GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 1401

Configuración segura de pasarelas de AUTEK INGENIERÍA

Junio 2018

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.06.07 11:11:25 +02'00'

NIPO: 785-18-035-6

Fecha de Edición: junio 2018
Autek Ingeniería ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

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

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Junio de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

1. INTRODUCCIÓN

1. Los dispositivos de protección de perímetro PSTgateways del fabricante Autek Ingeniería están especialmente diseñados para controlar el intercambio de información entre diferentes dominios de seguridad y evitar la entrada y la salida de información no autorizada, lo que permite implementar mecanismos de defensa en profundidad y neutralizar o minimizar el efecto de las APT[1].
2. El término "dominio de seguridad' normalmente se emplea para referirse a redes con diferentes niveles de clasificación, pero también incluye redes con distintas autoridades operativas o redes sin clasificar que se mantienen aisladas por razones de seguridad.
3. Para permitir este intercambio controlado, las pasarelas proporcionan las siguientes funciones básicas de seguridad:
    a) **Separación de redes**. Ruptura de la continuidad de los protocolos de comunicaciones entre dos redes interconectadas en todas las capas del modelo OSI. Las pasarelas PSTgateways están formadas por dos unidades, una que se conecta a la red interna (a la que protege) y otra a la externa, unidas por un dispositivo pasivo de lectura y escritura. Ambas unidades se comunican mediante un protocolo desarrollado *ad-hoc*. De esta forma se asegura que nunca se establece una conexión TCP/IP entre las entidades origen y destino (independientemente de la configuración software del dispositivo), ni que a la red externa lleguen paquetes con información de la red interna.
    b) **Filtrado de contenidos**. Las pasarelas permiten el paso de información siempre que cumpla las reglas de filtrado definidas, tanto para la entrada como para la salida. Además, para evitar la divulgación de información no autorizada desde la red interna, las pasarelas PSTgateways utilizan mecanismos de firma electrónica, de tal forma que solo se permite el envío cuando la información está firmada y se ha verificado dicha firma.
    c) **Separación de flujos de información de entrada/salida**.
4. La arquitectura de PSTgateways proporciona una plataforma certificada cuyas características principales son: seguridad, alta disponibilidad y facilidad de uso. Además, permiten que toda la configuración y administración del producto se realice desde el dominio de alta seguridad.

[1] *Advanced Persistent Threat.* Amenazas persistentes avanzadas

2. OBJETO Y ALCANCE

5. Los productos de la familia PSTgateways comparten la misma arquitectura y se diferencian en los servicios de flujo de datos que proporcionan.
6. En la presente guía se recoge el procedimiento de empleo seguro para dos productos de esta familia: PSTfile y PSTmail, que contienen los siguientes servicios:
    a) PSTmail – Pasarela segura de correo electrónico:
        i. IM – Servicio de entrada de correo.
        ii. OM – Servicio de salida de correo.
    b) PSTfile – Pasarela segura de ficheros:
        i. IF – Servicio de entrada de ficheros.
        ii. OF – Servicio de salida de ficheros.
7. Las medidas recogidas en este documento son de dos tipos: obligatorias y recomendadas. Para cumplir con el procedimiento de empleo seguro sería necesario implementar, como mínimo, todas las medidas obligatorias.

2.1 ORGANIZACIÓN DEL DOCUMENTO

8. El capítulo 3 contiene una visión general de la arquitectura PSTgateways.
9. Los capítulos 4, 5 y 6 son los que recogen todas las medidas de seguridad requeridas para el empleo seguro del producto. Cada uno de ellos recoge la siguiente información:
    a) Medidas requeridas en la fase de **Planificación** (capítulo 4).
    b) Medidas requeridas en la fase de **Despliegue e instalación** (capítulo 5).
    c) Medidas requeridas en la fase de **Mantenimiento** (capítulo 6).
10. Los mismos principios y medidas se tratan con el nivel de detalle adecuado a cada fase:
    a) Durante la planificación de manera introductoria y de más alto nivel.
    b) Durante el despliegue e instalación de manera concreta y detallada.
11. En el Anexo I se incluye una lista de comprobación que puede ser usada de referencia.

