

160. Los *appliances*, físicos y virtuales, para las soluciones de *Web Security* e *Email Security* además de actualización del *firmware* del sistema operativo, cuentan con actualizaciones periódicas de actualizaciones de seguridad, parches y *hotfixes*. Este proceso se puede realizar de forma controlada desde el interfaz de gestión de los *Content Gateways* (ver *[REF19] Forcepoint Security Appliance Manager Administrator Help)* o bien mediante interface de comandos CLI, siguiendo la guía de referencia *[REF20] V Series Appliance Upgrade Guide* .

161. Como información adicional, Forcepoint cuenta entre las guías de referencia con un apartado especial sobre actualizaciones, llamado *Upgrade Center*, para cada versión disponible. Para mayor facilidad, en la guía *[REF21] Upgrade Center for v8.5* se consolida toda la documentación necesaria para actualización de los componentes, recomendaciones, consideraciones previas, etc.

162. El componente *Forcepoint Web Security* realiza también actualizaciones periódicas de la base de datos para la categorización de la navegación de usuarios. La configuración de la tarea de descarga de esta base de datos se puede ver en la guía de referencia *[REF22] Configuring database downloads*.

163. Con respecto al componente Forcepoint DLP, las actualizaciones de políticas, reglas, clasificadores y otras características se realizan con las propias actualizaciones de las versiones *software* generales del producto.

164. Forcepoint DLP incluye muchas políticas predefinidas, clasificadores de contenido y tipos de archivos. Los equipos de investigación de Forcepoint mantienen las políticas y clasificadores actualizados. Cuando estos elementos se actualizan entre los ciclos de lanzamiento del producto, los administradores pueden actualizarlos a través de la página *Configuración> General> Actualizaciones* de políticas en el módulo *Seguridad de datos* de FSM. En la guía de referencia *[REF23] Updating predefined policies and classifiers* se encuentra la información al respecto.

165. Como buena práctica, **es también recomendable, seguir los procedimientos de copias de seguridad antes de comenzar cualquier tarea de actualización de las plataformas.**

6.11 AUTO-CHEQUEOS

166. Todos los componentes de *Forcepoint Security On-Prem* realizan chequeos continuos sobre la integridad y disponibilidad de los servicios necesarios para mantener la plataforma en el estado de salud óptimo.

167. A través de la interfaz de gestión deL FSM, se puede acceder a la información asociada a cada componente particular: web, email o DLP. Se puede acceder a los cuadros de mando que permiten obtener información e interactuar con los componentes cuando es posible, en caso de fallo.

168. Algunos de los auto chequeos que incorpora la solución, para cada plataforma son:

    a) *System Summary*. Muestra la información sobre el servidor, incluyendo sistema operativo, versión y espacio libre en disco.

    b) *CPU Usage*. Es el porcentaje de utilización de la CPU de la máquina para cada proceso en un rango de tiempo específico.

    c) *Memory Usage*. Es el porcentaje de utilización de la memoria de la máquina para cada proceso en un rango de tiempo específico.

169. Seleccionando cada uno de los componentes que aparecen, se podrá ver el estado de cada uno de ellos con parámetros más detallados, como:

a) Estado de cada uno de los componentes de la solución y si existe algún problema de disponibilidad o conectividad.

b) Tiempo de respuesta del motor de política DLP. Indica si existe sobrecarga o el tiempo es excesivo.

c) Volumen de peticiones y respuestas de cada uno de los componentes.

d) Mucha más información detallada de volumetría, carga y tiempos de respuesta de cada componente particular.

170. Para todos los módulos, también está disponible una sección avanzada ("*Advanced*"). Si se expande esta sección, se pueden ver las estadísticas sin procesar proporcionadas por el módulo seleccionado.

171. Si se desea, para tareas de resolución de problemas (*troubleshooting*) se puede descargar un archivo con los diagnósticos, con todos los logs y estadísticas. El archivo se descarga en formato .zip.

172. Como guía de referencia para la monitorización del estado de los componentes de Forcepoint DLP, ver *[REF24] Monitoring system health*.

