centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo D.11: Redes Definidas por *Software* (SDN)

Junio 2021

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

© Centro Criptológico Nacional, 2021
NIPO: 083-21-130-1

Fecha de Edición: junio de 2021

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 16:44:44 +02'00'

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN Y OBJETO 4
2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS 5
2.1 FUNCIONALIDAD 5
2.2 CASOS DE USO 6
2.2.1. CASO DE USO 1. PRODUCTO BASADO EN *SOFTWARE* 6
2.2.2. CASO DE USO 2. PRODUCTO *HARDWARE* Y *SOFTWARE* 7
2.3 ENTORNO DE USO 7
2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO 8
2.5 ALINEAMIENTO CON CRITERIOS COMUNES (*COMMON CRITERIA*) 8
3. ANÁLISIS DE AMENAZAS 9
3.1 RECURSOS QUE ES NECESARIO PROTEGER 9
3.2 AMENAZAS 9
4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS) 10
4.1 ADMINISTRACIÓN CONFIABLE 10
4.2 IDENTIFICACIÓN Y AUTENTICACIÓN 10
4.3 AUDITORÍA 11
4.4 CANAL SEGURO 11
4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES 12
4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES 12
4.7 REQUISITOS CRIPTOGRÁFICOS 12
4.8 SWITCHING LÓGICO 13
4.9 FIREWALL LÓGICO 13
5. ABREVIATURAS 15

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Redes Definidas por Software (SDN)** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos y Servicios 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 ALTA**. 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 **Redes Definidas por *Software* (SDN)** 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. La tecnología de **Redes Definidas por *Software*** (*Software-Defined Networking*) o **SDN** permite centralizar la lógica asociada al control de las redes de comunicaciones, desarrollar aplicaciones para programar dichas redes, y automatizar los procesos operativos de red.
7. En SDN se separa físicamente el plano de encaminamiento de paquetes o plano de datos (*forwarding o data plane*) del plano de control (*control plane*). Esto difiere de las redes tradicionales, donde ambos planos coexisten en un mismo elemento de red.
8. El plano de control está compuesto por uno o varios componentes denominados **controladores**. Esto permite la gestión y el control de la red mediante *software*. Los equipos de red del plano de datos únicamente se encargan de gestionar el tráfico en base a las órdenes recibidas del plano de control.
9. Un concepto muy relacionado con SDN es el de **Virtualización de Funciones de Red** (*Network Function Virtualization*) o **NFV**. Esta tecnología se basa en la virtualización de los diferentes elementos de una red (enrutadores, switches, cortafuegos, etc.), sirviéndose del *hardware* de red correspondiente a la capa de datos, para la implementación de dichos elementos o funciones de red.
10. Habitualmente, SDN y NFV se usan conjuntamente, con productos e infraestructuras basados en ambos paradigmas. Es común su integración con otros productos de virtualización, como hipervisores.
11. A continuación, se describen las funcionalidades principales de los productos de esta familia.

    a) Proporcionar a las aplicaciones una red de comunicaciones programable y configurable de forma centralizada, ofreciendo integración con elementos como hipervisores y orquestadores *cloud*, así como una API para el desarrollo de aplicaciones.

    b) Proteger las máquinas y aplicaciones que hagan uso de la red, proporcionando servicios de protección de datos, cortafuegos, etc. Esto se lleva a cabo mediante la aplicación de políticas que prevengan ante actividad maliciosa, tanto para el tráfico intercambiado entre las máquinas conectadas a la red, como para el tráfico intercambiado con el exterior.

    c) Definir grupos de máquinas en base a la aplicación o aplicaciones que ejecutan. Por ejemplo, una máquina que ejecute un servidor web con una máquina que contenga la base de datos asociada a esa aplicación web. Esto permite definir, a su vez, entornos de red para dichos grupos, como VLANs y redes privadas, aislándose del resto de máquinas conectadas a la red.

d) Automatizar procesos de gestión, despliegue y configuración de red, reduciendo la necesidad de realizar configuraciones manuales en los equipos que conforman la red.

2.2 CASOS DE USO

12. En base a las funcionalidades y características del producto, se contemplan dos (2) casos de uso para esta familia de productos, tal y como se definen a continuación.