3. ARQUITECTURA DE LAS PASARELAS PSTGATEWAYS

3.1 COMPONENTES

12. Todos los productos PSTgateways están formados por dos unidades tipo *appliance,* cada una de ellas conectada a un dominio de seguridad. Además,

existe la posibilidad de trabajar con redundancia hardware (alta disponibilidad), en cuyo caso serían 4 unidades.

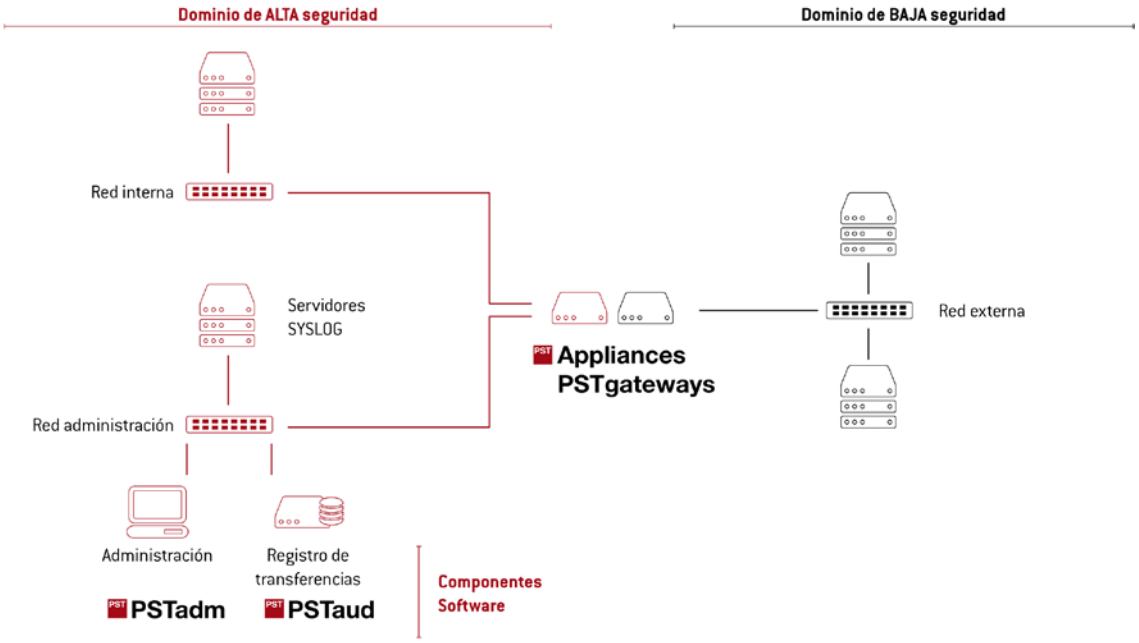

Figura 1 Componentes PSTgateways

13. También forman parte del sistema dos componentes software: el de administración (PSTadm) y el de auditoría (PSTaud), que permite almacenar la información de las transferencias de información que se han realizado a través de la pasarela.
14. Los *appliances* se suministran con el *firmware* preinstalado y con un DVD autoarrancable para cada uno de ellos que permite realizar un control de integridad del firmware e instalar nuevas versiones a medida que estén disponibles.

3.2 INFRAESTRUCTURA DE ADMINISTRACIÓN

15. Además de las unidades que componen las pasarelas, es necesario disponer de una infraestructura de administración que se conectará a la unidad interna en el dominio de alta seguridad y que está formada por los siguientes equipos:

    a) **Equipos de administración**: Uno o varios equipos de administración para instalar en ellos el software PSTadm. Estos equipos deberán disponer de un Sistema Operativo Windows versión 7 o superior.

    b) **Servidor de registro de transferencias:** Un equipo para instalar el software de registro de transferencias PSTaud. Este equipo deberá disponer de un Sistema Operativo Windows versión 7 o superior.

c) **Servidores de SYSLOG:** Uno o dos servidores de SYSLOG. Los productos PSTgateways tienen capacidad de enviar eventos de funcionamiento y de seguridad a servidores distintos.