173. Los chequeos no son configurables por el usuario. Están definidos por el fabricante para garantizar que los umbrales y estados de cada componente son los adecuados para el correcto funcionamiento de la solución.

6.12 SNMP

174. La monitorización SNMP aplica a los componentes *appliances* para la protección del correo electrónico y web. Desde el interfaz de gestión de los *Content Gateways* o por CLI se puede configurar si se desea utilizar SNMP v2 o v3. Para ver cómo realizar la configuración SNMP de los *appliances* desde el entorno de gestión de los appliances, ver la guía de referencia *[REF19] Forcepoint Security Appliance Manager Administrator Help*. Para configuración SNMP en modo CLI, ver la guía de referencia *[REF38] SNMP Traps and Queries.*

175. **Se recomienda la utilización de la versión SNMPv3 ya que proporciona mecanismos de seguridad y control de la información accedida.**

6.13 ALTA DISPONIBILIDAD

176. La solución *Forcepoint Security On-Prem* es una solución distribuida. Los módulos que se registran e identifican en el FSM siempre disponen de, al menos, un servicio de respaldo que hace referencia a la dirección IP del servidor que ejecuta este servicio de respaldo.

177. FSM permite su configuración con servidores de respaldo o réplicas. Para más información puede consultarse la referencia *[REF13] Managing Policy Broker Replication.*

178. *Forcepoint Web Security* permite el despliegue de múltiples *appliances* en modo alta disponibilidad, de modo que la caída de un *appliance* no afecte a los usuarios.

Para su despliegue puede consultarse la guía de referencia *[REF19] Forcepoint Security Appliance Manager Administrator Help*

179. En la solución Forcepoint DLP, la alta disponibilidad se puede realizar mediante el despliegue de servicios en servidores adicionales de Forcepoint (llamados *Suplemental Servers*). Para obtener más información se pude consultar la documentación de referencia para la instalación de servidores suplementales en *[REF26] Installation Guide Forcepoint DLP*.

180. Para garantizar un entorno seguro, según lo requerido en la presente documentación, **se debe bastionar y configurar los servidores suplementales con las mismas medidas, recomendaciones y buenas prácticas aplicadas para el despliegue de los servicios y servidores primarios.**

181. **Es muy recomendable complementar las medidas de alta disponibilidad con la realización de *backup* periódicos.** En el caso de que el entorno esté desplegado en una infraestructura virtual, se recomienda la realización de copias de seguridad también sobre la propia máquina virtual (*snapshots)*.

6.14 AUDITORÍA

6.14.1 REGISTRO DE EVENTOS

182. El entorno genera registros de auditoría para todos los eventos de inicio y cierre de sesión del administrador, cambios de política y cambios de configuración. Proporciona un conjunto de interfaces web que los administradores pueden usar para ver los eventos de auditoría registrados. Solo los roles "*Super Administrator*" y "*System Administrator*" podrán ver el registro de auditoría, a través de la GUI del FMS.

183. Los eventos del registro de auditoría contienen la siguiente información:

Parámetro	Descripción
Action ID	Número de identificación (ID) de la acción. Se puede consultar rápidamente los registros asociados a una acción introduciendo el número de ID en el campo "*Find Action ID*" y haciendo clic en "*Find*".
Date & Time	Fecha y hora en la sucedió la acción.
Administrator	Nombre y usuario administrador que inició la acción.
Access Role	Rol del administrador
Topic	Se puede filtrar el registro de auditoría por temática: – Administración: muestra las acciones realizadas por los administradores durante el período designado, la asignación de un nuevo role de acceso, la configuración de los directorios de usuarios, la agregación de un nuevo administrador y cambios en los permisos de un administrador. – *Log on/Log out*: muestra las acciones de inicio y cierre de sesión para saber qué administradores estuvieron activos durante el período designado. – *Status*: muestra las acciones realizadas en los informes y registros de estado: eliminación de una entrada o creación de un registro de auditoría. – *Policy Management* (Gestión de políticas): muestra las acciones realizadas sobre las políticas: actualización de políticas predefinidas, edición de políticas rápidas o creación de una nueva política. – *Reporting*: muestra las acciones realizadas en los informes durante el período designado como, por ejemplo, la modificación o creación un nuevo informe.

