centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC - Anexo D.5: Dispositivos de Red Inalámbricos

Junio 2021

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA 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
2021.06.23 16:40:11 +02'00'

NIPO: 083-21-130-1

Fecha de Edición: Junio 2021

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 **Dispositivos de Red Inalámbricos** 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 **Dispositivos de Red Inalámbricos** 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 esta familia están orientados a la protección de comunicaciones, proporcionando conectividad a una red local inalámbrica (WLAN[1]) mediante comunicaciones por radiofrecuencia. Su función principal consiste en enviar paquetes de datos de una red a otra o en la misma mediante el uso de conexiones de nodos de ondas electromagnéticas sin necesidad de una red cableada.
7. En este contexto proporcionan las siguientes funciones básicas de seguridad:
   - Acceso a redes WLAN de dispositivos inalámbricos con uso de criptografía para las comunicaciones y transmisiones por radiofrecuencia.
   - Administración de puertos, asignándoles prioridades, habilitándolos o deshabilitándolos para su uso.
   - Filtrado de tráfico en función de listas de control de acceso (ACLs[2]). Estas listas pueden filtrar el tráfico en base a: dirección IP[3] (origen o destino), tipo de protocolo o puerto de uso (en origen o destino).
8. Los productos incluidos en esta familia pueden ofrecer otras funcionalidades complementarias (p.ej.: conexión mediante Bluetooth) no específicamente contempladas en este documento.

2.2 CASOS DE USO

9. S contemplan dos (2) casos de uso para esta familia de productos tal y como se describen a continuación.

2.2.1. CASO DE USO 1 - PUNTO DE ACCESO INALÁMBRICO AUTÓNOMO

10. Un punto de acceso inalámbrico (AP) permite la conexión de forma inalámbrica de los dispositivos dentro de su alcance a una red.

[1] *Virtual Local Area Network*
[2] *Access Control List*
[3] *Internet Protocol*

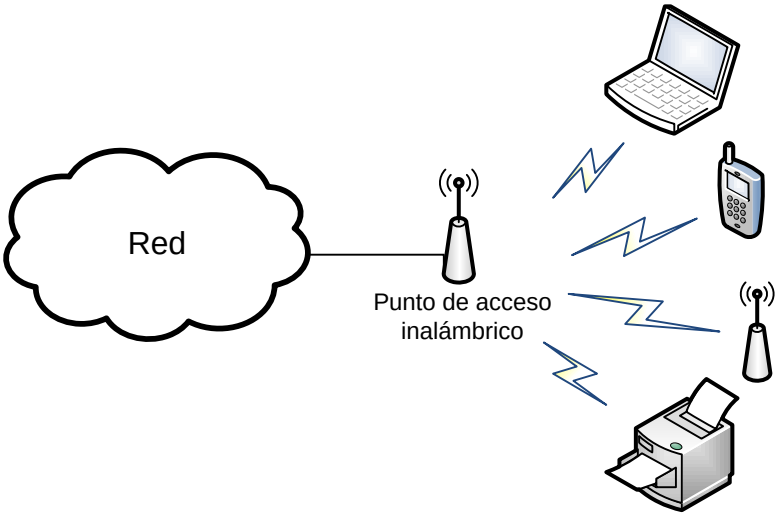

Figura 1. Punto de Acceso inalámbrico autónomo

2.2.2. CASO DE USO 2 - PUNTO DE ACCESO INALÁMBRICO GESTIONADO

11. Un punto de acceso inalámbrico (AP), gestionado por una controladora de acceso inalámbrico (AC), permite la conexión de forma inalámbrica de los dispositivos dentro de su alcance a una red.

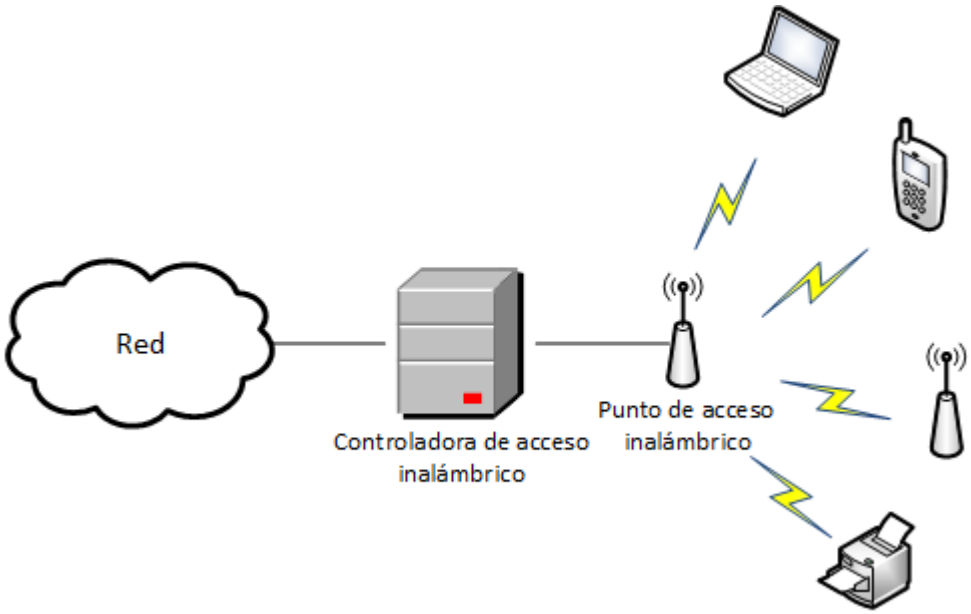

Figura 2. Punto de Acceso y Controladora de acceso inalámbrico

2.3 ENTORNO DE USO

12. Este tipo de dispositivos son de uso generalizado en grandes o medianas empresas, así como en redes del sector público como parte de una arquitectura de defensa en profundidad, existiendo medidas complementarias en diferentes capas de protección.

