centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

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

Diciembre 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
2019.12.27 13:20:16 +01'00'

NIPO: 083-19-053-9.

Fecha de Edición: diciembre 2019

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. Tan solo se contempla un caso de uso para esta familia de productos tal y como se describen a continuación.

2.2.1. CASO DE USO 1 – INTERMEDIARIO EN LA CONEXIÓN

10. El dispositivo 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*

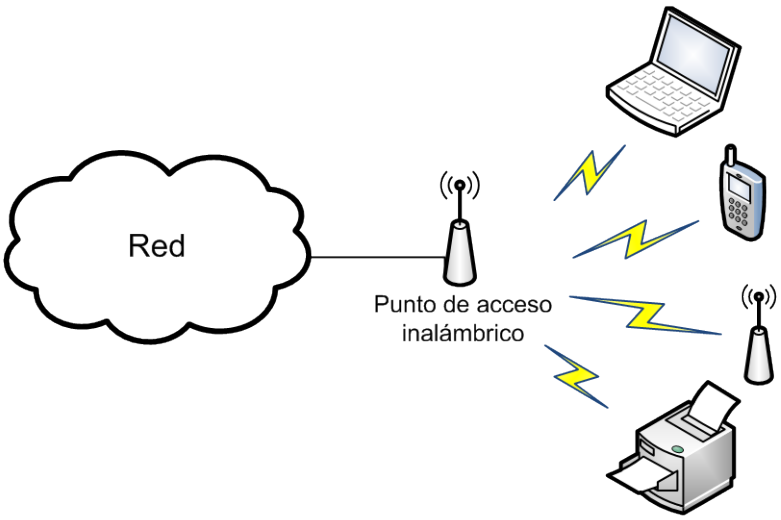

Figura 1 – Ejemplo de Caso de Uso 1: Punto de Acceso a Red

2.3 ENTORNO DE USO

11. 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.

12. 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

13. 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.
14. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2, éstas quedan fuera del alcance analizado, debiendo ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 CERTIFICACIÓN LINCE

15. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS Medio, deberá disponer de una Certificación Nacional Esencial de Seguridad (LINCE)[4] que incluya los RFS reflejados en el apartado 4, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.
16. El alcance de la evaluación deberá incluir el módulo de evaluación básico de 25 días de esfuerzo y el Módulo de Evaluación Criptográfica (MEC). El Módulo de Revisión de Código Fuente (MCF) será opcional.

[4] Toda la información relativa a esta metodología se encuentra disponible en la web del Organismo de Certificación (https://oc.ccn.cni.es)

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

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

- AC Administración. Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos.
- AC Datos. Datos de configuración del producto y de auditoría generados por éste. Información que atraviese el producto entre sus interfaces de red.
- AC. Actualizaciones. Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

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

3.2.1. COMUNICACIONES CON EL PRODUCTO

- **A.NOAUT Acceso no autorizado de administrador:** Un atacante puede obtener un acceso cómo administrador del producto haciéndose pasar por un administrador ante el producto, por el producto ante un administrador, reproduciendo una sesión de administración, realizando ataques del hombre en medio.
- **A.CIFRA Cifrado débil:** Utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **A.COM Canales de comunicación no confiables:** 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.
- **A.AUT Autenticación débil de los nodos:** Un producto puede utilizar protocolos de autenticación seguros que utilicen métodos de autenticación débiles (contraseñas no robustas, contraseñas cómo texto en claro, contraseñas precompartidas) para hacerse pasar por un usuario administrador u otro nodo para realizar un ataque de hombre en el medio.

3.3 ACTUALIZACIONES VÁLIDAS

- **A.ACT Actualización maliciosa:** un atacante puede realizar una actualización maliciosa que debilite las funcionalidades de seguridad del producto.

3.4 AUDITORÍA

- **A.AUD Actividades no detectadas:** Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.

3.5 INFORMACIÓN Y CREDENCIALES

- **A.CRED Funcionalidades de seguridad comprometidas:** un atacante puede comprometer las credenciales o información del producto permitiendo un acceso continuado al producto y a su información sensible.
- **A.CON Contraseñas débiles:** Un atacante puede aprovecharse del uso contraseñas débiles para acceder con acceso privilegiado al dispositivo.

3.6 FALLO DEL PRODUCTO

- **A.FUN Fallo de las funcionalidades de seguridad:** Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

19. 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 ADMINISTACIÓN

20. **REQ. 1.** El producto debe de definir al menos el rol de administrador y ser capaz de asociar usuarios a roles.
21. **REQ. 2.** El producto debe ser capaz de realizar la gestión de las siguientes funcionalidades:
    - Administración del producto de forma local y remota.
    - Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
    - Otros parámetros de configuración del producto (definir).
22. **REQ. 3.** El producto deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones anteriormente descritas.
23. **REQ. 4.** La opción de administración desde un cliente inalámbrico deberá estar deshabilitada por defecto.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

1. **REQ. 5.** El producto debe de identificar y autenticar a cada usuario antes de permitir acciones que modifiquen su configuración.
2. **REQ. 6.** El producto debe detectar cuando un administrador remoto realiza un número determinado de intentos de autenticación fallidos. En caso de que se alcance este número de intentos, el producto deberá impedir que ese administrador
3. período de tiempo.
4. **REQ. 7.** El producto debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad.
5. **REQ. 8.** El producto deberá tener la capacidad de denegar sesiones de usuarios inalámbricos basándose, al menos, en el interfaz, el día y la hora.
6. **REQ. 9.** El producto debe disponer de la capacidad de gestión de las contraseñas:
    a) La contraseña debe de poder configurarse con una longitud mínima o igual a 9 caracteres.

b) La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]

7. **REQ. 10.** El producto debe evitar que se lean contraseñas en texto plano y en ningún caso almacenarlas en memoria no volátil.
8. **REQ. 11.** El producto debe cumplir con el estándar IEEE 802.1X para un PAE (*Port Access Entity*) en el rol de “Autenticador”.
9. **REQ. 12.** El producto soportará comunicaciones con un servidor de autenticación RADIUS.
10. **REQ. 13.** El producto deberá asegurar que no se permite el acceso a sus puertos controlados con 802.1X a un cliente inalámbrico hasta que no complete el intercambio de autenticación.

4.3 CANAL SEGURO

11. **REQ. 14.** El producto debe ser capaz de proveer un canal de comunicación seguro entre entidades autorizadas (ej. Clientes WLAN, servidor de auditoría, servidores de autenticación 802.1X, etc.), a través de WPA2 (mandatorio), IEEE 802.1X (mandatorio), IPSec (mandatorio), TLS 1.2 o superior (opcional), DTLS (opcional) y/o HTTPS (opcional).
12. **REQ. 15.** El producto debe permitir comunicaciones a través de canales seguros iniciados por sí mismo o por entidades autorizadas.

4.4 CRIPTOGRAFÍA

13. **REQ. 16.** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos que utilicen suites de cifrado que estén incluidas entre las autorizadas para Categoría Media del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.
14. **REQ. 17** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).
15. **REQ. 18.** En caso de suministrar un servicio de generación de bits aleatorios (RBG[5]) determinísticos para la generación de claves, el producto deberá:
    - *Utilizar Hash_DRBG (any), HMAC_DRBG (any)* o *CTR_DRBG (AES).*
    - Usar una semilla de al menos una fuente de entropía que acumule entropía de varias fuentes o disponer de una fuente de entropía estudiada, con un mínimo de bits de entropía al menos igual a la mayor fortaleza de seguridad de las claves y hashes que generará, de acuerdo a la ISO/IEC 18031:2011.

[5] *Random Bit Generator*

4.5 ACTUALIZACIONES

16. **REQ. 19.** El producto debe ofrecer la posibilidad de iniciar actualizaciones de forma manual. Esta funcionalidad se permitirá únicamente a usuarios con rol de administrador.
17. **REQ. 20.** El producto debe ofrecer mecanismos (conforme a la criptografía de empleo en el ENS) a través de hashes o firma digital para autenticar las actualizaciones de firmware/software antes de instalarlas.
18. **REQ. 21.** El producto debe ofrecer la posibilidad de consultar la versión actual del firmware/software.

4.6 AUDITORÍA

19. **REQ. 22.** El producto debe generar información de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produzca alguno de los siguientes eventos:
    a) *Login* y *logout* de usuarios registrados.
    b) Cambios en la configuración del TOE.
    c) Generación, importación, cambio o eliminación de claves criptográficas.
    d) Cambios en las credenciales de usuarios.
    e) Otros eventos de seguridad relevantes (definir).
20. **REQ. 23.** El producto debe generar los registros de auditoría junto con, al menos, la fecha, hora, tipo de evento y resultado.
21. **REQ. 24.** El producto debe ser capaz de transmitir la información de auditoría a una entidad externa usando un canal seguro (según párrafo 4.3).
22. **REQ. 25.** El producto debe ser capaz de almacenar la información de auditoría generada en sí mismo.
23. **REQ. 26.** El producto debe ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno.
24. **REQ. 27** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: Sólo usuarios autorizados.
    b) Modificación: Ningún usuario.
    c) Borrado: Administradores.

4.7 PROTECCIÓN CONTRA FALLOS

25. **REQ. 28.** El producto deberá ser capaz de realizar un test durante el arranque o encendido del producto, periódicamente durante la operación normal del producto y a petición de un usuario autorizado para demostrar el

funcionamiento correcto del producto determinado previamente. En caso de fallo en el arranque deberá poder volver a un estado seguro.

26. **REQ. 29.** El producto deberá exponer los servicios mínimos que sean necesario para su correcto funcionamiento.

5. ABREVIATURAS

ACLs	*Access Control Lists*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
MAC	*Media Access Control*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
RFS	Requisitos Fundamentales de Seguridad
TOE	*Target of Evaluation*
WLAN	*Wireless Local Area Network*