centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo D.2M: Switches

Septiembre 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN 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
2019.10.01 15:19:01 +02'00'

NIPO: 083-19-053-9.

Fecha de Edición: Septiembre 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 ***Switches*** 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 para los 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 ***Switches*** 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

6. Los productos asociados a esta familia se utilizan para interconectar los segmentos físicos de una red y habilitar la circulación de datos entre dichos segmentos. Los conmutadores trabajan a nivel de enlace (capa 2) del modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1)[1]y dirigen el tráfico según direccionamiento físico o Media Access Control (MAC[2]) de Ethernet. Algunos conmutadores también ofrecen funciones adicionales tales como segmentación de redes virtuales (VLAN[3]) y conmutación a nivel de red (capa 3).

7. Salvo que existan características avanzadas que deban configurarse de manera específica siendo un dispositivo "administrado" (p.ej.: VLANs), el conmutador no requiere configuración ya que ésta es automática siendo considerados como dispositivos "no administrados". Para ello, su funcionalidad les permite escuchar el tráfico en cada puerto y descubrir en cuál está conectado cada dispositivo, para a continuación enviar el tráfico directamente al puerto de destino correspondiente. El proceso de conmutación se realiza en hardware a la velocidad que permite el cable sin prácticamente período de latencia.

8. En este contexto proporcionan las siguientes funciones básicas de seguridad:

   - Administración de puertos, asignándoles prioridades, habilitándolos o deshabilitándolos para su uso.
   - Filtrado MAC y otros tipos de funciones de "seguridad de puertos".
   - Definición de redes VLAN para la segregación en segmentos lógicos de una red.

9. Los productos incluidos en esta familia pueden ofrecer otras funcionalidades complementarias (p.ej. enrutamiento a nivel de enlace, capa 3) no específicamente contempladas en este documento.

2.1 CASOS DE USO

10. Dependiendo de las funcionalidades del producto explotadas y de la finalidad o el contexto en que se utilicen, se contemplan dos casos de uso para esta familia de productos tal y como se definen a continuación.

2.1.1. CASO DE USO 1 - UNIÓN DE SEGMENTOS DE UNA RED

11. En este caso se utiliza uno o varios conmutadores (*switches)* dentro de una red para realizar la conexión de múltiples equipos dentro del mismo segmento de red. Los equipos enviarán información por la red que pasará por los *switches*

[1] Modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1) es un modelo de referencia para los protocolos de la red de arquitectura en capas creado por la Organización Internacional de Normalización (ISO) y la Comisión electrotécnica Internacional (IEC).
[2] *Media Access Control*
[3] *Virtual Local Area Network*

que la encauzarán hacia su destino dentro de la misma red o hacia otras redes interconectadas mediante dispositivos capaces de realizar el debido enrutamiento.