2.2.1. CASO DE USO 1. PRODUCTO BASADO EN *SOFTWARE*

13. El producto está compuesto por uno o varios componentes *software*. Estos componentes controlan el plano de datos, compuesto por equipos de red *hardware,* encargados del manejo del tráfico y que no forman parte del producto. Estos equipos pueden ser switches y routers tradicionales, o equipos diseñados para trabajar en entornos SDN.

14. El producto también se integra con aplicaciones y servicios, o un hipervisor que soporta las máquinas virtuales donde se ejecutan las diferentes aplicaciones que hacen uso de la red. En muchos casos, el propio producto se puede ejecutar en una o varias máquinas virtuales soportadas por dicho hipervisor.

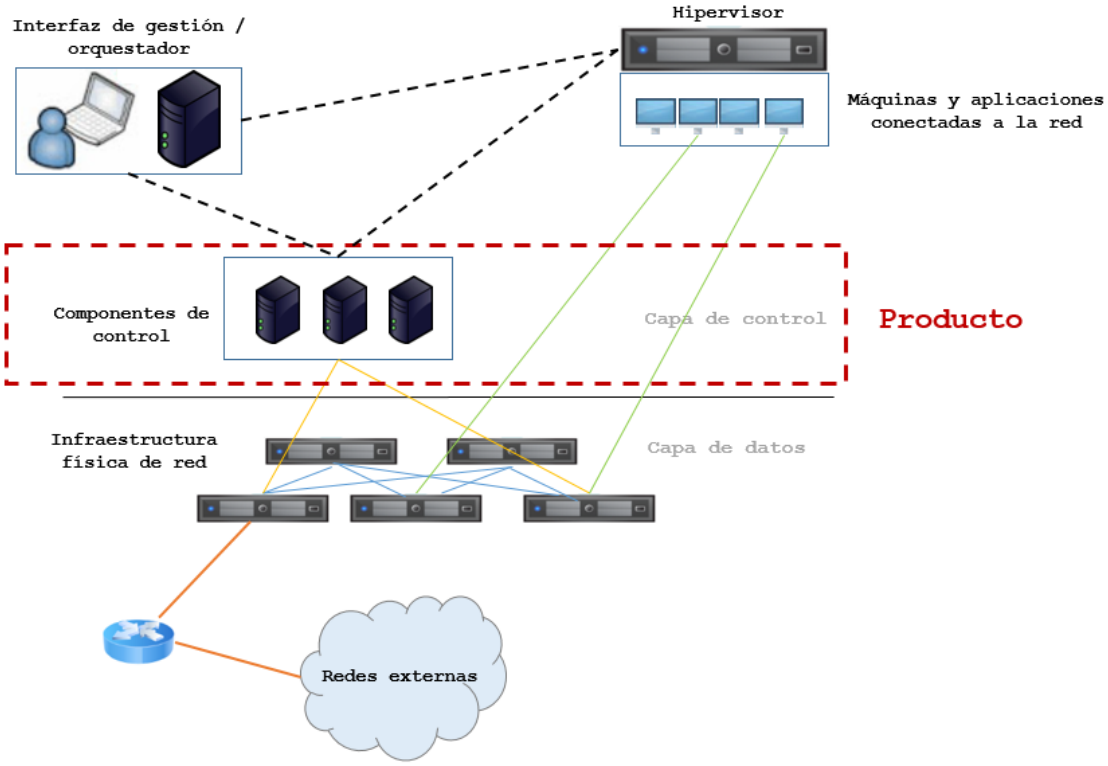

Figura 1: Producto basado en *software*

2.2.2. CASO DE USO 2. PRODUCTO *HARDWARE* Y *SOFTWARE*

15. El producto está compuesto por la infraestructura de red *hardware*, formando una red mallada programable, y por componentes *software* encargados de su control y programación.
16. Al igual que en el caso de uso anterior, el producto se puede integrar y comunicar con hipervisores que soportan máquinas virtuales conectadas a la red.

