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

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo D.6: Pasarelas para intercambio de datos

Noviembre 2017

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
2017.11.27 11:24:18 +01'00'

NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017
ISDEFE ha participado en el desarrollo del presente documento.

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Pasarelas de intercambio de datos** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el CCN.
2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado desde el punto de vista de la seguridad para ser empleado en los sistemas de información del sector público a las que sea de aplicación el Esquema Nacional de Seguridad (ENS). Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.
3. Además, la aplicación de estos criterios permitirá:
   - Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
   - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
   - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.
4. Por lo tanto, los productos catalogados dentro de la familia **Pasarelas de intercambio de datos** conforme a la taxonomía definida por el Centro Criptológico Nacional, serán susceptibles de ser evaluados usando como referencia este documento.
5. En el caso de productos multipropósito, queda fuera del alcance de este documento cualquier otra funcionalidad de seguridad proporcionada, más allá de la especificada para esta familia en la sección siguiente. Dichos productos podrían optar a ser incluidos de manera adicional como Productos Cualificados en otra(s) familia(s) del CPSTIC si cumpliesen los RFS correspondientes.

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

2.1 FUNCIONALIDAD

6. Los productos asociados a la familia Pasarelas de intercambio de datos están orientados a la protección de interconexiones, fundamentalmente para la separación de redes que manejan información con diferentes categorías o políticas de seguridad, con el fin de evitar la entrada o salida de información no autorizada.
7. Para ello proporcionan las siguientes funciones básicas de seguridad:
   - Separación de redes. Ruptura de la continuidad de los protocolos de comunicaciones entre dos redes interconectadas en todas las capas del modelo OSI[1]. Así, las pasarelas suelen estar formadas por dos unidades, una que se conecta a la red interna (la que se 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***, que impide que utilicen simultáneamente los mismos recursos. De esta forma se asegura que nunca se establece una conexión TCP[2]/IP[3] 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.
   - Filtrado de contenidos. Las pasarelas analizan el contenido del paquete y permiten el paso de información siempre que cumpla las reglas de filtrado definidas, tanto para la entrada como para la salida.
8. Suelen desarrollarse para prestar un servicio concreto, como intercambio de ficheros o correo electrónico.
9. Las pasarelas son especialmente útiles para implementar mecanismos de defensa en profundidad y neutralizar o minimizar el efecto de las APT[4], al no permitir la fuga de información sensible desde la red interna.

2.2 CASOS DE USO

10. En el caso de las pasarelas tan sólo se contempla un caso de uso, aunque los canales o políticas de intercambio de datos con los que se configuran pueden variar, incluyendo los servicios, procedimientos y protocolos con los que trabajan.

[1] *Open System Interconnection*
[2] *Transmission Control Protocol*
[3] *Internet Protocol*
[4] *Advanced Permanent* Th*reat.* Amenazas persistentes avanzadas

2.2.1. CASO DE USO 1 - SEGMENTACIÓN DE REDES

11. Estos dispositivos se utilizan para posibilitar la interconexión entre dos sistemas en red, el sistema al que deseamos proteger estará localizado en una red que denominaremos “red interna”, mientras que el sistema al que se desea conectar se encontrará situado en una red que denominaremos “red externa”.
12. Lo habitual es que la red interna esté aislada y tenga requisitos de protección de la información contenida mayores, mientras que la red externa cuenta con una categoría de seguridad más baja (p.ej.: una red corporativa).
13. El dispositivo que conecta ambas redes actúa como punto de unión entre ellas y asegura internamente la protección de los flujos de información conforme a su configuración.
14. Las tareas de administración y configuración del dispositivo deben llevarse a cabo desde la red interna (la más protegida) para evitar flujos de información externos más allá de los servicios prestados por el dispositivo.