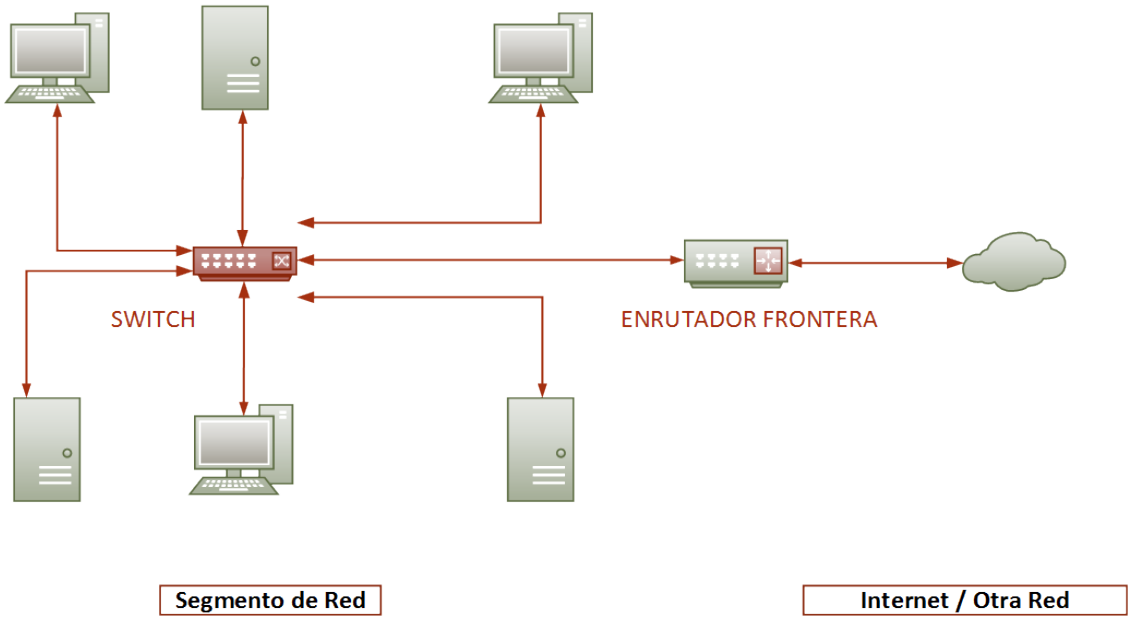

Figura 1-Caso de uso 1-Unión de segmentos de una red

2.1.2. CASO DE USO 2- CREACIÓN DE REDES VIRTUALES DENTRO DE UNA RED FÍSICA

12. Este caso de uso es compatible con el anterior, siendo una funcionalidad añadida que se explota en determinados entornos con la intención de crear redes aisladas/segregadas de forma virtual.
13. Las Redes de Área Local Virtuales (VLAN) son redes lógicas independientes configuradas dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. En este caso de uso, el conmutador o *switch* se utiliza para la creación de varias redes VLAN permitiendo el aislamiento de las redes virtuales (A, B y C en el ejemplo) o bien la interconexión sólo de aquellas que se desee.

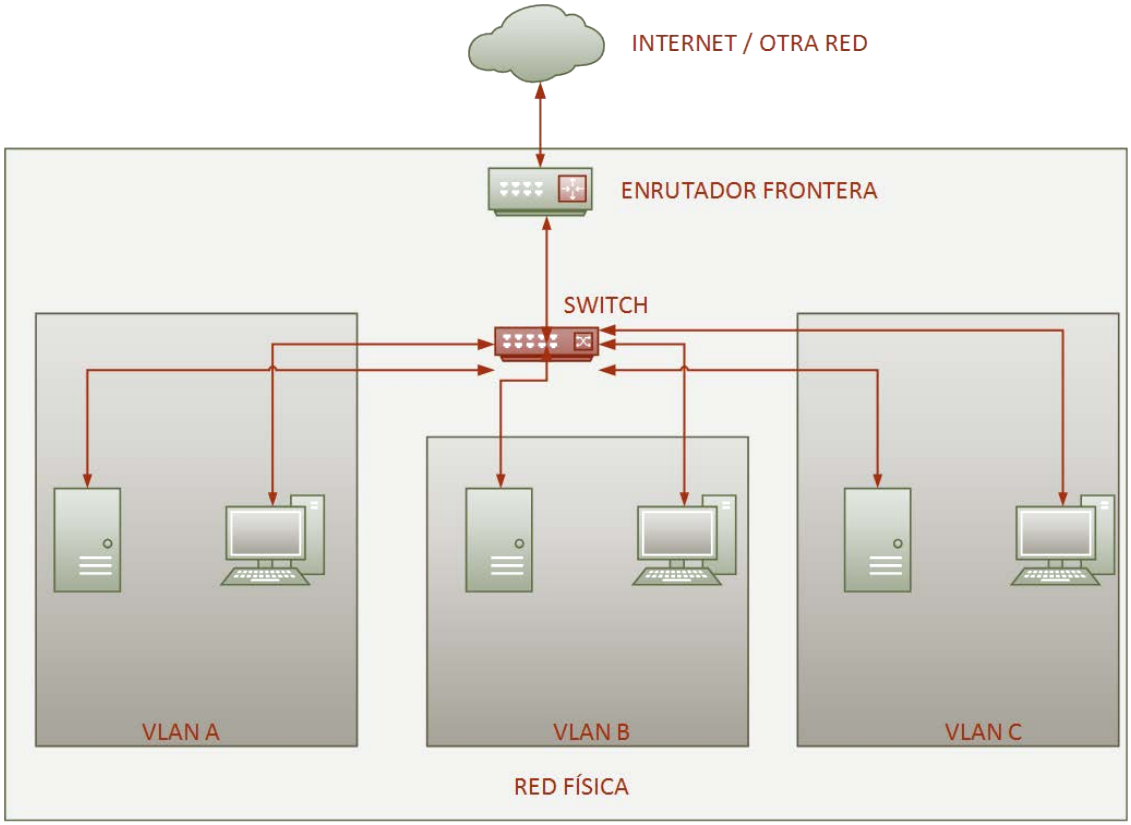

Figura 1 – Ejemplo de Caso de Uso 2: Creación de VLANs

2.2 ENTORNO DE USO

14. Este tipo de dispositivos son de uso generalizado en cualquier tipo de ámbito, debido a su trascendencia para la implementación de redes informáticas y de comunicaciones, tanto en el caso de redes desplegadas para usuarios privados, empresas u organismos del sector público.

15. Para la utilización en condiciones óptimas de seguridad de estos dispositivos, es necesario que se integre 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 la conmutación de redes 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 producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **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.
- **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.

