centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1408

Procedimiento de empleo seguro Diodo Autek Ingeniería

Abril 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.04.15 15:50:37 +02'00'

NIPO: 083-19-161-8

Fecha de Edición: abril de 2019
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, actualizado 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.

Abril de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. Introducción

1. Los diodos de datos PSTdiode están diseñados para transferir información en un único sentido entre dos dominios de seguridad aislados con garantía física de transmisión unidireccional.
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. PSTdiode está basado en el dispositivo de comunicación unidireccional PSTdiode ATKDDL® desarrollado por Autek Ingeniería y certificado *Common Criteria* EAL4+. Este dispositivo se compone de una tarjeta transmisora y una tarjeta receptora unidas mediante un cable de fibra óptica.
4. Además de la transferencia de información en un único sentido, PSTdiode proporciona las siguientes funciones básicas de seguridad:
    a) Separación de redes. Ruptura de la continuidad de los protocolos de comunicaciones entre las dos redes interconectadas en todas las capas del modelo OSI. Los diodos PSTdiode están formadas por dos *appliances*, uno que se conecta al domino origen y otro al dominio destino. Cada *appliance* dispone de la parte correspondiente del hardware de comunicación unidireccional PSTdiode ATKDDL® y del software necesario instalado (firmware).
    b) Filtrado de contenidos. Las diodos permiten el paso de información siempre que cumplan las reglas de filtrado definidas.

1.1 Casos de uso

5. El diseño de PSTdiode es adecuado para todos los usos en los que haya necesidad de transmisión de información en un único sentido, con garantía física de que la transmisión es unidireccional. De manera genérica son de aplicación a los siguientes escenarios:
    a) **Confidencialidad de redes aisladas.** Entrada de información en una red aislada, en la que se quiera garantizar la confidencialidad de sus recursos y datos.
    b) **Integridad y disponibilidad de redes de control industrial**. Salida de información de una instalación de control industrial aislada, en la que se quiera garantizar la integridad y disponibilidad de sus recursos y datos.

2. Objeto y alcance

6. Los diodos de datos PSTdiode soportan diferentes servicios de flujo de datos. Los servicios son completamente independientes unos de otros.
7. En la presente guía se recoge el procedimiento de empleo seguro para los siguientes servicios:
    a) DIF – Servicio entrada de ficheros (Diodo)
    b) DIUP – Servicio entrada de UDP (Diodo)
8. 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

9. El capítulo 3 contiene una visión general de la arquitectura de PSTdiode.
10. 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 (explotación)** (capítulo 6).
11. 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.
12. En el ANEXO A se incluye una lista de comprobación que puede ser usada de referencia.

3. Arquitectura de los diodos PSTdiode

3.1 Componentes

13. PSTdiode está formado por dos *appliances* cada uno de ellos conectado a un dominio de seguridad:
    a) El appliance origen PSTs (negro) se conecta al dominio de origen.
    b) El appliance destino PSTd (blanco) se conecta al dominio de destino.

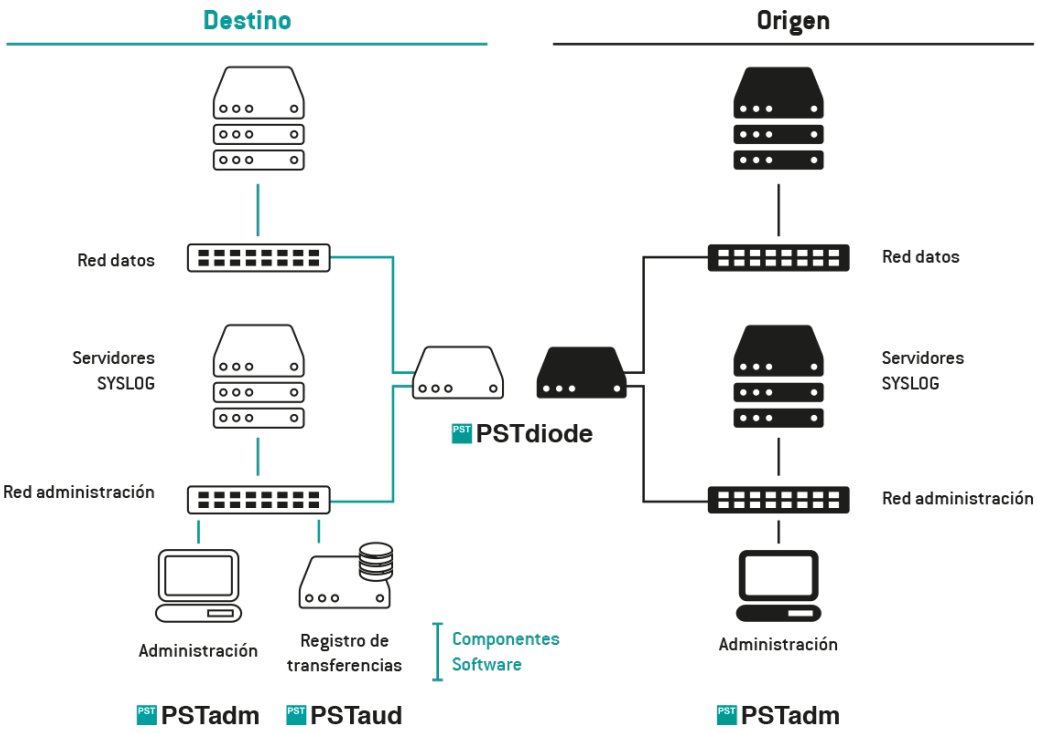

Figura 1 Componentes PSTdiode

14. También forman parte del sistema dos componentes software: la consola de administración (PSTadm) y el servicio de auditoría (PSTaud) que permite almacenar externamente la información de las transferencias de información que se han realizado a través del dispositivo.

15. 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

16. Además de los *appliances* que componen el diodo, es necesario disponer de una infraestructura de administración, en cada uno de los dominios de seguridad.

17. En el dominio de origen 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. Desde estos equipos se realiza la administración del *appliance* origen (PSTs).

b) **Servidores de SYSLOG:** Uno o dos servidores de SYSLOG. El *appliance* origen (PSTs) tiene capacidad de enviar eventos de funcionamiento y de seguridad a servidores distintos. Estos eventos son referentes al propio *appliance.*

18. En el dominio de destino 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. Desde estos equipos se realiza la administración del *appliance* destino (PSTd) y la monitorización del sistema completo.

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. El *appliance* destino (PSTd) tiene capacidad de enviar eventos de funcionamiento y de seguridad a servidores distintos. Estos eventos son referentes al sistema completo.

3.3 Esquema de despliegue

19. El despliegue del diodo se llevará a cabo en los siguientes pasos:

a) Instalación física de los *appliances*.

b) Configuración local mínima del *appliance* origen (PSTs).

c) Configuración local mínima del *appliance* destino (PSTd).

d) Instalación del software adicional en el dominio origen (PSTAdm).

e) Instalación del software adicional en el dominio destino (PSTAdm y PSTAud).

f) Configuración remota desde dominio origen:

i. Alta de administradores.

ii. Configuración de la infraestructura.

iii. Configuración de los servicios de flujo de datos.

g) Configuración remota desde dominio destino:

i. Alta de administradores.

ii. Configuración de la infraestructura.

iii. Configuración de los servicios de flujo de datos.

h) Puesta en servicio.

3.4 Entorno

20. Los diodos PSTdiode trabajan por encima del nivel de aplicación. Están pensados para ser el único punto de intercambio de información (en un único sentido) entre los dos dominios que separan y no permitir la transferencia de paquetes ni de conexiones entre ellos.
21. Los diodos se consideran dispositivos de protección de perímetro de sentido único 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.
22. No obstante, excede del ámbito de esta guía el prescribir una determinada topología.

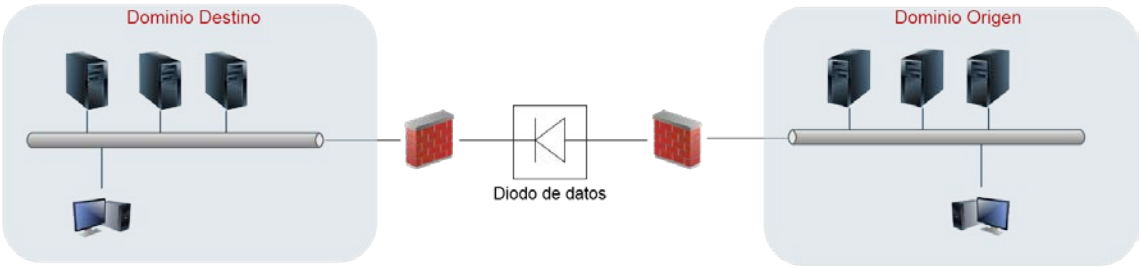

Figura 2 Ejemplo de arquitectura de protección de perímetro (Diodo en DMZ)

3.5 Configuración de cortafuegos

23. La configuración de los cortafuegos deberá permitir exclusivamente el tráfico necesario para el funcionamiento del diodo. 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 [DIG].
    b) La parte correspondiente a cada servicio de flujo de datos, descrita en un anexo 'Características del tráfico de red' del manual de operación de cada servicio [OG-DIF] y [OG-DIUDP].