3.3 ESQUEMA DE DESPLIEGUE

16. El despliegue de la pasarela se llevará a cabo en los siguientes pasos:
    a) Instalación física de los *appliances*.
    b) Configuración local mínima del sistema en el *appliance* interno.
    c) Instalación del software adicional. (PSTAdm y PSTAud).
    d) Configuración remota desde dominio de alta seguridad:
        i. Alta de administradores.
        ii. Configuración de la infraestructura.
        iii. Configuración de los servicios de flujo de datos.
    e) Puesta en servicio.

3.4 ENTORNO

17. Los productos de la familia PSTgateways son pasarelas del nivel de aplicación, pensados para ser el único punto de intercambio de información entre las dos redes que separan y no permitir la transferencia de paquetes ni de conexiones entre ellas.
18. Las pasarelas se consideran dispositivos de protección de perímetro que normalmente se instalan en una DMZ con cortafuegos en ambos extremos, que sería equivalente a:
    a) Una arquitectura de protección de perímetro Tipo 7 de acuerdo a la clasificación establecida en la guía CCN-STIC-811 Interconexión en el ENS.
    b) Una arquitectura del tipo SPP-2, de acuerdo a lo estipulado en la guía CCN-STIC-302 Interconexión de sistemas TIC que manejan información nacional clasificada en la Administración.

    No obstante, excede del ámbito de esta guía el prescribir una determinada topología.

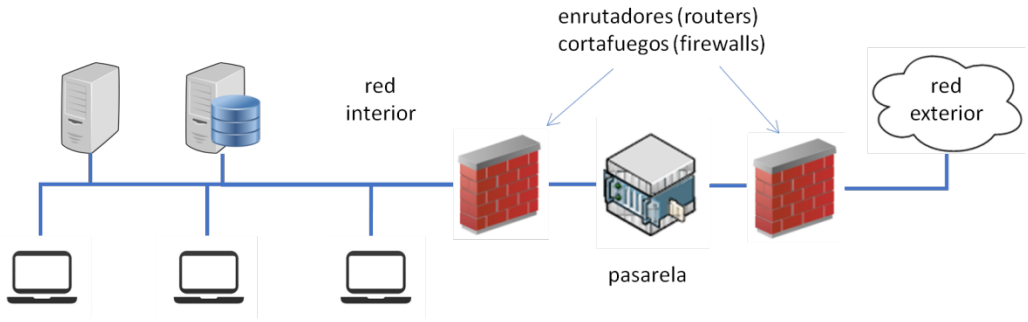

Figura 2 Ejemplo de arquitectura de protección de perímetro tipo 7 (APP-7)

3.5 CONFIGURACIÓN DE CORTAFUEGOS

19. La configuración de los cortafuegos deberá permitir exclusivamente el tráfico necesario para el funcionamiento de la pasarela. Este tráfico se divide en dos partes:

    a) La parte general de administración y auditoría, descrita en el anexo 'Características del tráfico de red' del manual de instalación y puesta en servicio [IG].

    b) La parte correspondiente a cada servicio de flujo de datos, descrita en el anexo *'Características del tráfico de red'* del manual de operación de cada servicio [OG-IF], [OG-OF], [OG-IM] y [OG-OM].

4. FASE DE PLANIFICACIÓN

20. Las consideraciones contenidas en este apartado deberán tenerse en cuenta durante una fase temprana del proyecto de implantación de la pasarela. Básicamente, se tienen en cuenta aspectos relacionados con:

    a) Seguridad física.

    b) Flujos de datos.

    c) Topología de red.

    d) Infraestructura de administración.

    e) Infraestructura de clave pública (PKI).

    f) Administradores.

4.1 SEGURIDAD FÍSICA

21. **Entorno controlado**: los *appliances* de la pasarela deberán desplegarse en una zona de acceso restringido. Por ello, será necesario implementar las medidas técnicas y organizativas necesarias para garantizar que solo los administradores locales dispongan de acceso físico a los *appliances*.