Parámetro	Descripción
	– *Incident Management* (Gestión de incidentes): muestra las acciones realizadas relacionadas con incidentes o incumplimientos de políticas. – *Archiving* (Archivado): muestra las acciones realizadas en el archivado de incidentes, como eliminar o restaurar un archivo. – *System Modules* (Módulos del sistema): muestra las acciones realizadas sobre los módulos del sistema como la modificación de una configuración o agregación de un módulo.
Action Performed	Descripción de la acción realizada por el administrador, por ejemplo, "*Incidente DLP exportado a archivo PDF*".
Details	Información adicional sobre la acción. Por ejemplo, para una acción de agregación de una política, regla o excepción, mostraría el nombre de la política, regla o excepción. Para acciones como la vista previa o la exportación de un informe, incluiría el nombre del informe.
Modified Item	Identifica el objeto que se modificó, agregó o eliminó. Para las acciones realizadas en incidentes incluye la identificación del incidente. Para la generación de informes, incluye un número identificador de tarea.

184. Para información más detallada sobre los diferentes niveles de eventos, se puede consultar la guía de referencia *[REF27] Viewing Forcepoint DLP Logs*.

6.14.2 ALMACENAMIENTO

185. La solución *Forcepoint OnPrem Security* utiliza dos (2) bases de datos, una para incidentes y otra para el repositorio de datos forenses.

186. La base de datos de incidentes requiere de la utilización de una base de datos *SQL Server*, donde se recoge información de cuándo una regla ha sido utilizada, cuántas veces, cuáles fueron los desencadenantes de esa violación, la fecha y hora, el origen, el destino, etc. También almacena los datos de configuración de las políticas.

187. Esta base de datos puede ser SQL Express, cuando se trata de un entorno con no más de 350 usuarios y necesidades de registro de actividades y reporting bajo.

188. Se desaconseja totalmente que la base de datos resida en la misma máquina servidor que los componentes de gestión Forcepoint para evitar posible impacto en el rendimiento global del servidor ante una alta demanda de recursos de máquina por los servicios Forcepoint y Microsoft SQL Server, salvo en el caso

comentado anteriormente, para entornos pequeños de no más de 350 usuarios aproximadamente.

189. La base de datos de incidentes es particionada cada 90 días. **Para optimizar el rendimiento, se debe realizar un archivado de particiones periódicamente.** El archivado de particiones se puede llevar a cabo de forma manual. Para información sobre la configuración del archivado, dimensionamiento y otras recomendaciones, consulte la guía de referencia *[REF29] Archiving Incident partitions*.

190. El repositorio forense contiene información sobre la transacción origen de un incidente, el contenido del cuerpo de un correo electrónico y los campos De:, Para: y Cc:, así como archivos adjuntos, categoría de URL, nombre de *host*, nombre de archivo, etc.

191. El almacenamiento del archivado se puede realizar localmente o seleccionar la ruta remota donde realizar este almacenado**. Se deberán aplicar las mismas medidas de seguridad de acceso y de comunicación a esta ubicación remota**.

192. Para saber más de estas bases de datos, ver la guía de referencia *[REF 28] Administering Forcepoint databases*.

6.15 *BACKUP*

193. Para realizar una copia de seguridad de los módulos de la solución, se utiliza la interfaz de gestión FSM. Será necesario seleccionar dónde se almacenará la copia de seguridad, local o en un repositorio remoto.

6.15.1 *BACKUP* SOLUCIÓN *FORCEPOINT WEB SECURITY*

194. *Forcepoint Web Content Gateway* permite guardar todos los ajustes de configuración actuales a través del interfaz de administración de *Content Gateway*. Existe la posibilidad de realizar este almacenamiento de la configuración sobre el sistema local del propio *appliance*, o bien enviarlo a un servidor FTP externo.