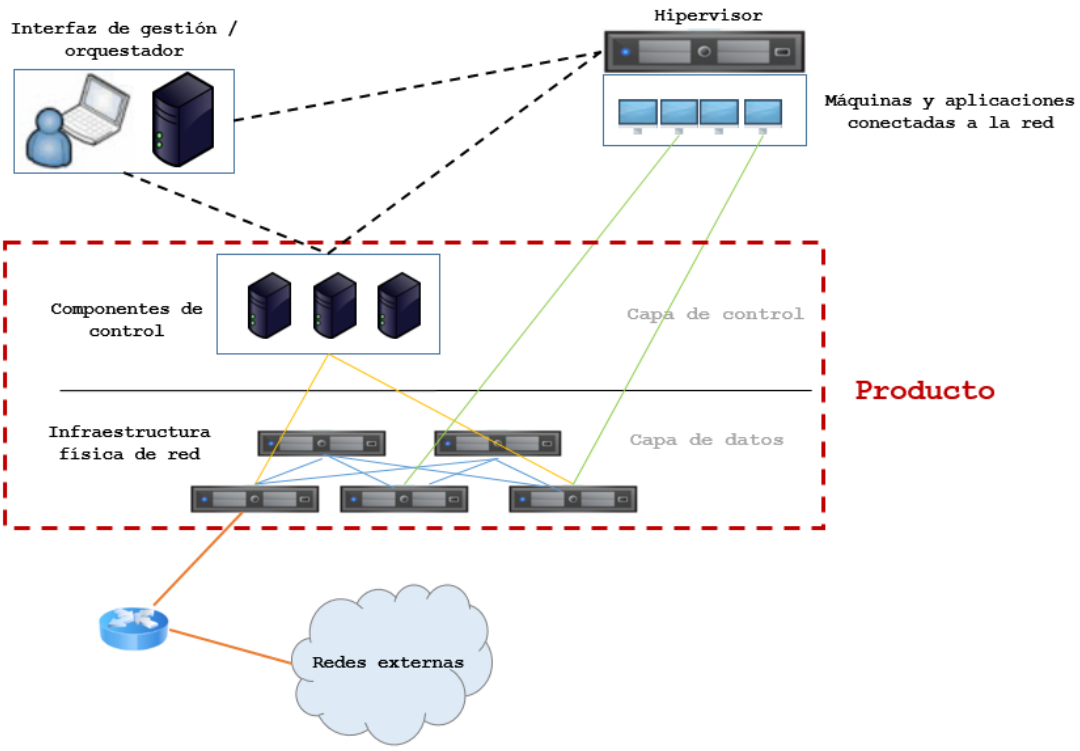

Figura 2: Producto basado en hardware y software

2.3 ENTORNO DE USO

17. Estos productos son habitualmente usados en entornos de Centros de Datos (*Data Centers*). Su uso proporciona una importante reducción de costes al operador del centro de datos, ya que permite un mejor aprovechamiento de los recursos, así como la automatización de procesos de despliegue, mantenimiento y configuración de red.
18. Para la utilización en condiciones óptimas de seguridad de los productos de **Redes Definidas por Software (SDN)**, es necesario que se integren en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:
    - **Plataforma segura:** El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.

- **Protección física:** Los componentes del producto deberán instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.

- **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 maliciosa.
- **Flujo de información en red:** El intercambio de información en la red deberá ser controlado por el producto, mediante la configuración y aplicación de políticas de filtrado de tráfico.
- **Actualizaciones periódicas:** El *software* del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

19. Estos productos constan de varios componentes, que en función del tipo de producto pueden ser sólo *software*, o tanto *software* como *hardware*. Suelen desplegarse en entornos de centros de datos, integrándose con otras soluciones de virtualización.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (*COMMON CRITERIA*)

20. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos TIC (Tecnologías de la Información y de las Comunicaciones).
21. En el ámbito de CC se definen un conjunto de objetivos y requisitos de seguridad, tanto funcionales (*SFR, Security Functional Requirements*) como de evaluación (*SAR, Security Assurance Requirements*), independientes de la implantación, que cada producto incluirá dentro de su declaración de seguridad (*ST, Security Target*).
22. **Los productos dentro de esta familia, deberán disponer de una declaración de seguridad (ST) certificada con un nivel de confianza EAL2 o superior (*Evaluation Assurance Level*), que contenga los SFR indicados en el apartado 4.**
23. En caso de que alguno de los requisitos indicados en dicho apartado 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

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

- Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos.
- Funcionalidad del producto, y datos de configuración y auditoría generados por éste.
- Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad.
- Flujos de tráfico entre las distintas máquinas conectadas al producto, y con el exterior.