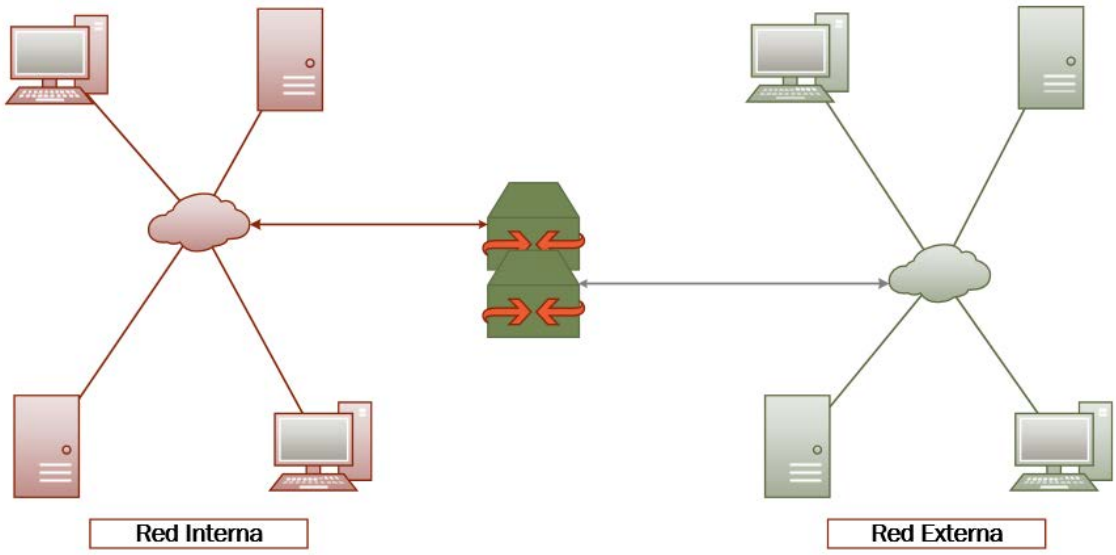

Figura 1 – Ejemplo de Caso de Uso: Segmentación de Redes

2.3 ENTORNO DE USO

15. Por lo general, este tipo de dispositivos se encuentran en grandes o medianas empresas, así como en redes del sector público, formando parte de una arquitectura de defensa en profundidad, en combinación con medidas complementarias en diferentes capas de protección.
16. Para la utilización en condiciones óptimas de seguridad de las pasarelas de intercambio de datos, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

- **Protección física**: El producto deberá instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.
- **Aislamiento de red**: La red interna no deberá disponer de otras interfaces con la red externa que permitan evadir el control de los flujos de información a través de la pasarela.
- **Administración confiable**: El Administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Por ello se asume que dicha persona estará altamente capacitada, formada y carecerá de cualquier intención dañina al administrar el producto.
- **Actualizaciones periódicas**: El firmware y el software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **Protección de las credenciales**: Todas las credenciales, en especial la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.
- **Política de seguridad de la información**: Una política de seguridad deberá recoger el conjunto de principios, organización y procedimientos impuestos por una organización para hacer frente a sus necesidades de seguridad de la información, incluyendo el uso de las TIC.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

17. Este tipo de productos se presentan en formato **Equipo dedicado o (*Appliance*:** hardware provisto de firmware[5] dedicado) con las funcionalidades estrictamente necesarias para cumplir su finalidad y acotadas al servicio específico que presten.
18. Adicionalmente, puede ser habitual que incluyan un **Software** instalable en un equipo informático estándar que sirva para realizar las funciones de control y administración del dispositivo.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

19. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TI (Tecnologías de la Información).
20. En el ámbito de CC se elaboran unos perfiles de seguridad que definen, para un dominio o categoría de productos, un conjunto de objetivos y requisitos de

[5] *Firmware* funciona como el nexo de unión entre las instrucciones (software) que llegan al dispositivo desde el exterior y las diversas partes electrónicas (hardware)

seguridad, tanto funcionales como de evaluación, independientes de la implantación.

21. Los productos dentro de esta familia deberán cumplir con los requisitos Fundamentales de Seguridad reflejados en el apartado 4 y con los SFR (*SecurityFunctional Requirements*) que se especifican en alguno de los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria:*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Devices.[6]	1.0	27/02/2015	CCDB
Protection Profile for Network Devices.[7]	1.1	08/06/2012	NIAP

Tabla 1. Perfiles de protección

22. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será:

- **El determinado por el perfil de protección** para aquellos SFR incluidos en los perfiles exigidos cuando los productos se encuentren certificados contra alguno de los perfiles anteriormente descritos.
- **EAL2 o superior** para los RFS adicionales que no encuentren incluidos dentro de un perfil.
- **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra ningún perfil.