4. Fase de planificación

24. Las consideraciones contenidas en este apartado deberán tenerse en cuenta durante una fase temprana del proyecto de implantación del diodo. Básicamente, se incluyen aspectos relacionados con:

a) Seguridad física.

b) Flujos de datos.

c) Topología de red.

d) Infraestructuras de administración.

e) Infraestructuras de clave pública (PKI).

f) Administradores.

4.1 Seguridad física

25. **Entorno controlado**: los *appliances* del diodo 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

26. **Mínimos flujos de datos**: Los diodos desplegados deberán disponer únicamente de licencias de los servicios que vayan a utilizar.
27. **Protocolos seguros**: Para las comunicaciones del servicio de entrada de ficheros del diodo (DIF) con los servidores de ficheros en ambos dominios de seguridad 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.

4.3 Topología de red

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

4.4 Infraestructura de administración

30. **Consola de administración PSTadm:** La consola de administración de los *appliances* (PSTadm) deberá instalarse exclusivamente en los equipos de administración necesarios.
31. **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.

32. **Servidores de SYSLOG:** Deberá disponerse de uno o dos servidores de SYSLOG en cada dominio de seguridad para recibir los eventos de funcionamiento y seguridad. Es recomendable integrar los eventos en el sistema de monitorización de la organización.
33. En el caso de que el diodo se vaya a emplear en sistemas clasificados, los servidores anteriormente indicados deberán estar acreditados.

4.5 Infraestructura de clave pública (PKI)

34. Deberá disponerse de una infraestructura de clave pública en cada uno de los dominios de seguridad 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 los *appliances* del sistema.
35. ***Common Name* únicos:** Los diodos PSTdiode 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 en cada uno de los dominios de seguridad.
36. **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.
37. **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. Estos requisitos serán igualmente válidos para sistemas clasificados.

4.6 Administradores

38. 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 diodos PSTdiode. En la configuración local de cada *appliance*, serán los responsables de dar de alta los certificados de los administradores raíz. A partir de aquí, cada *appliance* se encargará de verificar la identidad y autenticar a los administradores en cada uno de los dominios. Los administradores raíz, dan de alta al resto de perfiles de administración.

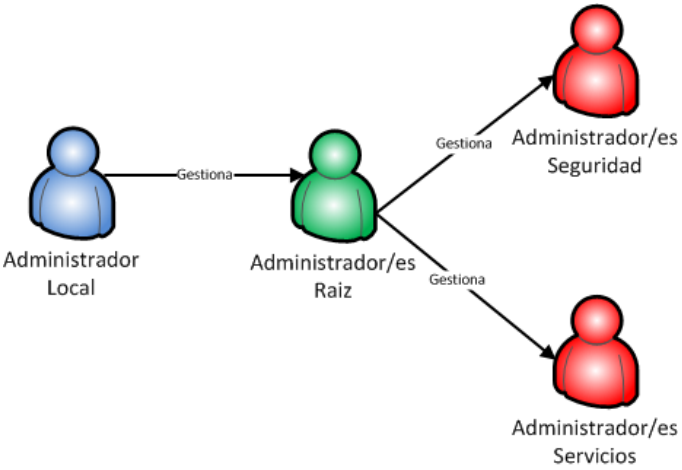

Figura 3 Jerarquía de perfiles de administración

39. **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

40. **Comprobaciones de integridad:** en la recepción de los equipos se deberá 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 PSTdiode. 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' [DIG].*

41. **Entorno controlado:** la instalación de los *appliances* del diodo se deberá realizar en un entorno físicamente controlado.

5.2 Infraestructuras de administración

42. **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).
43. **Longitud mínima de claves de certificados:** Deberán utilizarse claves de longitud igual o superior a las indicadas en el párrafo 37.
44. **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' [DIG].

45. **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

46. El administrador local tiene como única función realizar la configuración local de cada *appliance*.

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

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

5.3.2. Administrador raíz

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

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

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

5.3.3. Administrador de seguridad

55. El administrador de seguridad tiene como principal función realizar la configuración del entorno del diodo.

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

56. **Configuración de servidores de SYSLOG.** Se deberá incluir en la configuración de cada *appliance* las direcciones de los servidores de SYSLOG de su dominio.
57. **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 en cada uno de los *appliances*.
58. **Configuración del servidor de registro de transferencias.** Se deberá incluir en la configuración del *appliance* del dominio destino las direcciones del servidor de registro de transferencias.

5.3.4. Administrador de servicios

59. 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].*

60. **Configuración de servidores por IP**. Se deberán utilizar direcciones IP en lugar de nombres de dominio en la especificación de servidores.
61. **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.