2.3 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

16. Este tipo de productos se presentan en formato de **Equipo dedicado** o (***Appliance*****:** hardware provisto de firmware 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 4, éstas quedan fuera del alcance analizado, debiendo ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.4 CERTIFICACIÓN LINCE

17. 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.
18. En el caso de que el producto incluya funcionalidades de enrutador, se permite que la certificación Nacional Esencial de Seguridad (LINCE)[5] incluya los RFS reflejados en el presente documento y se añadan los RFS incluidos en el anexo D1.M: Enrutadores de la guía CCN-STIC 140 *Taxonomías de referencia para productos de seguridad TIC*.
19. 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)
[5] 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

20. 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

21. 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)

22. 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.
23. **REQ. 1.** El producto debe de definir al menos el rol de administrador (A.NOAUT).
24. **REQ. 2.** El Producto debe ser capaz de asociar un usuario con un rol (A.NOAUT).
25. **REQ. 3.** El producto debe ser capaz de realizar la gestión de las siguientes funcionalidades del producto: (A.NOAUT).
    - 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.
26. **REQ. 4.** Sólo podrán realizar actualizaciones de seguridad de forma manual usuarios con rol de administrador (A.NOAUT).
27. **REQ. 5.** El producto debe de identificar y autenticar a cada usuario antes de permitir acciones que modifiquen la configuración del producto (A.NOAUT).
28. **REQ. 6.** El producto debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad (A.NOAUT).
29. **REQ. 7.** El producto debe ser capaz de proveer un canal de comunicación seguro entre entidades autorizadas (ej. Servidor de auditoría), a un administrador remoto autorizado y sí mismo a través de IPSec, SSH, TLS 1.2 o superior, DTLS y/o HTTPS. (A.NOAUT, A.CIFRA,)
30. **REQ. 8.** El producto debe permitir comunicaciones a través de canales seguros iniciadas por sí mismo o por entidades autorizadas (A.COM).
31. **REQ. 9.** El producto hará uso de certificados X.509v3 para la autenticación cuando utilice cualquiera de estos protocolos (A.COM).
32. **REQ. 10.** El producto debe soportar el uso de suites de cifrado compuestas únicamente por funciones y algoritmos criptográficos aceptados, como mínimo, para Categoría Media del ENS según la guía CCNSTIC-807, así como proporcionar capacidades de configuración que permitan obligar el uso de estas suites exclusivamente (A.CIFRA. A.COM).
33. **REQ. 11** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas) (A.CIFRA. A.COM).

34. **REQ. 12.** Generador de bits aleatorios. En caso de suministrar un servicio de generación de bits aleatorios (RBG[6]) determinísticos, el producto deberá (A.CIFRA):
    - Utilizar Hash_DRBG (any), HMAC_DRBG (any) o CTR_DRBG (AES).
35. **REQ. 13** 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 (A.CIFRA).
36. **REQ. 14.** 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. (A.ACT).
37. **REQ. 15.** El producto debe ofrecer la posibilidad de consultar la versión actual del firmware/software (A.ACT).
38. **REQ. 16.** El producto debe ofrecer la posibilidad de iniciar actualizaciones de forma manual y de comprobar si existen nuevas actualizaciones disponibles (A.ACT).
39. **REQ. 17.** 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.AUD):
    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.
40. **REQ. 18.** El producto debe generar los registros de auditoría junto con, al menos, la fecha, hora, tipo de evento y resultado (A.AUD).
41. **REQ. 19.** El producto debe ser capaz de transmitir la información de auditoría a una entidad externa usando un canal seguro (según párrafo 27) (A.AUD).
42. **REQ. 20.** El producto debe ser capaz de almacenar la información de auditoría generada en sí mismo (A.AUD).
43. **REQ. 21.** El producto debe ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno (A.AUD).
44. **REQ. 22** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: Sólo usuarios autorizados.
    b) Modificación: Ningún usuario.
    c) Borrado: Administradores.

[6] *Random Bit Generator*

45. **REQ. 23.** El producto debe proteger las credenciales de autenticación, claves o información sobre las claves (A.CRED).
46. **REQ. 24.** El producto debe disponer de la capacidad de gestión de las contraseñas (A.CON):
    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 [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]
47. **REQ. 25.** El producto debe permitir el establecimiento de un número determinado de intentos fallidos de autenticación (A.CON).
48. **REQ. 26.** Cuando se alcance el número de intentos fallidos debe impedirse que el usuario pueda autenticarse con éxito (A.CON).
49. **REQ. 27.** El producto no debe almacenar contraseñas en texto plano (A.CON).
50. **REQ. 28.** El producto debe evitar que se lean contraseñas en texto plano (A.CON).
51. **REQ. 29.** 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 (A.FUN).

4.1 SWITCH

52. **REQ. 30.** El producto debe de ser capaz de administrar puertos, habilitándolos o deshabilitándolos para su uso, así como asignándoles prioridades (A.FUN).
53. **REQ. 31.** El producto debe reenviar el tráfico de red a través de sus puertos a nivel de de enlace (capa 2) del modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1)[7] según direccionamiento físico o Media Access Control (MAC[8]) de Ethernet.
54. **REQ.30.** El producto debe tener la capacidad de segmentación de redes virtuales (VLAN[9]).

[7] Modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1) es un modelo de referencia para los protocolos de la red de arquitectura en capas creado por la Organización Internacional de Normalización (ISO) y la Comisión electrotécnica Internacional (IEC).
[8] *Media Access Control*
[9] *Virtual Local Area Network*

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*
RFS	Requisitos Fundamentales de Seguridad