[6] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf
[7] https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V1.1.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

23. Los recursos que es necesario proteger mediante el uso de esta familia de productos incluyen:

- Dispositivos de red y subredes asociadas a la interfaz interna a la que se conecta el producto.
- Toda la información que tenga que hacer uso del producto para ser transmitida.
- Datos de configuración del producto y de auditoría generados por éste.
- Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

24. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente serían:

- **Divulgación de información no autorizada:** Un atacante, desde dentro o desde fuera de la red, consigue enviar información no autorizada de la red interna al exterior a través del dispositivo (p.ej.: divulgar información protegida o configuraciones de red de la red interna).
- **Acceso no autorizado**: Un atacante, desde dentro o desde fuera de la red, consigue acceder a información intercambiada a través del dispositivo para la que no estaba autorizado (p.ej.: recibir información transmitida a través de la pasarela, pero no destinada a él) o utilizar el dispositivo como mecanismo de acceso a la red interna aislada.
- **Envío de tráfico dañino**: Un atacante, desde o desde fuera de la red, consigue enviar información no autorizada desde el exterior a la red interna a través del dispositivo (p.ej.: introducir información maliciosa de manera encubierta proveniente de la red externa).
- **Canales de comunicación no seguros.** Un atacante podría aprovecharse de la utilización de canales de comunicación inseguros para desarrollar ataques *man in the middle* o de replicación, que pudieran suponer una pérdida de confidencialidad e integridad de los datos y comprometer el dispositivo.
- **Compromiso de la funcionalidad del dispositivo**: Un atacante o un fallo en el dispositivo compromete la funcionalidad de seguridad de este, permitiendo modificarla o desactivarla de manera no conforme a las políticas de seguridad (p.ej. instalación de actualizaciones dañinas o administración no autorizada del dispositivo).

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

25. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC en esta familia.

4.1 PERFIL DE PROTECCIÓN

26. **REQ. 1.** Los productos deberán estar certificados con uno de los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria:*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Devices.[8]	1.0	27/02/2015	CCDB
Protection Profile for Network Devices.[9]	1.1	08/06/2012	NIAP

Tabla 2. Perfiles de protección

27. **REQ. 2.** En caso de que el producto no esté certificado contra ningún perfil de los anteriores, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) del perfil *Collaborative Protection Profile for Network Devices. Version 1.0*con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior.**

4.2 CONTROL DE LOS FLUJOS DE INFORMACIÓN

28. **REQ. 3.** El producto debe tener la capacidad de conectarse a dos interfaces de red físicos entre los que debe transmitir la información.
29. **REQ. 4.** Los protocolos de comunicación disponibles serán los estrictamente necesarios para implementar el servicio específico al que se oriente el producto.
30. **REQ. 5.** El producto asociará políticas de seguridad o restricciones aplicadas a los flujos de información a los canales de comunicación establecidos entre la red interna y la red externa (p.ej.: mecanismos de autorización de la información a transmitir o volumen máximo de datos admitidos).
31. **REQ. 6.** El producto no permitirá ningún flujo de información ni de entrada ni de salida que no se encuentre autorizado en las políticas de seguridad definidas.
32. **REQ. 7.** La configuración de los canales de comunicación debe poderse activar o desactivar. Por defecto, el estado de un canal debe ser desactivado.

[8] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf
[9] https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V1.1.pdf

33. **REQ. 8.** La definición, configuración, modificación o eliminación de canales para la transmisión o recepción de información debe ser llevada a cabo o autorizada por un perfil de usuario responsable del canal con los permisos específicos para ello (p.ej.: perfil de administración).
34. **REQ. 9.** El producto sólo utilizará los recursos estrictamente asociados a los servicios para los que se orienta y a los canales configurados para la transmisión de la información.
35. **REQ. 10.** El producto no permitirá los flujos de información entre ambas interfaces que no se ajusten a alguno de los canales configurados disponibles (teniendo en cuenta los recursos, políticas y restricciones asociados).
36. **REQ. 11.** El producto debe asegurar que cuando un canal se utiliza para la transmisión de información no podrá ser utilizado, al menos simultáneamente, para su recepción, evitando el uso compartido de los recursos del canal.
37. **REQ. 12.** Los canales y protocolos de comunicación implementados deben permitir la configuración de parámetros de seguridad (p.ej.: características de la cifra en protocolos seguros) así como de otros parámetros necesarios para un correcto establecimiento de la comunicación entre ambos extremos.
38. **REQ. 13.** El producto debe filtrar y evitar el uso de campos no aplicables, irrelevantes o innecesarios del protocolo de comunicación, que pudieran permitir la ocultación y transmisión encubierta de información no autorizada relativa a la configuración de la red interna.
39. **REQ. 14.** El producto debe asegurar la integridad y confidencialidad de los datos que maneja cuando estos se transmitan entre cada una de las partes que lo constituyen.

4.3 AUDITORÍA Y REGISTROS DE SEGURIDAD

40. **REQ. 15.** La gestión de los registros sólo podrá ser realizada por un perfil de usuario privilegiado (p.ej.: rol de auditor).
41. **REQ. 16.** El producto debe proporcionar una forma de acceso legible a los registros de auditoría para facilitar su revisión a los usuarios autorizados.
42. **REQ. 17.** El producto debe permitir realizar una copia de seguridad de los registros de auditoría, mediante dispositivos extraíbles autorizados o a través de su interfaz con la red interna.
43. **REQ. 18.** El producto deberá utilizar IPsec[10], TLS[11] o TLS/HTTPS[12] para establecer un canal de comunicaciones seguro entre él y las entidades autorizadas que provean servicios remotos de auditoría.

[10] *Internet Protocol Security*
[11] *Transport Layer Security*
[12] *Hypertext Transfer Protocol Secure*

4.4 CONTROL DE ACCESOS, AUTENTICACIÓN Y PRIVILEGIOS

44. **REQ. 19.** La gestión de usuarios, incluyendo su creación y asignación de privilegios, así como la baja o supresión de aquellos, sólo podrá ser realizada por un perfil de usuario privilegiado (p.ej.: rol de administrador).

45. **REQ. 20.** Un usuario requerirá un proceso de autenticación positivo antes de realizar ningún tipo de acción en la pasarela.

4.5 ADMINISTRACIÓN DEL PRODUCTO

46. **REQ. 21.** La administración del producto sólo podrá ser realizada por un perfil de usuario privilegiado (p.ej.: rol de administrador de seguridad).

47. **REQ. 22.** El producto deberá distinguir lógicamente entre entrada de datos y de administración, y salida de datos y administración.

48. **REQ. 23.** La administración remota sólo podrá ser realizada a través de la interfaz conectada con la red interna.

49. **REQ. 24.** El producto deberá utilizar IPsec, TLS o TLS/HTTPS para establecer un canal de comunicaciones seguro entre él y las entidades autorizadas de administración remota.

4.6 PROTECCIÓN DEL DISPOSITIVO Y SUS SERVICIOS

50. **REQ. 25.** El producto debe ser capaz de detectar y reaccionar ante un acceso indiscriminado al servicio para evitar posibles denegaciones de servicio, a través de ambas interfaces.

51. **REQ. 26.** En caso de fallo de algún componente, el producto debe asegurar una adecuada funcionalidad y que no se incumplen las políticas de seguridad permitiendo flujos de información no autorizados.

52. **REQ. 27.** El producto debe permitir realizar una copia de seguridad de su configuración mediante dispositivos extraíbles autorizados o a través de su interfaz con la red interna.

53. **REQ. 28.** El producto debe permitir restablecer su configuración a partir de una copia de seguridad, mediante los mismos mecanismos usados para la realización de las copias de seguridad.

54. **REQ. 29.** El producto deberá implementar:

    a) Auto chequeos de arranque, donde se verifique la integridad del software o firmware y de funciones críticas, si procede.

    b) Auto chequeos condicionales, donde se verifique la integridad y autenticidad del software o firmware durante su carga.

55. **REQ. 30.** El producto deberá tener la capacidad de verificar las actualizaciones del software/firmware utilizando firma digital con anterioridad a

la instalación de estas actualizaciones. Solo permitirá la actualización en el caso de que la verificación de la firma haya sido correcta.

4.7 REQUISITOS CRIPTOGRÁFICOS

56. **REQ. 31.** Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse dentro de los acreditados por el CCN para su uso en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807 Criptología de empleo en el ENS (Categoría ALTA).

5. ABREVIATURAS

APT	*Advanced Permanent Threat*
CC	*Common Criteria*
CCDB	*Common Criteria Development Board*
CCN	*Centro Criptológico Nacional*
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones*
EAL	*Evaluation Assurance Level*
ENS	*Esquema Nacional de Seguridad*
HTTPS	*Hypertext Transfer Protocol Secure*
IP	*Internet Protocol*
IPSec	*Internet Protocol Security*
NIAP	*National Information Assurance Partnership*
OSI	*Open System Interconnection*
RFS	*Requisitos Fundamentales de Seguridad*
TCP	*Transmission Control Protocol*
TLS	*Transport Layer Security*