195. Se recomienda el uso de la primera opción: realizar el volcado de la configuración sobre el sistema de archivos del propio *appliance* y no emplear el mecanismo basado en el uso del protocolo FTP.

6.15.2 *BACKUP* SOLUCIÓN *FORCEPOINT DLP*

196. La copia de seguridad del sistema crea una carpeta y varias subcarpetas en la ruta especificada. Las subcarpetas contienen copias de seguridad de los siguientes componentes del sistema:

- *PreciseID_DB*: el repositorio de huellas digitales.
- *MngDB*: la base de datos de FSM (que contiene políticas, incidentes y configuración).
- *Forensics_repository*: la información de incidentes forenses (cifrada).

- *Crawlers*: información sobre el descubrimiento y rastreo de huellas digitales.

197. La copia de seguridad también contiene información adicional que puede incluir:

- Claves de cifrado. Incluyendo:
    - Las claves utilizadas por la acción "*Encrypt*" de las políticas DLP *Endpoint*. Estas claves son utilizadas para el cifrado de información sobre repositorios externos (USB, Discos externos) cuando se detecta la transmisión de información sensible y se desea proteger. Esas claves de cifrado son guardadas en la copia de seguridad.
    - Las claves de cifrado utilizadas para salvaguardar las evidencias de información en el repositorio forense.
- Archivo de suscripción.
- Paquetes de pólizas personalizados.
- Otra información relevante que completa una "instantánea" del sistema.

198. Durante la instalación del *software* en el FSM, se crean tareas dentro de las tareas programadas de Windows, cuyo momento de ejecución puede ser modificado para garantizar el cumplimiento de los requerimientos. La tarea relativa a la realización de copia de seguridad de los componentes Forcepoint se muestra en Windows con el nombre "*Websense TRITON AP-DATA Backup*".

199. Las copias de seguridad de los *appliances*, llamadas "*snapshots*", se realizan en cada uno de los *appliances* mediante CLI. Estas tareas e información adicional se pueden definir según la guía de referencia *[REF30] Backup and restore*.

7. FASE DE OPERACIÓN

200. Se recomienda que, durante la fase de operación y mantenimiento del producto, se sigan los siguientes procedimientos operativos:

- Realizar comprobaciones periódicas del *hardware* y *software* para asegurar que no se ha introducido *hardware* o *software* no autorizado.
- Realizar verificaciones periódicas del *firmware* activo y su integridad, para comprobar que está libre de *software* malicioso.
- Aplicar regularmente los parches de seguridad, con objeto de mantener una configuración segura.
- Mantener 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.
- Garantizar que la información de auditoria se guarda 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.

201. El *Anexo IV – Refuerzo de la Seguridad en la Operación* incluye ajustes de configuración que permiten el funcionamiento continuo de la plataforma de una forma más robusta. Entre estos cambios recomendados se incluye **habilitar el modo de funcionamiento FIPS; protección de las claves privadas en el *appliance*; y la utilización de certificados en caso de realizar intercepción sobre el tráfico cifrado en navegación.**

