centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo A.1: Dispositivos de Control de Acceso a Red

Julio 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
2019.07.19 10:05:32 +02'00'

NIPO: 083-19-053-9

Fecha de Edición: julio de 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

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Control de acceso a red** 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 los 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 **Control de acceso a red** 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. El objetivo del control de acceso a red es asegurar que todos los dispositivos que se conectan a las redes corporativas de una organización cumplen con las políticas de seguridad establecidas, incluyendo las de pre-admisión, el cumplimiento de las políticas de seguridad implementadas por el usuario final y los controles post-admisión sobre los recursos de red a los que pueden acceder los usuarios y dispositivos, de cara a reducir el riesgo de entrada de virus, fuga de información sensible, etc.
7. En este contexto, las funciones básicas de seguridad que proporciona esta familia de productos son las siguientes:
    - Impedir aquellos accesos a la red a entidades que no estén autorizadas o no implementen las políticas de seguridad exigidas.
    - Administrar el acceso a los recursos de la red, en base a permisos o roles definidos conforme a la política de seguridad establecida.

2.2 CASOS DE USO

8. Para esta familia de productos se contempla un solo caso de uso que admitirá múltiples configuraciones, ya que serán las políticas de seguridad con las que se configure el dispositivo las que puedan variar e incluir más o menos restricciones.

2.2.1. CASO DE USO 1– GESTIÓN DEL CONTROL DE ACCESO A LA RED

9. El dispositivo de control de acceso se encuentra ubicado, dentro de la arquitectura de red, en una capa anterior a los servicios o redes de la organización para los cuales se requiere un control de acceso.
10. Las fases en las que se divide el proceso de control de acceso a red son:
    - Autenticación de la entidad en función de las políticas establecidas por la organización. Esta tarea podría ser realizada por el propio dispositivo o tratarse de un servicio externo.
    - Si el resultado del proceso de autenticación es positivo, el producto realiza una verificación de que esa entidad cumple los requisitos de seguridad establecidos para la protección de los servicios de la red.
    - Por último, en caso de que se hayan verificado con éxito los requisitos indicados anteriormente, se permitiría el acceso a los recursos de la red en función de los privilegios asignados al perfil de usuario, que residen en un servicio de directorio.
11. Por lo tanto, los datos que maneja el sistema de control de accesos a red son:

- Los archivos de configuración en base a las políticas de seguridad definidas.
- Los objetos de archivos con los que opera, que podrían ser de granularidad diferente a los utilizados por el sistema operativo. Así, mientras el sistema operativo se enfoca a trabajar con objetos fundamentales como ficheros o interfaces de comunicación entre procesos, este tipo de productos tiene la capacidad de trabajar con abstracciones de más alto nivel que pueden ser implementadas como una combinación de objetos fundamentales.
- Los eventos de auditoría registrados.

12. La Figura 1 muestra un esquema de la arquitectura del sistema, que podrá ser implementada por un solo producto con múltiples capacidades o por un conjunto de productos.

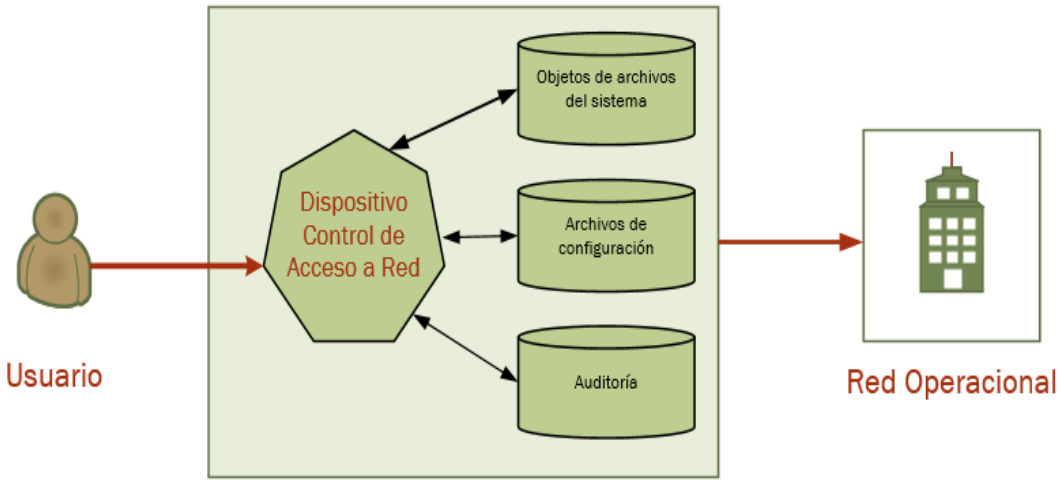

Figura 1 Ejemplo de caso de uso de Control de acceso a red.

2.3 ENTORNO DE USO

13. Por lo general estos dispositivos se utilizan en grandes o medianas empresas y en redes del sector público, junto con otras medidas de seguridad complementarias, formando parte de una arquitectura de defensa en profundidad que busca asegurar el entorno de comunicación.
14. Para la utilización en condiciones óptimas de seguridad de estos productos, es necesaria su integración en un entorno operacional que cumpla las siguientes condiciones:

- **Protección física.** El dispositivo se encuentra protegido por su entrono operacional y no puede sujeto de ataques físicos que pudiesen comprometer su seguridad o interferir en su correcta operación.
- **Administración confiable.** El usuario administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la red de comunicaciones. Por ello, se asume que dicha

persona estará altamente capacitada y carecerá de cualquier intención dañina al administrar estos dispositivos.

