centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo D7: Diodos de datos

Febrero 2019

MINISTERIO DE DEFENSA

Edita:

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
2019.02.27 09:32:15 +01'00'

NIPO: 083-19-053-9.

Fecha de Edición: febrero 2019

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN Y OBJETO 4
2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS 5
2.1 FUNCIONALIDAD 5
2.2 CASOS DE USO 5
2.2.1. CASO DE USO 1 - ENTRADA DE INFORMACIÓN A RED INTERNA 5
2.2.2. CASO DE USO 2 – SALIDA DE INFORMACIÓN DESDE RED INTERNA 6
2.3 ENTORNO DE USO 7
2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO 7
2.5 ALINEAMIENTO CON COMMON CRITERIA 7
3. ANÁLISIS DE AMENAZAS 8
3.1 ACTIVOS 8
3.2 AMENAZAS 8
4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS) 8
4.1 AUDITORÍA Y REGISTROS DE SEGURIDAD 8
4.2 CONTROL DE ACCESOS, AUTENTICACIÓN Y PRIVILEGIOS 9
4.3 ADMINISTRACIÓN DEL PRODUCTO 9
4.4 PROTECCIÓN DEL DISPOSITIVO Y SUS SERVICIOS 10
4.5 CONTROL DE LOS FLUJOS DE INFORMACIÓN 10
4.6 REQUISITOS CRIPTOGRÁFICOS 10
5. ABREVIATURAS 12

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia de **Diodos 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 de **Diodos 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 Diodos de Datos son dispositivos de protección de perímetro utilizados habitualmente en interconexiones entre sistemas con diferentes categorías o políticas de seguridad. Su funcionalidad principal es la de separar redes, permitiendo el flujo de información en un único sentido y haciendo inviable la transmisión de información en el sentido opuesto.
7. Para ello, proporcionan las siguientes funciones básicas de seguridad:
    a) Transmisión del tráfico de red de manera unidireccional, para lo que se deberá elegir si se desea que el sentido de la comunicación sea de entrada hacia, o salida desde, la red interna.
    b) Capacidad de interpretar protocolos bidireccionales, "romperlos" y convertirlos en unidireccionales para luego presentarlos en la segunda red de nuevo como bidireccionales.
8. La protección tiene lugar a diferentes niveles dentro de las capas definidas por el modelo OSI (*Open Systems Interconnection*), fundamentalmente a nivel de capa física limitando el flujo de información en el sentido autorizado y haciendo inviable la transmisión de señales de comunicación en el opuesto, pero también a nivel de las capas de red, transporte y/o aplicación para habilitar el uso de protocolos bidireccionales.

2.2 CASOS DE USO

9. En el caso de los Diodos de Datos se contemplan dos casos de uso, que permiten aprovechar de manera diferente las características del producto, según se permita el flujo hacia o desde la red que se desea proteger.

2.2.1. CASO DE USO 1 - ENTRADA DE INFORMACIÓN A RED INTERNA

10. Se cuenta con dos redes separadas mediante un diodo de datos. Una de las redes es la que se desea proteger (debido a que maneja información sensible o unas políticas de seguridad más restrictivas) mientras que la otra es una red con un nivel de confianza inferior.
11. El diodo de datos en este caso está implementado y configurado para permitir únicamente el flujo de información desde la red externa hacia la red interna y evitar cualquier comunicación en sentido opuesto que posibilite la fuga de información.
12. En este caso los componentes que dan soporte a la transmisión quedan ubicados en la red externa y los de recepción en la red interna, conectados al respectivo extremo del diodo físico.
13. Este tipo de caso de uso es típico de infraestructuras en las que se maneja información cuyos requisitos de confidencialidad son elevados, por lo que se

requiere impedir los flujos de información que permitan filtrar la información, pero que al mismo tiempo requieren procesar información proveniente del exterior como parte de su misión.