8. CHECKLIST

202. Se incluye un *checklist* que incluye todas las recomendaciones de seguridad:

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Comprobación del registro de acceso a sitio web de Forcepoint como cliente autorizado	☐	☐	
Registro de las licencias en FSM	☐	☐	
Actualización de firmware preinstalado en los *appliances*	☐	☐	
Chequeo del MD5 del software descargado desde Forcepoint	☐	☐	
Cumplimiento de las Consideraciones Previas específicas Windows	☐	☐	
Provisionamiento de usuario local *admin*	☐	☐	
Sincronización de tiempos de los componentes FP On-Prem Security	☐	☐	
Creación de las exclusiones de escaneo del software antivirus	☐	☐	
Deshabilitar DEP y UAC en FSM	☐	☐	
Aprovisionamiento de instancia SQL Server con los derechos requeridos	☐	☐	
Descarga de la Master Database en FP Web Security	☐	☐	
Apertura de puertos firewall para comunicación entre componentes	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Activación de servicio Examinador de Equipos en Windows Server de la FSM	☐	☐	
Revisión del Firewall Local en máquina con *Network Agent*	☐	☐	
Linux. - Verificación de asignación IP en interfaz para *Network Agent*	☐	☐	
Asignación de NIC en diferentes segmentos de red para *Network Agent*	☐	☐	
Linux. - Deshabilitar SeLinux	☐	☐	
Linux. - Deshabilitar firewall de Linux	☐	☐	
Linux. - Configuración de *Hostname*	☐	☐	
Comprobar que servidor Windows para *Forcepoint* no es un DC	☐	☐	
Revisión del nivel de restricción por GPO	☐	☐	
Orden de instalación de la FSM, Prioritario	☐	☐	
Hardening SQL Server	☐	☐	
Comprobación inicial de los componentes FSM del primer arranque	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado (FIPS-CC)	☐	☐	
Implementación del modo FIPS 140-2 en FSM	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Correcto arranque inicial de los *appliances* con imagen preinstalada	☐	☐	
Configuración básica inicial de los *appliances*. Conectividad	☐	☐	
Cambio a modo FIPS de *appliances*	☐	☐	
Comprobación de sincronización de los componentes *Forcepoint* en modo FIPS	☐	☐	
Creación de paquete de instalación *Forcepoint Endpoint*	☐	☐	
Establecer método de autenticación de administradores	☐	☐	
Establecer método de autenticación de usuarios para servicio de red	☐	☐	
Creación de Cuentas Locales de administración FSM	☐	☐	
Creación de Cuentas de Red de administración FSM	☐	☐	
Definición de Roles de Administración	☐	☐	
Asignación de roles a cuentas de administración	☐	☐	
Revisión de la política de contraseñas seguras	☐	☐	
Creación de certificado corporativo para administración FSM	☐	☐	
Importación del certificado de administración FSM	☐	☐	
Asignación de interfaces para gestión	☐	☐	
Deshabilitar puertos y servicios innecesarios	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Revisión Estado del Sistema	☐	☐	
Generación de Informes de Rendimiento	☐	☐	

9. REFERENCIAS

REF1 *Forcepoint System requirements for this version*

REF2 *Modo FIPS-2*

REF3 *Preparing for Installation*

REF4 *Guía completa de instalación Forcepoint On-Prem 8.5*

REF5 *Setting User Directory Information*

REF6 *Content Gateway Security*

REF7 *Accessing the CLI*

REF8 *Adding a network account*

REF9 *Adding a local account*

REF10 *Content Gateway Manager Help*

REF11 *Default ports for on-premises Forcepoint security solutions*

REF12 *Security Enhancements for Forcepoint On-Premises Products*

REF13 *Managing Policy Broker Replication*

REF14 *Accessing the Content Gateway manager*

REF15 *Content Gateway user authentication*

REF16 *Configuring two-factor authentication*

REF17 *Time and date*

REF18 *Upgrading Forcepoint Security Solutions to 8.5.x*

REF19 *Forcepoint Security Appliance Manager Administrator Help*

REF20 *V Series Appliance Upgrade Guide*

REF21 *Upgrade Center for v8.5*

REF22 *Configuring database downloads*

REF23 *Updating predefined policies and classifiers*

REF24 *Monitoring system health*

REF25 *Configuring general alert options*

REF26 *Installation Guide Forcepoint DLP*

REF27 *Viewing Forcepoint DLP Logs*

REF28 *Administering Forcepoint databases*

REF29 *Archiving incident partitions*

REF30 *Backup and restore*

REF31 *FIPS 140-2 and Forcepoint DLP white paper*

REF32 *FIPS 140-2*

REF33 *Applying FIPS 140-2 Validated Cryptography in Forcepoint DLP v8.5.2*

REF34 *Entering a Subscription Key*

REF35 *Excluding Forcepoint files from antivirus scans*

REF36 *Network Agent Quick Start*

REF37 Roles de Administración

REF38 SNMP Traps and Queries

REF39 Enhancing Forcepoint DLP with Boldon James Data Classification

REF40 How to create and install a new server certificate in the TRITON EIP infrastructure

REF41 Rebuilding the Connection Between Forcepoint DLP Endpoint Clients and Endpoint Servers

REF42 Re-registering Forcepoint DLP components.