4.2 FLUJOS DE DATOS

22. **Mínimos flujos de datos**: Las pasarelas desplegadas deberán disponer únicamente de licencias de los servicios que vayan a utilizar.
23. **Protocolos seguros**:
    a) Para las comunicaciones de la pasarela con los servidores remotos de ficheros y en las comunicaciones entre *appliances* de la pasarela se utilizarán los protocolos FTPS o SFTP. El orden de preferencia será de FTPS sobre SFTP. Además de confidencialidad y garantía de integridad deberán aportar autenticación de cliente. Este requisito es especialmente crítico en redes sobre las que no se tenga control.
    b) Para las comunicaciones de la pasarela con los servidores de ficheros de la red interna se utilizarán, preferiblemente, los protocolos FTPS o SFTP. El orden de preferencia será de FTPS sobre SFTP. Además de confidencialidad y garantía de integridad deberán aportar autenticación de cliente.

4.3 TOPOLOGÍA DE RED

24. **Red de administración dedicada:** Se recomienda utilizar una red de administración dedicada en el dominio de alta seguridad, con objeto de separar el tráfico de datos del tráfico de administración. Los *appliances* internos tienen una interfaz de red prevista para tal fin.
25. **Redes aisladas:** Las redes entre las cuales se producirá el intercambio de información a través de la pasarela no deberán estar conectadas por ningún otro medio.

4.4 INFRAESTRUCTURA DE ADMINISTRACIÓN

26. **Consola de administración PSTadm:** La consola de administración de la pasarela (PSTadm) deberá instalarse exclusivamente en los equipos de administración necesarios.
27. **Servidor de auditoría PSTaud:** Deberá disponerse de un servidor o estación de trabajo donde se instalará tanto el servicio de registro de información de transferencias (PSTaud) como la base de datos empleada para dicho registro.
28. **Servidores de SYSLOG:** Deberá disponerse de uno o dos servidores de SYSLOG para recibir los eventos de funcionamiento y seguridad. Es recomendable integrar los eventos en el sistema de monitorización de la organización.
29. En el caso de que las pasarelas se vayan a emplear en sistemas clasificados, los servidores anteriormente indicados deberán estar acreditados.

4.5 INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

30. Deberá disponerse de una infraestructura de clave pública con capacidad de proporcionar y gestionar las claves y los certificados necesarios para la autenticación y el cifrado de las comunicaciones entre componentes del sistema y entre los administradores y el sistema.
31. ***Common Name* únicos:** Los productos PSTgateways utilizan el *Common Name* (CN) de los certificados para su identificación. Deberá evitarse la duplicidad de los *Common Name* de los certificados emitidos por las entidades certificadoras configuradas en el sistema.
32. **Dispositivos de seguridad hardware:** Los certificados de administración se deberán almacenar en dispositivos de seguridad hardware externos: *criptotokens*, tarjetas inteligentes, etc. para garantizar la seguridad de la clave privada y evitar que pueda ser exportada. De este modo, la autenticación de los administradores será de doble factor.
33. **Requisitos mínimos de certificados:** los certificados utilizados serán X509.v3 y utilizarán claves de cifrado con una fortaleza criptográfica de 128 bits o superior (RSA 3.072 bits o superior) y funciones resumen SHA-2, de acuerdo a lo indicado en la CCN-STIC-807 Criptografía de empleo en el ENS.

4.6 ADMINISTRADORES

34. Los administradores locales deberán ser los únicos con acceso físico a los *appliances*. La identificación y autenticación de éstos se realizará aplicando medios técnicos u organizativos ajenos a los productos PSTgateways. En la configuración local, serán los responsables de dar de alta los certificados de los administradores raíz. A partir de aquí, el *appliance* interno se encargará de verificar la identidad y autenticar a los administradores. Los administradores raíz, dan de alta al resto de perfiles de administración.