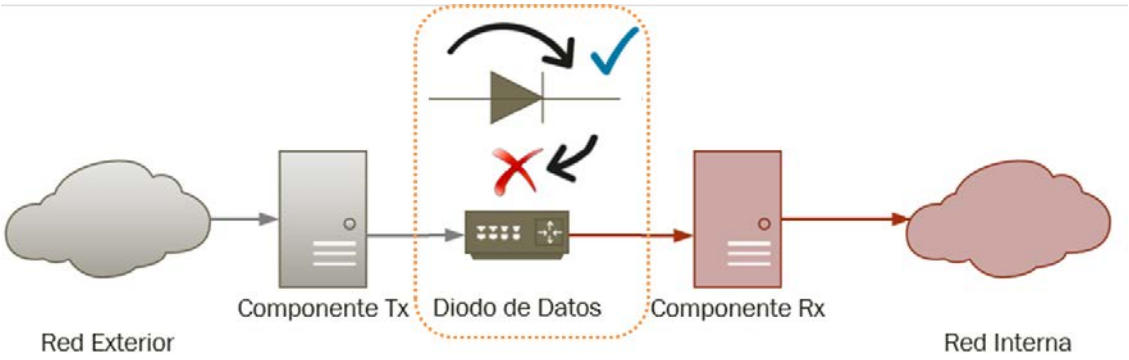

Figura 1 – Ejemplo de Caso de Uso 1: Entrada de Información a Red Interna

2.2.2. CASO DE USO 2 – SALIDA DE INFORMACIÓN DESDE RED INTERNA

14. Se cuenta con dos redes separadas mediante un diodo de datos. Una de las redes es la que se desea proteger (debido a que maneja información sensible o unas políticas de seguridad más restrictivas) mientras que la otra es una red con un nivel de confianza inferior.
15. El diodo de datos está implementado y configurado para permitir únicamente el flujo de información desde la red interna hacia la red externa (conforme a las políticas que defina e implemente el organismo que despliegue el producto) y evitar cualquier comunicación en sentido opuesto que posibilite introducir información desde la red externa hacia la red interna.
16. En este caso, los componentes que dan soporte a la transmisión y recepción estarían en la red interna y en la red externa respectivamente, conectados al extremo del diodo físico correspondiente. Su uso es típico de infraestructuras en las que es necesario reportar hacia el exterior datos de los sistemas, manteniendo el aislamiento de la red interna frente a riesgos externos.

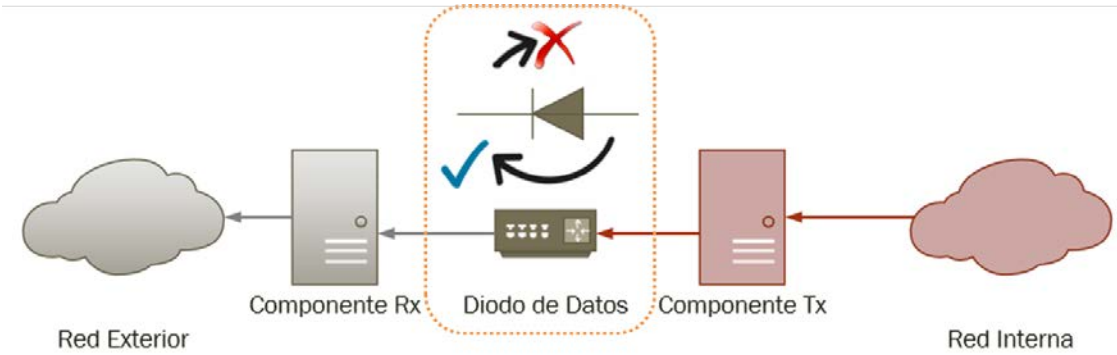

Figura 2 – Ejemplo de Caso de Uso 2: Salida de Información desde Red Interna

2.3 ENTORNO DE USO

17. Por lo general, este tipo de dispositivos se encuentran en grandes o medianas empresas, así como en redes de las Administraciones Públicas, como parte de una arquitectura de defensa en profundidad, en combinación con medidas complementarias en diferentes capas de protección.

18. Para la utilización en condiciones óptimas de seguridad de los Diodos de datos, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    a) **Protección física:** El producto deberá instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones de seguridad física adecuadas.

    b) **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 del diodo.

    c) **Administración confiable:** El usuario 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 y carecerá de cualquier intención maliciosa al administrar los diodos de datos.

    d) **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.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

19. Este tipo de productos se presentan en formato *Appliance* (hardware provisto de firmware dedicado) con las funcionalidades estrictamente necesarias para cumplir su finalidad y acotadas al servicio específico que presten.

20. Adicionalmente, puede ser habitual que incluyan un Software instalable en equipos informáticos estándar que sirva para realizar las funciones de administración del dispositivo o auditoría.

2.5 ALINEAMIENTO CON COMMON CRITERIA

21. No se utilizará ningún perfil de protección *Common Criteria* de referencia para esta familia de productos.

22. El nivel de confianza EAL (*Evaluation Assurance Level*) conforme a CC, al que deben ser evaluados los Requisitos Fundamentales de Seguridad descritos en este documento debería ser EAL 2 o superior.

3. ANÁLISIS DE AMENAZAS

3.1 ACTIVOS

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

    a) Dispositivos de red asociados a la interfaz del producto a que se conecta la red interna, incluyendo la información que manejan.

    b) Toda la información que tenga que hacer uso del producto para ser transmitida.

    c) Datos de configuración del producto y de auditoría generados por éste.

    d) Actualizaciones del dispositivo.