10.ABREVIATURAS

3DES	*Triple Data Encryption Standard*
ACE	*Advanced Classification Engine*
AES	*Advanced Encryption Standard*
API	*Application Programming Interface*
BATV	*Bounce Address Tag Validation*
BEV	*Border Encryption Value*
BOM	*Bill of Materials*
CA	*Certification Authority*
CAVP	*Cryptographic Algorithm Validation Program*
CBC	*Cipher-Block Chaining*
CC	*Common Criteria for Information Technology Security Evaluation*
CCN-CERT	*Centro Criptológico Nacional Computer Emergency Response Team*
CG	*Content Gateway*
CLI	*Command Line Interface*
CMVP	*Cryptographic Module Validation Program*
CPU	*Central Processing Unit*
DB	*Database*
DC	*Domain Controller*
DEK	*Data Encryption Key*
DEP	*Data Execution Prevention*
DLP	*Data Loss Prevention*
DNS	*Domain Name System*
DRBG	*Deterministic Random Bit Generator*
DSA	*Digital Signature Algorithm*

DSS	*Digital Signature Standard*
EAL	*Evaluation Assurance Level*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
EE	*Encryption Engine*
ENS	*Esquema Nacional de Seguridad.*
FIPS	*Federal Information Processing Standard*
FQDN	*Fully Qualified Domain Name*
FSM	*Forcepoint Security Manager*
FTP	*File Transfer Protocol*
GB	*Gigabytes*
GCM	*Galois Counter Mode*
GPO	*Group Policy Object*
GUI	*Graphical User Interface*
HMAC	*Hashed Message Authentication Code*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IT	*Information Technology*
IV	*Initialization Vector*
IWA	*Integrated Windows Authentication*
KAS	*Kerberos Authentication Server*
KEK	*Key Encryption Key*
KMD	*Key Management Description*
LDAP	*Lightweight Directory Access Protocol*

MD5	*Message-Digest Algorithm 5*
NIC	*Network Interface Card*
NTLM	*New Technology (NT) Lan Manager*
NTLMSSP	*NTLM Security Support Provider*
NTP	*Network Time Protocol*
PCI	*Payment card industry*
RADIUS	*Remote Authentication Dial-In User Service*
RAID	*Redundant Array of Independent Disks*
RBG	*Random Bit Generator*
RFC	*Request for Comments*
RNG	*Random Number Generator*
RSA	*Rivest, Shamir and Adleman (algorithm for public-key cryptography)*
SAR	*Security Assurance Requirement*
SED	*Self Encrypting Drive*
SFP	*Security Functional Policy*
SFR	*Security Functional Requirement*
SHA	*Secure Hash Algorithm*
SHS	*Secure Hash Standard*
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*
SP	*Service Pack*
SPD	*Security Problem Definition*
SPI	*Serial Peripheral Interface*
SPNEGO	*Simple and Protected GSSAPI Negotiation Mechanism*
SQL	*Structured Query Language*

SSL	*Secure Socket Layer*
ST	*Security Target*
TCP	*Transmission Control Protocol*
TLS	*Transport Layer Security*
TOE	*Target of Evaluation*
TSF	*TOE Security Functions*
UAC	*User Account Control*
URL	*Uniform Resource Locator*
XOR	*Exclusive or*
XTS	*XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing*

11.ANEXOS

Anexo I - Configuración de Administración Segura

Anexo II - Empleo de mecanismos de cifrado robusto

Anexo III - Comunicación Segura entre FSM y Web Content Gateway

Anexo IV - Refuerzo de la seguridad en la operación

PUBLICACIONES DE DEFENSA

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