62. **Configuración de auditoría.** Se deberá activar el registro de información de transferencias de todos los servicios.
63. **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 ficheros (diodo) - DIF

La información de configuración del servicio se describe en el manual de operación del servicio entrada de ficheros (Diodo) [OG - DIF].

64. **Protocolos seguros.** Se deberán utilizar los protocolos FTPS ó SFTP en ambos dominios.
65. **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.

5.4.2. Servicio entrada de UDP (diodo) - DIUDP

La información de configuración del servicio se describe en el manual de operación del servicio entrada de UDP (Diodo) [OG - DIUDP].

66. **Filtrado por IP de origen.** Se deberá establecer el filtro de 'IP origen' en la configuración de cada uno de los canales del *appliance* origen (PSTs).
67. **Filtrado por tamaño de *payload*.** Se deberá establecer el filtro de tamaño máximo y mínimo, de forma que se ajuste al tamaño de los payloads a transferir, en la configuración de cada uno de los canales del *appliance* origen (PSTs).
68. **Filtrado de contenido.** Se deberá establecer filtro de contenido, si el tráfico UDP se ajusta a los filtros de contenido disponibles, en la configuración de cada uno de los canales del *appliance* destino (PSTd).
69. **Fijar puerto de origen.** Se recomienda fijar el puerto de origen de los paquetes en el dominio destino, en la configuración de cada uno de los canales del *appliance* destino (PSTd)

6. Fase de explotación

70. 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

71. Estas tareas se podrían incorporar al plan de mantenimiento. Se recomienda registrar las acciones realizadas y las fechas de caducidad de los certificados.

72. El administrador local deberá:

    a) **Realizar controles de integridad periódicos** de los *appliances* del diodo. 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

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

6.3 Administrador de seguridad

74. El administrador de seguridad deberá:

    a) **Monitorizar los eventos de seguridad generados por el *appliance*.**

    b) **Monitorizar el registro de información de transferencias realizadas por el *appliance* destino (PSTd).**

6.4 Administrador de servicios

75. **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 en cada.

7. Referencias

DIG	PSTdiode - Manual de instalación y puesta en servicio (550-17)
OG	Dispositivos de protección de perímetro PST - Manual de operación (550-2)
OG-DIF	PSTdiode – Manual de operación DIF. Servicio entrada de ficheros (Diodo) (550-20)
OG-DIUDP	PSTdiode – Manual de operación DIUDP. Servicio entrada de UDP (Diodo) (550-19)
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

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*
OSI	*Open System Interconnection*
RSA	*Rivest, Shamir y Adleman*
SFTP	*SSH File Transfer Protocol*
SHA	*Secure Hash Algorithm*
STIC	*Seguridad de las Tecnologías de la Información y la Comunicación*
TLS	*Transport Layer Security*
UDP	*User Datagram Protocol*

ANEXO A. LISTA DE COMPROBACIONES

76. Las listas de comprobaciones de este anexo permiten realizar un control sobre el nivel de implantación de las medidas de seguridad en la fase de despliegue e instalación del diodo PSTdiode.
77. Las comprobaciones se dividen en:
    - **a)** Seguridad física
    - **b)** Dominio origen
    - **c)** Dominio destino

1. ***Nota:*** Las medidas con carácter recomendado se encuentra marcadas con un asterisco (*).

1. SEGURIDAD FÍSICA

78. La siguiente lista detalla las comprobaciones a realizar sobre la seguridad física del diodo PSTdiode.

	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

2. DOMINIO ORIGEN

79. La siguiente lista detalla las comprobaciones a realizar sobre el entorno y la configuración del *appliance* origen (PSTs) en el dominio origen.

	MEDIDAS DE SEGURIDAD	
Infraestructuras 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 el *appliance*
	☐	Configuración de la interfaces 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
Administrador de servicios / **Servicio de entrada de ficheros (Diodo) - DIF**	☐	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
Servicio de entrada de UDP (Diodo) - DIUDP	☐	Filtrado de datos
	☐	Filtrado por IP de origen
	☐	Filtrado por tamaño de *payload*

3. DOMINIO DESTINO

80. La siguiente lista detalla las comprobaciones a realizar sobre el entorno y la configuración del *appliance* destino (PSTd) en el dominio destino.

		MEDIDAS DE SEGURIDAD	
Infraestructuras 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 el *appliance*
		☐	Configuración de la interfaces 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 ficheros (Diodo) - DIF	☐	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
	Servicio de entrada de UDP (Diodo) - DIUDP	☐	Configuración de servidores por IP
		☐	Filtrado de datos
		☐	Filtrado de contenido

		☐	Configuración de auditoría
		☐	Fijar puerto de origen (*)