3.2 AMENAZAS

24. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente, atendiendo a los casos de uso expuestos, serían:

    a) Divulgación de información no autorizada (caso de uso 1): Un atacante consigue enviar información no autorizada de la red interna a la externa a través del dispositivo (p.ej.: información confidencial o configuraciones de red de la red interna).

    b) Acceso no autorizado: Un atacante, desde dentro de la red o desde fuera, consigue acceder al dispositivo y a los datos contenidos en este.

    c) Actualizaciones / modificaciones no autorizadas. Un atacante consigue realizar una actualización/modificación del producto que comprometa sus funcionalidades de seguridad instalando software o firmware que lo permitan o que contengan código dañino.

    d) Envío de tráfico malicioso (caso de uso 2): Un atacante, desde fuera de la red, consigue introducir información no autorizada en la red interna a través del dispositivo (p.ej.: código malicioso).

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 AUDITORÍA Y REGISTROS DE SEGURIDAD

26. **REQ. 1.** La gestión de los registros sólo podrá ser realizada por un perfil de usuario privilegiado (p.ej.: rol de auditor).

27. **REQ. 2.** Los registros de auditoría contendrán al menos la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento (si aplica).
28. **REQ. 3.** Como mínimo, se registrarán en la auditoria los siguientes eventos:
    a) Iniciar o detener la auditoria de la aplicación
    b) Cambios en los permisos de usuarios.
    c) Utilización por parte del usuario de los mecanismos de autenticación.
    d) Cualquier utilización de los mecanismos de autenticación del producto.
    e) Todas las decisiones en cuanto a las peticiones en el intercambio de información entre la red interna y externa.
    f) Cambio de hora o fecha.
    g) Cambios de la configuración del producto.
29. **REQ. 4.** 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.
30. **REQ. 5.** El producto deberá utilizar IPsec[1], TLS[2] o TLS/HTTPS[3] para establecer un canal de comunicaciones seguro entre él y las entidades autorizadas que provean servicios remotos de auditoría.

4.2 CONTROL DE ACCESOS, AUTENTICACIÓN Y PRIVILEGIOS

31. **REQ. 6.** 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).
32. **REQ. 7.** Un usuario requerirá un proceso de identificación y autenticación positivo antes de realizar ningún tipo de acción en el diodo.

4.3 ADMINISTRACIÓN DEL PRODUCTO

33. **REQ. 8.** La administración del producto sólo podrá ser realizada por un perfil de usuario privilegiado (p.ej.: rol de administrador de seguridad).
34. **REQ. 9.** El producto deberá distinguir lógicamente entre entrada de datos y de administración, y salida de datos y administración.
35. **REQ. 10.** La administración remota sólo podrá ser realizada a través de la interfaz conectada con la red interna.

[1] *Internet Protocol Security*
[2] *Transport Layer Security*
[3] *Hypertext Transfer Protocol Secure*

36. **REQ. 11.** 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.

4.4 PROTECCIÓN DEL DISPOSITIVO Y SUS SERVICIOS

37. **REQ. 12.** En caso de fallo de algún componente, el producto debe asegurar una adecuada funcionalidad y que no se permiten flujos de información no autorizados.
38. **REQ. 13.** El producto debe permitir realizar una copia de seguridad de su configuración mediante dispositivos extraíbles o a través de su interfaz con la red interna.
39. **REQ. 14.** 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.
40. **REQ. 15.** 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.
41. **REQ. 16.** 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.

4.5 CONTROL DE LOS FLUJOS DE INFORMACIÓN

42. **REQ. 17.** El producto deberá impedir todo flujo de información desde la interfaz de la red receptora hacia la interfaz de la red transmisora, independientemente de su configuración. La unidireccionalidad será física, dado que no contará con hardware que permita la emisión de información en la parte receptora ni con hardware que permita la recepción de información en la parte emisora.
43. **REQ. 18.** El producto deberá implementar mecanismos de control de integridad de la información desde que es recibida por la interfaz del transmisor hasta que es transmitida por la interfaz del receptor.
44. **REQ.19.** El producto no almacenará ningún tipo de información relevante (información transmitida, configuración de red) a la que pueda accederse desde la red externa.

4.6 REQUISITOS CRIPTOGRÁFICOS

45. **REQ. 20.** El producto debe soportar el uso de *ciphersuites* compuestas únicamente por funciones y algoritmos criptográficos aceptados para nivel Alto

del ENS según la guía CCN-STIC-807, así como proporcionar capacidades de configuración que permitan obligar el uso de estas *ciphersuites* exclusivamente.

5. ABREVIATURAS

CC	Criterios Comunes / *Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
EAL	*Evaluation Assurance Level*
ENS	Esquema Nacional de Seguridad
HTTPS	*Hypertext Transfer Protocol*
IPSEC	*Internet Protocol Security*
OSI	*Open Systems Interconnection*
PP	Perfil de Protección
RFS	Requisitos Fundamentales de Seguridad
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
TIC	Tecnologías de la Información y la Comunicación
TLS	*Transport Layer Security*