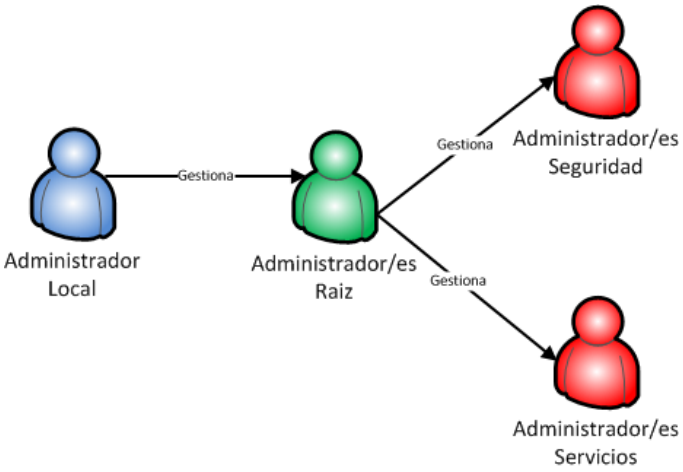

Figura 3 Jerarquía de perfiles de administración

35. **Perfiles de administración:** Se debe disponer del mínimo número de administradores posibles y cada uno de ellos debe disponer de los mínimos privilegios necesarios.

> *Los perfiles de administración disponibles, así como la funcionalidad asociada a cada uno de ellos, se describen en el capítulo 5 'Perfiles de administración' del manual de operación [OG].*

5. FASE DE DESPLIEGUE E INSTALACIÓN

5.1 SEGURIDAD FÍSICA

36. **Comprobaciones de integridad:** en la recepción de los equipos se deberán realizar una serie de comprobaciones que permitan garantizar la integridad del material recibido, tanto hardware como software.

    a) Comprobación de que las cajas no han sido abiertas.

    b) Comprobación de la firma del mensaje enviado por Autek Ingeniería.

    c) Comprobación de integridad de las imágenes ISO correspondientes al producto PSTgateways. Para ello, el fabricante suministrará un hash SHA256 que deberá coincidir con el hash SHA256 de la imagen ISO del software proporcionado.

    d) Comprobación de la integridad del firmware instalado en los *appliances* arrancando desde los soportes físicos (DVDs) recibidos.

> *Los procedimientos que describen estas comprobaciones se detallan en el capítulo 2 'Recomendaciones de seguridad' del 'Manual de instalación y puesta en servicio' [IG].*

37. **Entorno controlado:** la instalación de los *appliances* de la pasarela se deberá realizar en un entorno físicamente controlado.

5.2 INFRAESTRUCTURA DE ADMINISTRACIÓN

38. **Sistemas operativos securizados:** El sistema operativo de los equipos que se destinen a administración y registro de transferencias deberá estar securizado siguiendo las guías CCN-STIC correspondientes. (Ver listado de guías serie 500 y serie 600 en la página del CCN-CERT www.ccn-cert.cni.es).

39. **Longitud mínima de claves de certificados:** Deberán utilizarse certificados con claves de longitud igual o superior a las indicadas en el párrafo 33.

40. **Mínimas propiedades de uso de la clave de los certificados:** Deberán establecerse las mínimas propiedades posibles de uso de la clave en los certificados utilizados.

Las propiedades de uso de la clave de los distintos certificados se detallan en el anexo I 'Características de los certificados digitales' del 'Manual de instalación y puesta en servicio' [IG].

41. **Uso de *criptotokens* de seguridad o almacenes de claves hardware:** Las claves y certificado digitales de los administradores deberán almacenarse en dispositivos hardware.

5.3 ADMINISTRADORES

5.3.1. ADMINISTRADOR LOCAL

42. El administrador local tiene como única función realizar la configuración local de la pasarela.

La funcionalidad asociada al administrador local se describe en los capítulos 4 y 5 del 'Manual de instalación y puesta en servicio' [IG].

43. **Establecimiento de contraseña en BIOS en los *appliances***. Se deberá establecer una contraseña de acceso a la BIOS de cada uno de los *appliances*.
44. En caso de que el sistema en el que se instale la pasarela sea clasificado, la política de contraseñas deberá cumplir con los requisitos indicados en la guía CCN-STIC-301 para el nivel de clasificación correspondiente.
45. **Configurar la interfaz de administración.** Se deberá activar y configurar la interfaz de administración para separar el tráfico de administración del tráfico de datos.
46. **Mínimas CAs de confianza.** Se deberán utilizar las mínimas CAs necesarias para el funcionamiento del sistema.
47. **Mínimos CNs de administradores raíz.** Se deberán configurar únicamente los '*Common name*' (CN) del mínimo número de administradores raíz posibles.