3.2 AMENAZAS

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

- **A.RED. Ataque a la red.** Un atacante, desde dentro o desde fuera de la red, podría acceder y/o modificar la información intercambiada entre el producto y otras entidades autorizadas o entre los distintos módulos del producto.
- **A.LOCAL. Ataque local.** Un atacante podría actuar a través de software no privilegiado ejecutado en la misma plataforma de computación donde se ejecuta el producto. Los atacantes podrían modificar de forma maliciosa los ficheros o comunicaciones que utiliza el producto.
- **A.REST. Acceso a información almacenada.** Un atacante podría acceder a información sensible almacenada en la plataforma en la que se instala y ejecuta el producto.
- **A. SEG. Acceso a las funciones de seguridad.** Un atacante podría acceder y modificar las funciones y datos de seguridad del producto.
- **A.NODET. Actividad no detectada.** Un atacante podría acceder, cambiar o modificar la funcionalidad de seguridad de la herramienta sin que esto sea apreciado por el administrador.
- **A.TRAF. Tráfico no autorizado**. Uno o varios de los endpoints conectados a la red podrían realizar intercambios de tráfico no autorizado con otras máquinas y aplicaciones o con el exterior, lo que podría ser aprovechado por un atacante para explotar vulnerabilidades.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

26. 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 ADMINISTRACIÓN CONFIABLE

27. Estas funcionalidades de seguridad mitigan la amenaza (A.SEG). **Podrán ser cubiertos por el producto o por su entorno operacional**.

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

29. **ADM.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.

    Nota de aplicación: En este punto se espera que el fabricante enumere todas las tareas de administración que puedan ser realizadas.

30. **ADM.3** El producto deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones anteriormente descritas (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 funcionales para las que tengan permiso.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

31. Estas funcionalidades de seguridad mitigan la amenaza (A.REST, A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**

32. **IAU.1.** El producto deberá identificar y autenticar a cada usuario antes de otorgar acceso.

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

34. **IAU.3.** El producto deberá proteger de lectura y modificación no autorizada las credenciales de autenticación.

35. **IAU.4.** El producto deberá disponer de la capacidad de gestión de las contraseñas:

a) La contraseña debe 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 producto implemente otros mecanismos de autenticación. Será estudiado caso por caso.

36. **IAU.5.** El producto debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad.

4.3 AUDITORÍA

37. Estas funcionalidades de seguridad mitigan la amenaza (A.NODET).
38. **AUD.1.** El producto deberá generar registros 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 personal autorizado.
    b) Cambios en las credenciales de usuarios.
    c) Cambios en la configuración del producto.
    d) Eventos relativos a la funcionalidad del producto
39. **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 (si aplica).
40. **AUD.3.** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: usuarios autorizados.
    b) Modificación: Ningún usuario.
    c) Borrado: administradores.
41. **AUD.4.** El producto debe ser capaz de almacenar la información de auditoría generada en sí mismo o en una entidad externa.
42. **AUD.5.** El producto debe ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno.

4.4 CANAL SEGURO

43. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).
44. **COM.1.** El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas o entre distintas partes del producto empleando funciones, algoritmos y protocolos que estén de acuerdo a

lo establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.).

45. **COM.2** El TOE debe permitir que estos canales de comunicación seguros sean iniciados por él mismo o por entidades autorizadas.
46. **COM.3** El producto hará uso de certificados digitales para la autenticación cuando utilice cualquiera de estos protocolos.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

47. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL).
48. **ACT.1** El producto ofrecerá la posibilidad de consultar la versión actual del firmware/software, iniciar actualizaciones manualmente y comprobar si existen nuevas actualizaciones disponibles**.**
49. **ACT.2** El producto deberá 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.
50. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.
51. **ACT.5** En caso de tratarse de un producto *software*, este deberá estar empaquetado de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).
52. **ACT.6** En caso de tratarse de un producto *software*, este no descargará ni modificará su propio código binario.
53. **ACT.7** En caso de tratarse de un producto *software*, este solamente utilizará las bibliotecas de terceras partes declaradas por el fabricante

4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

54. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional.**
55. **CRD.1.** En el caso en que el producto almacene credenciales y/o datos sensibles, éstos no deberán almacenarse en claro.

4.7 REQUISITOS CRIPTOGRÁFICOS

56. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.REST).
57. **CIF.1** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos criptográficos que estén incluidas entre las autorizadas para categoría ALTA del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.
58. **CIF.2** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).

4.8 SWITCHING LÓGICO

59. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.TRAF).