13. Para la utilización en condiciones óptimas de seguridad de estos dispositivos, es necesaria su integración 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.
    - **Funcionalidad limitada**: El producto deberá utilizarse para el enmascaramiento y filtrado de las conexiones como su función básica y no proporcionar ninguna otra funcionalidad, salvo aquellas determinadas compatibles orientadas a la protección de las comunicaciones.
    - **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 capacitada, formada y carecerá de cualquier intención dañina.
    - **Actualizaciones periódicas**: El firmware y el software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
    - **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

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

15. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1**¡Error! No se encuentra el origen de la referencia.**, éstas quedan fuera del alcance analizado, debiendo ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

16. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TIC (Tecnologías de la Información y de las Comunicaciones).
17. 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, tanto funcionales como de evaluación, independientes de la implantación.
18. Los productos dentro de esta familia deberán estar certificados de acuerdo a la norma *Common Criteria*. Dicha certificación deberá evidenciar el problema de seguridad definido en el presente documento e incluir los requisitos fundamentales de seguridad recogidos en el apartado 4.
19. 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** en el caso en el que el producto no se encuentre certificado contra ningún perfil.
20. En caso de que alguno de los requisitos indicados en el apartado 4 no se encuentre recogido en la declaración de seguridad del producto, pero este sí implemente esa función de seguridad, se podrá llevar a cabo una ***evaluación STIC complementaria***, cuyo objetivo será verificar el cumplimiento de esos requisitos.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

21. Los recursos a proteger mediante el uso de estos productos, así como para su correcto funcionamiento, incluyen:

    - Información que atraviese el producto entre sus interfaces de red.
    - Interfaces de gestión del producto y la 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.

3.2 AMENAZAS

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

    - **Divulgación de información no autorizada:** Un atacante ya sea desde dentro de la red o desde fuera consigue enviar información no autorizada a través de la red o hacia una ubicación en el exterior (p.ej.: filtrar información protegida o configuraciones de la red).
    - **Acceso no autorizado**: Un atacante ya sea desde dentro de la red o desde fuera consigue acceder a información, intercambiada a través del dispositivo o almacenada en él, para la que no estaba autorizado (p.ej.: comunicaciones entre el punto de acceso y dispositivos inalámbricos ajenos) o utilizar el dispositivo como mecanismo de acceso a los recursos y servicios de una red para los que no está autorizado (p.ej. acceder a la red WLAN sin la debida autorización).
    - **Envío de tráfico dañino**: Un atacante consigue enviar información maliciosa a la red WLAN a través del dispositivo, con el fin de poner en riesgo la seguridad de éste o de aquellos otros recursos a los que da acceso (p.ej. provocar una denegación de servicio).
    - **Cifrado débil**: Utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
    - **Uso de canales de comunicación inseguros**: Mala implementación de protocolos estándar o utilización de protocolos no estandarizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones del dispositivo.
    - **Compromiso de la funcionalidad del dispositivo**: Un atacante o un fallo en el dispositivo compromete la funcionalidad de seguridad, permitiendo

modificarla o desactivarla de manera no conforme a las políticas de seguridad.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

23. 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

24. **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[4]	2.2e	27/03/2020	CCDB
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 1. Perfiles de protección

25. **REQ. 2** En caso de que el producto no esté certificado contra ninguno de los perfiles anteriores, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) de *Collaborative Protection Profile for Network Devices V.2.2e* con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

26. **REQ. 3.** Los productos deberán estar certificados con los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria:*

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

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Extended Package Wireless Local Area Network (WLAN) Access Systems[8]	1.0	29/05/2015	NIAP

Tabla 2. Perfiles de protección

27. **REQ. 4.** 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*) de *Extended Package Wireless Local Area Network (WLAN) Access Systems v1.0.* con **un nivel de confianza EAL (Evaluation Assurance Level) EAL2 o superior.**

4.2 REQUISITOS CRIPTOGRÁFICOS

28. **REQ. 5.** 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).

4.3 PROTECCIÓN DEL DISPOSITIVO Y SUS SERVICIOS

29. **REQ.4.** En caso de que el producto disponga de interfaces de conexión inalámbricas adicionales, fuera de las especificadas para redes WLAN, debe permitir deshabilitarlas para limitar la conectividad al producto sólo a través de las interfaces certificadas.

4.4 NOTAS DE APLICACIÓN

30. En el CASO DE USO 2 - PUNTO DE ACCESO INALÁMBRICO GESTIONADO, los requisitos deberán aplicarse tanto al punto de acceso inalámbrico (AP) como a la controladora de acceso inalámbrico (AC) que lo gestiona. Por tanto, el alcance de la certificación deberá incluir tanto al punto de acceso inalámbrico (AP) como a la controladora de acceso inalámbrico (AC).

[8] https://www.niap-ccens.org/pp/pp_wlan_as_ep_v1.0.pdf

5. ABREVIATURAS

AC	Controladora de acceso inalámbrico (*Access Controller*)
ACL	*Access Control List*
AP	Punto de acceso inalámbrico (*Access Point*)
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*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
MAC	*Media Access Control*
NIAP	*National Information Assurance Partnership*
OSI	*Open System Interconnection*
RFS	*Requisitos Fundamentales de Seguridad*
SFR	*Security Functional Requirements*
SW	*Software*
VLAN	*Virtual Local Area Network*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL