centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

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

Noviembre de 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.01.03 14:54:34 +01'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: 083-22-102-1

Fecha de Edición: noviembre de 2022

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 y Servicios STIC (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), categoría MEDIA**. 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. Se 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*

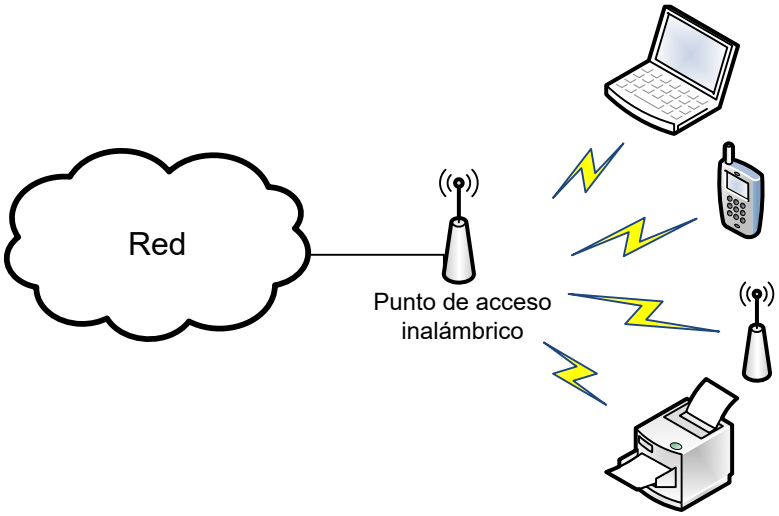

Figura 1. Punto de Acceso inalámbrico autónomo

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.

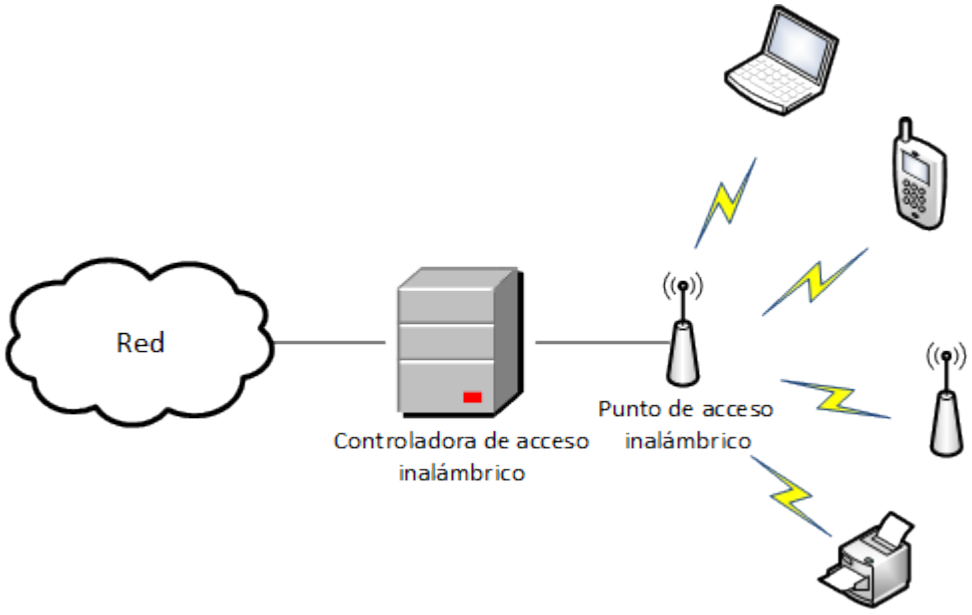

Figura 2. Punto de Acceso y Controladora de acceso inalámbrico

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

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 debe estar protegido físicamente por su entorno operacional y no sujeto a ataques físicos que puedan comprometer su seguridad o interferir en su correcta operación. En caso de productos software, esta hipótesis aplica a la plataforma física sobre la que se ejecuta el producto.
    - **Administración confiable**. Los administradores son miembros de plena confianza y velan por los mejores intereses en materia de seguridad de la organización. Dichas personas deben estar debidamente capacitadas y carecer de cualquier intención maliciosa o conflicto de intereses al administrar el producto.
    - **Actualizaciones periódicas**: El *firmware/software* del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
    - **Funcionalidad limitada**. El producto solo debe proporcionar la funcionalidad de dispositivo de red inalámbrico como función principal y no debe proporcionar ninguna otra funcionalidad o servicio.
    - **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

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. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, 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 ACTIVOS SENSIBLES A 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, que debe ser protegida en Confidencialidad, Trazabilidad, Autenticidad e Integridad.
- **AC.PSS.** Datos de configuración, registros auditoría y [***asignación****: listado de datos definidos por el fabricante*] que deben ser protegidos en Integridad.
- **AC.PSC.** [**selección**: credenciales; claves; [**asignación**: *listado de datos definidos por el fabricante*] que deben ser protegidos en Confidencialidad e Integridad.
- **AC.Actualizaciones.** Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad, que deben ser protegidos en Integridad y Autenticidad.
- **AC.Comunicaciones.** Comunicaciones del producto, establecidas entre sus propios componentes y con [**asignación**: *listado de entidades autorizadas*] que deben ser protegidas en Confidencialidad, Integridad y Autenticidad.

3.2 AMENAZAS

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

- **A.NOAUT Acceso no autorizado de administrador:** Un atacante puede obtener un acceso de administración no autorizado haciéndose pasar por un administrador ante el producto, haciéndose pasar por el producto ante un administrador, reproduciendo una sesión de administración, o realizando ataques del hombre en medio.
- **A.CRYPTO Mecanismos criptográficos débiles:** Utilización en el producto de mecanismos criptográficos o longitudes de clave débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **A.COM Protocolos de comunicación no autorizados:** Utilización de protocolos no autorizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones críticas del producto.
- **A.ACT Actualización maliciosa:** un atacante puede realizar una actualización maliciosa que comprometa las funcionalidades del producto.
- **A.AUD Actividades no detectadas:** Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.

- **A.PSC Compromiso de parámetros de seguridad críticos:** un atacante puede comprometer los parámetros de seguridad críticos y acceder de forma continuada al producto y a sus datos críticos.

- **A.FUN Fallo de las funcionalidades de seguridad:** Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad declaradas del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.
- **A.NOAUTUSR Acceso no autorizado de usuario:** Un atacante puede obtener un acceso no autorizado haciéndose pasar por un usuario ante el producto, haciéndose pasar por el producto ante un usuario, reproduciendo una sesión de usuario, o realizando ataques del hombre en medio.
- **A.CRE Compromiso de credenciales:** Un atacante puede aprovecharse del uso de credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.
- **A.RED Ataque a la red:** Un atacante consigue acceder a la red pudiendo realizar mapeos de las máquinas que residen en ella y obtener datos de dirección IP, servicios o cualquier otra información que le permita lanzar ataques a dichas máquinas y servicios.

3.3 TRAZABILIDAD AMENAZAS/ REQUISITOS DE SEGURIDAD

19. En la siguiente tabla se trazan que Requisitos Fundamentales de Seguridad definidos en el apartado 4 cubren las amenazas definidas:

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSC	A.FUN	A.NOAUTUSR	A.CRE	A.INT	A.RED
ADM.1	X										
ADM.2	X										
ADM.3	X										
IAU.1	X							X			
IAU.2									X		
IAU.3									X		
COM.1		X	X								
COM.2			X								
ACT.1				X							
ACT.2				X							
ACT.3				X							
AUD.1					X						
AUD.2					X						

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSC	A.FUN	A.NOAUTUSR	A.CRE	A.INT	A.RED
AUD.3					X						
AUD.4					X						
AUD.5					X						
PSC.1						X					
PRO.1							X				
CIF.1		X	X								
CIF.2		X	X								
DRI.1	X										X
DRI.2											X
DRI.3											X
DRI.4											X
DRI.5											X
DRI.6											X
DRI.7											X

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

20. 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.

21. La convención utilizada en las descripciones de los RFS es la siguiente:

- Selección: se deberá seleccionar al menos una opción de las indicadas en el RFS y se incluirá en la declaración de seguridad. Ejemplo:

  RFS: Administración del producto [**selección***: local; remota*]

  DS: Administración del producto local y remota

- Asignación: se deberá especificar el listado de opciones que sean de aplicación al TOE (podría no haber ninguna). Ejemplo:

  RFS: El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación:** otros usuarios del producto] antes de otorgar acceso.

22. DS: El TOE deberá identificar y autenticar a cada usuario administrador, auditor y usuario avanzado antes de otorgar acceso.

4.1 ADMINISTACIÓN CONFIABLE

23. Podrán ser cubiertas por el producto o por su entorno operacional.

24. **ADM.1** El TOE debe de definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.

25. **ADM.2** El TOE debe ser capaz de realizar la gestión de las siguientes funcionalidades:

- Administración del producto [**selección**: *local; remota*].
- Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
- [**asignación**: otras funcionalidades administrables del producto].

26. **ADM.3** El TOE deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones descritas en **ADM.2**.

> Nota de aplicación: en el caso de que existan distintos tipos de administrador, cada uno de ellos con distintos permisos, deberá probarse que únicamente pueden realizar aquellas funcionalidades para las que tengan permiso.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

27. Podrán ser cubiertas por el producto o por su entorno operacional.

28. **IAU.1** El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación**: *otros usuarios del producto*] antes de otorgar acceso, salvo para las siguientes funcionalidades [**asignación**: *listado funcionalidades*].

29. **IAU.2** El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.

30. **IAU.3** El TOE debe disponer de la capacidad de gestión de las contraseñas:

    a) La contraseña debe de poder configurarse con una longitud mínima o igual a 12 caracteres.

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

Nota de aplicación: este requisito podría ser modificado en el caso de que el TOE implemente otros mecanismos de autenticación.

4.3 CANALES SEGUROS

31. Podrán ser cubiertas por el producto o por su entorno operacional.

32. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas: [**selección***: servidor de auditoría;* [***asignación****: otras entidades*]] o entre distintas partes del producto, usando [**selección***: IPSec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

    NOTA: Este requisito se extiende con el requisito DRI.6 (Apartado 4.9).

33. **COM.2** El TOE debe permitir que los canales de comunicación definidos en **COM.1** sean iniciados por él mismo o por las entidades autorizadas.

4.4 CRIPTOGRAFÍA

34. **CIF.1** El TOE permitirá exclusivamente el empleo de mecanismos criptográficos: [***asignación****: listado de mecanismos*] autorizados de acuerdo a lo establecido en la guía CCN-STIC-807. La fortaleza de clave empleada será la indicada en esa guía para Categoría MEDIA del ENS, y de acuerdo al nivel de amenaza establecido.

35. **CIF.2.** Generador de bits aleatorios. En caso de suministrar un servicio de generación de bits aleatorios (RBG[5]) determinísticos, el producto deberá:

    - Utilizar [**selección:** *Hash_DRBG (any), HMAC_DRBG (any)* o *CTR_DRBG (AES)*].

[5] *Random Bit Generator*

- Usar una semilla de, al menos, una Fuente de entropía que acumule entropía [selección: de una o varias fuentes; 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.

4.5 INSTALACIÓN Y ACTUALIZACIONES CONFIABLES

36. **ACT.1** El TOE ofrecerá la posibilidad de consultar la versión actual del firmware/software y podrá [**selección**: actualizarse automáticamente; iniciar actualizaciones manualmente] y [**selección**: comprobar si existen nuevas actualizaciones disponibles; ningún otro].
37. **ACT.2** El TOE deberá utilizar [**selección***: hashes publicados; firma digital*] que estén autorizados en la guía CCN-STIC-807 para autenticar las actualizaciones *firmware/software* antes de instalarlas.
38. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.

4.6 AUDITORÍA

39. **AUD.1** El producto debe generar registros de auditoría cuando se produzca alguno de los siguientes eventos:
    a) Al inicio y finalización de las funciones de auditoría.
    b) *Login* y *logout* de usuarios registrados.
    c) Cambios en las credenciales de usuarios.
    d) Cambios en la configuración del producto [**asignación**: *listado de cambios*].
    e) Eventos relativos a la funcionalidad del producto [**asignación:** *listado de eventos*].
    f) Si el TOE gestiona claves criptográficas, [**selección:** generación; importación; cambio; eliminación de claves criptográficas; ningún otro].
40. **AUD.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.
41. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: usuarios autorizados.
    b) Modificación: ningún usuario.
    c) Borrado: [**selección**: solo administradores; ningún usuario]

42. **AUD.4** El TOE debe ser capaz de almacenar en sí mismo la información de auditoría generada y transmitir la información de auditoría generada a una entidad externa utilizando un canal seguro COM.1.

43. **AUD.5** El TOE deberá [**selección**: sobreescribir los registros siguiendo el criterio de mayor antigüedad; enviar a una entidad externa y eliminar; otra opción validada por el CPSTIC] en el caso de que el espacio para almacenamiento de los registros alcance su límite.

4.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

44. **PSC.1** En el caso en que el TOE almacene [***selección**: credenciales; claves privadas; [**asignación**: otros parámetros de seguridad críticos*] estos no deberán almacenarse en claro, sino que se utilizarán mecanismos de protección criptológica que cumplan con **CIF.1**.

4.8 PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

45. **PRO.1** El TOE deberá ser capaz de realizar un test durante el arranque o encendido del producto, [**selección***: periódicamente durante la operación normal del producto; a petición de un usuario autorizado; ninguna*] para verificar la integridad del software/firmware, [***selección**: el correcto funcionamiento de los mecanismos criptográficos; [**asignación**: otros]; ninguno*].

4.9 DISPOSITIVO DE RED INALÁMBRICO

46. **DRI.1.** La opción de administración desde un cliente inalámbrico deberá estar deshabilitada por defecto.

47. **DRI.2.** El TOE deberá tener la capacidad de denegar sesiones de usuarios inalámbricos basándose, al menos, en el interfaz, el día y la hora.

48. **DRI.3.** El TOE debe cumplir con el estándar IEEE 802.1X para un PAE (*Port Access Entity*) en el rol de "*Autenticador*".

49. **DRI.4.** El TOE soportará comunicaciones con un servidor de autenticación RADIUS.

50. **DRI.5.** El TOE 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.

51. **DRI.6.** El TOE deberá ser capaz de utilizar WPA2 con 802.1X para las comunicaciones con clientes WLAN e IPsec para la comunicación con los servidores de autenticación.

4.10 NOTAS DE APLICACIÓN GENERALES

52. 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).

5. ABREVIATURAS

AC	Controladora de acceso inalámbrico (*Access Controller*)
ACLs	*Access Control Lists*
AP	Punto de acceso inalámbrico (*Access Point*)
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
IP	*Internet Protocol*
ISP	*Internet Service Provider*
MAC	*Media Access Control*
RFS	Requisitos Fundamentales de Seguridad
TOE	*Target of Evaluation*
WLAN	*Wireless 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