5.3.2. ADMINISTRADOR RAÍZ

48. El administrador raíz tiene como única función la gestión de administradores y equipos desde los que se puede administrar la pasarela.

La funcionalidad disponible al administrador raíz se escribe en el capítulo 6 del 'Manual de operación' [OG].

49. **Limitación de equipos de administración por IP**. Se deberán limitar las direcciones IP de los equipos desde los que se puede administrar la pasarela.
50. **Mínimo número de administradores y mínimos privilegios.** Se deberán dar de alta el mínimo número de administradores necesarios para la pasarela y se configurarán con los menores privilegios posibles.

5.3.3. ADMINISTRADOR DE SEGURIDAD

51. El administrador de seguridad tiene como principal función realizar la configuración del entorno de la pasarela.

> *La funcionalidad disponible al administrador de seguridad se describe en el capítulo 7 del 'Manual de operación' [OG].*

52. **Configuración de servidores de SYSLOG.** Se deberá incluir en la configuración de la pasarela las direcciones de los servidores de SYSLOG.
53. **Configuración de la severidad mínima de los eventos.** Se deberá realizar la configuración de la severidad mínima de los eventos que serán enviados a los servidores de SYSLOG.
54. **Configuración del servidor de registro de transferencias.** Se deberá incluir en la configuración de la pasarela las direcciones del servidor de registro de transferencias.

5.3.4. ADMINISTRADOR DE SERVICIOS

55. El administrador de servicios es el encargado de realizar la configuración de los servicios (flujos de datos) y de los canales asociados.

> *La funcionalidad disponible al administrador de servicios se describe en el capítulo 8 del 'Manual de operación' [OG].*

56. **Configuración de servidores por IP**. Se deberán utilizar direcciones IP en lugar de nombres de dominio en la especificación de servidores.
57. **Filtrado de datos.** Se deberán utilizar las opciones de filtrado de datos (tipo de datos, tamaño de datos, etc.) disponibles en cada uno de los flujos para restringir lo máximo posible los datos que se van a transferir.
58. **Configuración de auditoría.** Se deberá activar el registro de información de transferencias de todos los servicios.
59. **Mínimas CAs de confianza en servicios con protocolos seguros.** Se deberá utilizar el mínimo número de CAs necesarias para el funcionamiento del servicio.

5.4 FLUJOS DE DATOS

5.4.1. SERVICIO ENTRADA DE CORREO IM

> *La información de configuración del servicio se describe en el manual de operación del servicio entrada de correo [OG - IM].*

60. **Protocolos seguros.** Todos los protocolos de transferencia de correo (SMTP, POP o IMAP) utilizados deberán correr sobre TLS 1.2.

61. **Autenticación de servidor.** Se deberá forzar la validación de la identidad de los servidores de correo: Configuración del 'Common Name' (CN) del certificado del servidor.
62. **Configuración de registro extendido.** Deberá configurarse la opción de registro extendido, que permite guardar información más completa sobre las transferencias que se realizan.

5.4.2. SERVICIO SALIDA DE CORREO OM

La información de configuración del servicio se describe en el manual de operación del servicio salida de correo [OG - OM].

63. **Protocolos seguros.** El protocolo SMTP, de transferencia de ficheros, deberá correr sobre TLS 1.2.
64. **Autenticación de servidor.** Se deberá forzar la validación de la identidad de los servidores de correo: Configuración del 'Common Name' (CN) del certificado del servidor.
65. **Configuración de registro extendido.** Se deberá configurar el registro de información de transferencias extendido.
66. **Configuración de nombres de dominio internos.** Se deberá crear una lista de los nombres de domino internos para que se eliminen de las cabeceras de los mensajes de salida.
67. **Mínimos CNs de supervisores.** Los supervisores son aquellos usuarios que, usando mecanismos de firma electrónica, tienen la capacidad de autorizar la salida de correo de los usuarios a los que supervisan. Se recomienda configurar únicamente, en cada canal, los 'Common name' (CN) de los supervisores necesarios.
68. **Limitar envíos directos.** Se recomienda limitar, en la medida de lo posible, que un supervisor se autorice los correos de salida a sí mismo.
69. **Enviar copia interna.** Para cada canal, se recomienda configurar la opción de copia interna, que permite enviar una copia exacta del mensaje enviado a la red externa a un buzón de la red interna.

5.4.3. SERVICIO ENTRADA DE FICHEROS IF

La información de configuración del servicio se describe en el manual de operación del servicio entrada de ficheros [OG - IF].

70. **Protocolos seguros.** Se deberán utilizar los protocolos FTPS ó SFTP.
71. **Autenticación de servidor.** Se deberá forzar la validación de la identidad de los servidores de ficheros:
    a) En FTPS: configuración del 'Common Name' (CN) del certificado del servidor.

b) En SFTP: configuración de la huella digital ('Fingerprint') del servidor.

5.4.4. SERVICIO SALIDA DE FICHEROS OF

La información de configuración del servicio se describe en el manual de operación del servicio salida de ficheros [OG - OF].

72. **Protocolos seguros.** Se deberán utilizar los protocolos FTPS o SFTP.
73. **Autenticación de servidor.** Se deberá forzar la validación de la identidad de los servidores de ficheros:
    a) En FTPS: configuración del *Common Name* (CN) del certificado del servidor.
    b) En SFTP: configuración de la huella digital (*Fingerprint*) del servidor.
74. **Uso de algoritmo de firma seguro.** Se deberán utilizar un algoritmo de firma RSA con longitud de claves 3072 o superior y que utilice funciones resumen SHA-2.
75. **Mínimos CNs de las autoridades de firma.** Se recomienda configurar únicamente, en cada canal, los *Common name* (CN) de las autoridades de firma necesarias.

6. FASE DE EXPLOTACIÓN

76. Se ha establecido una clasificación de las distintas recomendaciones de acuerdo a los perfiles de los administradores que las tienen que llevar a cabo.

6.1 ADMINISTRADOR LOCAL

77. Estas tareas se podrían incorporar al plan de mantenimiento. Se recomienda registrar las acciones realizadas y las fechas de caducidad de los certificados.
78. El administrador local deberá:
    a) **Realizar controles de integridad periódicos** de los *appliances* de la pasarela. La ejecución de esta operación se realiza con el sistema detenido.
    b) **Actualizar del sistema.** Se deberá mantener el *firmware* de los *appliances*, la BIOS, el software de administración y el registro de transferencias actualizado a la última versión disponible.
    c) **Actualizar los certificados.** Para ello deberá realizar un control de la caducidad de los certificados de los componentes del sistema, solicitar su renovación y realizar su instalación.

6.2 ADMINISTRADOR RAÍZ

79. **El administrador raíz deberá gestionar las altas y bajas del resto de administradores.** Es importante eliminar los administradores que ya no estén activos.

6.3 ADMINISTRADOR DE SEGURIDAD

80. El administrador de seguridad deberá:

    a) **Monitorizar eventos de seguridad generados por la pasarela.**

    b) **Monitorizar el registro de información de transferencias realizadas por la pasarela.**

6.4 ADMINISTRADOR DE SERVICIOS

81. **El Administrador de servicios se ocupará de la supervisión de los flujos de datos.** Se deberá realizar una supervisión activa de los servicios y canales. Prestará especial atención a mantener parados los servicios de flujos de datos que no se estén utilizando y desactivar los canales que no presten servicio.

7. REFERENCIAS

IG	PSTgateways - Manual de instalación y puesta en servicio (550-1)
OG[2]	PSTgateways - Manual de operación (550-2)
OG-IM	PSTgateways – Manual de operación IM. Servicio entrada de correo (550-7)
OG-OM	PSTgateways – Manual de operación OM. Servicio salida de correo (550-8)
OG-IF	PSTgateways – Manual de operación IF. Servicio entrada de ficheros (550-4)
OG-OF	PSTgateways – Manual de operación OF. Servicio salida de ficheros (550-5)
STIC.1	CCN-STIC-811 Interconexión en el ENS.
STIC.2	CCN-STIC-302 Interconexión de sistemas TIC que manejan información nacional clasificada en la Administración.
STIC.3	CCN-STIC-807 Criptografía de empleo en el ENS.
STIC.4	CCN-STIC-301 Requisitos STIC

[2] Los manuales de operación de los servicios (IF, OF, IM y OM) están incluidos en el Manual de operación [OG] en ediciones anteriores a la revisión 8.

8. ABREVIATURAS

BIOS	*Basic Input/Output System*
CA	*Certification Authority*
CCN	Centro Criptológico Nacional
CN	*Common Name*
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
DMZ	*Demilitarized Zone*
ENS	Esquema Nacional de Seguridad
FTPS	*File Transfer Protocol over Secure Sockets Layer*
IMAP	*Internet Message Access Protocol*
OSI	*Open System Interconnection*
POP	*Post Office Protocol*
RSA	Rivest, Shamir y Adleman
SFTP	*SSH File Transfer Protocol*
SHA	*Secure Hash Algorithm*
SMTP	*Simple Mail Transfer Protocol*
STIC	*Seguridad de las Tecnologías de la Información y la Comunicación*
TLS	*Transport Layer Security*

ANEXO I. LISTA DE COMPROBACIONES

82. La siguiente lista de comprobaciones permite realizar un control sobre el nivel de implantación de las medidas de seguridad en la fase de despliegue e instalación de las pasarelas PSTgateways.

	MEDIDAS DE SEGURIDAD	
Seguridad física	☐	Comprobación de integridad de las cajas
	☐	Comprobación de la firma del correo electrónico
	☐	Comprobación de integridad de los DVDs
	☐	Comprobación de integridad del firmware de los *appliances*
	☐	Entorno físico controlado
Infraestructura de administración	☐	Sistemas operativos securizados
	☐	Longitud de clave de certificados
	☐	Mínimas propiedades de uso de la clave de los certificados
	☐	Uso de criptotokens de seguridad o almacenes de claves hardware
Administrador local	☐	Establecimiento de contraseña BIOS en los *appliances*
	☐	Configuración de la interfaz de administración
	☐	Mínimas CAs de confianza
	☐	Mínimos CNs de administradores raíz
Administrador raíz	☐	Limitación de equipos de administración por IP
	☐	Mínimo número de administradores y mínimos privilegios
Administrador de seguridad	☐	Configuración de servidores SYSLOG
	☐	Configuración de la severidad mínima de los eventos
	☐	Configuración del servidor de auditoría

Administrador de servicios	Servicio de entrada de correo (IM)	☐	Configuración de servidores por IP
		☐	Filtrado de datos
		☐	Configuración de auditoría
		☐	Mínimas CAs de confianza en servicios con protocolos seguros
		☐	Protocolos seguros
		☐	Autenticación del servidor
		☐	Configuración de registro extendido
	Servicio de salida de correo (OM)	☐	Configuración de servidores por IP
		☐	Filtrado de datos
		☐	Configuración de auditoría
		☐	Mínimas CAs de confianza en servicios con protocolos seguros
		☐	Protocolos seguros
		☐	Autenticación del servidor
		☐	Configuración de registro extendido
		☐	Configuración de nombres de dominio internos
		☐	Mínimos CNs de supervisores (*)
		☐	Limitar envíos directos (*)
		☐	Enviar copia interna (*)
	Servicio de entrada de ficheros (IF)	☐	Configuración de servidores por IP
		☐	Filtrado de datos
		☐	Configuración de auditoría
		☐	Mínimas CAs de confianza en servicios con protocolos seguros
		☐	Protocolos seguros
		☐	Autenticación de servidor
	Servicio de salida de ficheros (OF)	☐	Configuración de servidores por IP
		☐	Filtrado de datos
		☐	Mínimas CAs de confianza en servicios con protocolos seguros
		☐	Configuración de registro de transferencias

		☐	Mínimos CNs de las autoridades de firma
		☐	Protocolos seguros
		☐	Autenticación de servidor
		☐	Uso de algoritmo de firma seguro

Nota: Las medidas con carácter recomendado se encuentra marcadas con un asterisco (*), el resto de medidas se consideran obligatorias.