60. **SWI.1**. Listas blancas de IPs y MAC Addresses. El producto debe permitir establecer de forma manual las IPs y/o MACs que se usarán a modo de lista blanca en un puerto lógico. Es decir, por ese puerto lógico solo podrá existir tráfico desde y hacia las IPs / MACs definidas. El resto será descartado.

61. **SWI.2**. Limitación de ancho de banda por puerto lógico. El producto debe permitir limitar el ancho de banda del tráfico generado por puerto lógico. El objetivo es la protección frente a ataques cuyo objetivo sea inundar de tráfico la red (*flooding*).

62. **SWI.3**. El producto debe tener la capacidad de segmentación de redes virtuales (VLAN).

63. **SWI.4**. El producto debe permitir filtrar el tráfico no IP en la red.

64. **SWI.5**. Filtrado BPDU. El producto debe permitir el filtrado de tramas BPDU[1], así como la especificación de listas blancas con las direcciones MAC origen que sí podrán enviar estas tramas BPDU. El objetivo es la protección frente a tramas BPDU que podrían proporcionar información maliciosa a los switches lógicos.

65. **SWI.6**. Filtrado DHCP. El producto debe permitir el filtrado de tráfico DHCP, tanto de tramas DHCP cliente, correspondientes a máquinas que solicitan de forma dinámica una IP, como de tramas DHCP servidor correspondientes a respuestas de un servidor DHCP a peticiones de IPs dinámicas. El objetivo es la protección frente a DHCP spoofing.

66. **SWI.7**. Filtrado de mensajes *ICPMv6 Router Advertisement*. El producto debe permitir filtrar los mensajes ICMPv6 type 134 (*Router Advertisement*)[2]. El objetivo es la protección frente a entidades ilegítimas que se hagan pasar por routers para redireccionar tráfico.

4.9 FIREWALL LÓGICO

67. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.TRAF).

68. **FRW.1** El producto debe permitir la configuración y aplicación de *políticas de seguridad* para gobernar el tráfico de red que lo atraviesa. Las políticas permitirán la configuración de *reglas de seguridad* por parte de los administradores a través de las que se tomará la decisión de transferir los paquetes de un interfaz a otro, o realizar otras acciones.

[1] Los switches de una red LAN que utilizan el *Spanning Tree Protocol (STP)* necesitan intercambiar información entre ellos para el funcionamiento correcto de este protocolo. Esta información se intercambia a través de las tramas BPDU (*Bridge Protocol Data Units*). Los switches envían las tramas BPDU a direcciones multicast, usando como origen la dirección MAC de su puerto.

[2] *ICMPv6 Router Advertisement* son mensajes ICMP empleados para anunciarse como router operacional dentro de una subred IPv6.

69. **FRW.2.** Las reglas de seguridad podrán definirse en función de, al menos, los siguientes atributos de la información: direcciones origen y destino, puertos origen y destino, y protocolo. También deben poder configurarse en función del tipo de aplicación (L7).

70. **FRW.3** En función de las reglas configuradas, se podrán lanzar las acciones especificadas por el administrador. Al menos, las acciones de permitir y denegar el tráfico.

71. **FRW.4** El producto sólo permitirá la configuración de políticas y reglas para el control de flujo de información a administradores autorizados.

72. **FRW.5** El producto permitirá la creación de listas blancas (explícitamente autorizadas) y negras (explícitamente denegadas). Estas listas podrán basarse en direcciones IP, protocolo, servicio, etc.

73. **FRW.6**. El producto deberá permitir realizar *rollback* al aplicar una política. Es decir, poder revertir al estado anterior a la aplicación de una política.

74. **FRW.7** El producto permitirá aplicar las políticas a nivel del primer punto de contacto del *endpoint* con la red. Es decir, la política podrá ser aplicada (*enforcement*) a nivel de VNIC (*Virtual Network Interface Cards*) o de puerto físico al que se conecta el endpoint. Esto permitirá micro segmentación (*Zero Trust*).

75. **FRW.8** El producto permitirá crear zonas completamente aisladas dentro de la red. Estas zonas tendrán, asociados en exclusividad, los componentes físicos que las conforman (hipervisores, switches físicos, agentes instalados en sistemas operativos, etc.).

5. ABREVIATURAS

API	*Application Programming Interface*
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
NFV	*Network Function Virtualization*
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SDN	*Software-defined Networking*
SFR	*Security Functional Requirements*
TOE	*Target of Evaluation*
URL	*Uniform Resource Locator*

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