- **Actualizaciones periódicas.** El administrador actualiza periódicamente el firmware o software del dispositivo con los últimos parches de seguridad.
- **Credenciales de administrador protegidas**. Las credenciales de administrador se encontrarán protegidas por la plataforma en la que residen.
- **Política de seguridad de la información.** El producto recibirá las políticas de seguridad del entorno operacional.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

15. Este tipo de productos se presentan en formato de equipo dedicado (*Appliance*: hardware provisto de firmware[1] dedicado) con las funcionalidades estrictamente necesarias para cumplir su finalidad y acotadas al servicio específico que presten.
16. Adicionalmente, suele ser habitual que en las máquinas y dispositivos que protegen se incluya un software instalable (agente) que ejerce un papel de control de las entidades conectadas en la red.
17. Por último, para realizar las funciones de control y administración del dispositivo es normal incluir con el producto un software específico para instalarlo en un equipo informático estándar.
18. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, éstas quedan fuera del alcance analizado, y deberán ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

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 seguridad independientes de la implantación.
21. Los productos dentro de esta familia deberán cumplir con los RFS reflejados en el apartado 4 y con los SFR (*Security Functional Requirements*) que se especifica en el siguiente perfil de protección certificado de acuerdo a la norma *Common Criteria*:

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

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Devices[2]	2.1	24/09/2018	CCDB
Collaborative Protection Profile for Network Devices[3]	2.0 + Errata 20180314	14/03/2018	CCDB
Collaborative Protection Profile for Network Devices.[4]	1.0	27/02/2015	CCDB

Tabla 1. Perfiles de protección

22. En caso de que el producto no esté certificado contra este perfil, la declaración de seguridad deberá contener al menos los SFR de éstos con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

[2] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.1.pdf
[3] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.0E.pdf
[4] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

23. Los recursos que deben protegerse mediante el uso de estos productos incluyen:

- Credenciales y permisos de acceso, así como cualquier otra información sensible asociada al control de acceso. Podrá estar almacenada en el producto o ser intercambiada a través de la red con usuarios u otras entidades.
- Interfaces de gestión del producto e información transmitida a través de ellas, en ambos sentidos.
- Datos de configuración del producto y de auditoría generados por éste.
- Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.
- La propia funcionalidad de seguridad del producto.

3.2 AMENAZAS

24. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente, atendiendo al caso de uso expuesto en la sección 2.1, serían:

- **Acceso no autorizado de administrador.** Un atacante consigue acceso de administrador haciéndose pasar por él, mediante ataques *man in the middle*, o accediendo a sesiones de administración abiertas. Este acceso no autorizado permite acciones maliciosas que comprometen la funcionalidad de seguridad al dispositivo y de la red en la que se encuentra instalado.
- **Criptografía débil.** Un atacante podría explotar algoritmos criptográficos débiles o desarrollar ataques de fuerza bruta contra el espacio de claves. Algoritmos débiles o tamaños de clave inadecuados podrían permitir a los atacantes acceder al dispositivo y leer, controlar o manipular los activos del sistema.
- **Canales de comunicación no confiables**. Un atacante podría comprometer tráfico de red crítico debido al uso de protocolos inadecuados o mala gestión de claves (p. ej. Ataques *man in the middle,* ataques de repetición) o que usan autenticación débil extremo a extremo.
- **Compromiso de las actualizaciones del sistema.** Un atacante consigue comprometer la actualización del sistema y modificar el firmware o software, de manera que se comprometa la seguridad del dispositivo.
- **Actividad no detectada.** Un atacante consigue acceder, cambiar o modificar la funcionalidad de seguridad del dispositivo sin que esto sea apreciado por el administrador.

- **Compromiso de datos de usuario y credenciales.** Un atacante consigue comprometer los las credenciales del dispositivo y acceder y/o modificar los datos de usuario y/o las credenciales de éstos.
- **Fallo en la funcionalidad de seguridad.** Un componente del dispositivo podría fallar durante el arranque o la operación del equipo y comprometer la funcionalidad de seguridad de éste exponiéndolo a ataques.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

1. 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 COMMON CRITERIA

2. **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[5]	2.1	24/09/2018	CCDB
Collaborative Protection Profile for Network Devices[6]	2.0 + Errata 20180314	14/03/2018	CCDB
Collaborative Protection Profile for Network Devices.[7]	1.0	27/02/2015	CCDB

Tabla 2. Perfiles de protección

3. **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. **REQ. 3** Serán obligatorios los SFR FMT_MOF.1/AdminAct y FMT_MTD.1/AdminAct.

4.2 REQUISITOS CRIPTOGRÁFICOS

5. **REQ. 4**. En caso de que el producto utilice algoritmos y funciones criptográficas, debe soportar el uso de aquellas aceptadas para nivel Alto del ENS según la guía CCN-STIC-807, así como proporcionar capacidades de configuración que permitan obligar al uso de estos algoritmos exclusivamente.
6. **REQ. 5.** El producto debe soportar el uso de longitudes de clave que proporcionen una fortaleza equivalente a 128 bits o superior.

[5] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.1.pdf
[6] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.0E.pdf
[7] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf

5. ABREVIATURAS

CC	*Common Criteria*
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
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*