centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 140

# Taxonomía de referencia para productos y servicios de Seguridad TIC


Septiembre de 2023

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
Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2023

CCN 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
2023.09.19 13:22:21 +02'00'

NIPO: 083-23-071-5
Fecha de Edición: septiembre de 2023

# ÍNDICE

# 1. INTRODUCCIÓN

1. La adquisición de un producto de seguridad TIC que va a manejar información nacional clasificada o información sensible debe estar precedida de un proceso de comprobación de que los mecanismos de seguridad implementados en el producto son adecuados para proteger dicha información.

2. La evaluación y certificación de un producto de seguridad TIC es el único medio objetivo que permite valorar y acreditar la capacidad de un producto para manejar información de forma segura. En España, esta responsabilidad está asignada al Centro Criptológico Nacional (CCN) a través del RD 421/2004 de 12 de marzo en su Artículo 1 y en su Artículo 2.1, el cual establece que el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y comunicaciones y la autoridad de certificación criptológica.

3. Así mismo, dentro del RD 311/2022 de 3 de mayo por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración electrónica, se indica que el Organismo de Certificación del CCN será el responsable de determinar los requisitos exigibles a cada producto o servicio de Seguridad TIC en materia de certificaciones y/o evaluaciones adicionales.

4. En base a estas competencias, el CCN publica la guía **CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)** [1]. Este catálogo tiene como finalidad ofrecer a los organismos de la Administración un conjunto de productos o servicios STIC de referencia, cuyas funcionalidades de seguridad relacionadas con el objeto de su adquisición han sido certificadas.

5. De esta forma, el CPSTIC permite proporcionar un nivel mínimo de confianza al usuario final en los productos o servicios adquiridos, en base a las mejoras de seguridad derivadas del proceso de evaluación y certificación y a un procedimiento de empleo seguro.

6. El CPSTIC consta de tres (3) partes: Productos Aprobados, Productos y Servicios Cualificados y Productos y Servicios de Conformidad y Gobernanza de la Seguridad[1].

7. En el apartado de **Productos Aprobados** se recogen aquellos productos que se consideran adecuados para el manejo de información clasificada.

8. En el apartado de **Productos Cualificados** se incluyen aquellos que cumplen los requisitos de seguridad exigidos para el manejo de información sensible en el ENS, en cualquiera de sus categorías (ALTA, MEDIA y BÁSICA).

9. En el apartado **Productos de Conformidad y Gobernanza de la Seguridad** se engloban las herramientas de gobernanza y planificación de la seguridad, las herramientas de normativa y conformidad y, por último, las herramientas de análisis y gestión de riesgos. Se trata de productos que no encajan en las familias

[1] Aunque en el CPSTIC se recogen Productos y Servicios Cualificados o Productos y Servicios de Conformidad y Gobernanza de la Seguridad, por economía del lenguaje, de aquí en adelante hablaremos de Productos Cualificados o Productos **de Conformidad y Gobernanza de la Seguridad**.

de productos definidas en la taxonomía de productos aprobados y cualificados, al tratarse de productos que no pertenecen a la arquitectura de seguridad del sistema.

| TIPO DE PRODUCTO O SERVICIO | INFORMACIÓN QUE MANEJA |
|---|---|
| **APROBADO** | CLASIFICADA |
| **CUALIFICADO** | SENSIBLE (ENS) |
| **CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD** | CUALQUIER TIPO |

**Tabla 1. Tipos de productos incluidos en el CPSTIC**

10. Para la inclusión de un producto en el catálogo, el CCN tendrá en cuenta los siguientes criterios:

    a) En el caso **Productos Aprobados** para el manejo de información clasificada, el máximo nivel de clasificación de la información que puede manejar (DIFUSIÓN LIMITADA, CONFIDENCIAL, RESERVADO, SECRETO).

    b) En el caso de **Productos Cualificados**, la máxima categoría del sistema de información en el que puede emplearse (ALTA, MEDIA, BÁSICA[2]).

    c) Las funcionalidades de seguridad que implementa el producto y las certificaciones aportadas.

    d) Otros aspectos como el análisis de riesgos del producto o sistema, la necesidad operativa dentro de la Administración, la disponibilidad o no de otros productos certificados que satisfagan la misma funcionalidad, etc.

11. En función de esta información, se determinarán las pruebas o evaluaciones que deberá superar el producto de seguridad TIC correspondiente.

12. El procedimiento para la inclusión en el CPSTIC de un producto STIC aprobado para manejar información nacional clasificada se describe en la guía **CCN-STIC 102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada** [2]. Los requisitos exigidos, la relación de la documentación y el equipamiento a aportar para realizar la evaluación criptológica se describe en la **CCN-STIC 130 Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada** [3] y para realizar la evaluación TEMPEST se describe en la guía **CCN-STIC 151 Evaluación y Clasificación TEMPEST de equipos** [4]. Ver Figura 1. Inclusión de productos de seguridad en el CPSTIC.

[2] Clasificación por categorías definida en el ENS.

13. Así mismo, el procedimiento para la inclusión de un producto STIC aprobado en el CPSTIC para manejar información nacional clasificada se describe en la **guía CCN-STIC 102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada** [2]. Los requisitos exigidos, la relación de la documentación y el equipamiento a aportar para realizar la evaluación criptológica se describe en la CCN-STIC 130 Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada [3] y para realizar la evaluación TEMPEST se describe en la guía CCN-STIC 151 Evaluación y Clasificación TEMPEST de equipos [4]. Ver Figura 1.

14. El producto o servicio STIC cualificado o aprobado por el CCN hará referencia a una versión concreta y con una configuración determinada, de acuerdo a unas normas de utilización que serán descritas en un Procedimiento de Empleo Seguro (PES). Dicho PES será distribuido por la empresa fabricante junto con el producto y además se publicará como una guía CCN-STIC de la serie 1000.

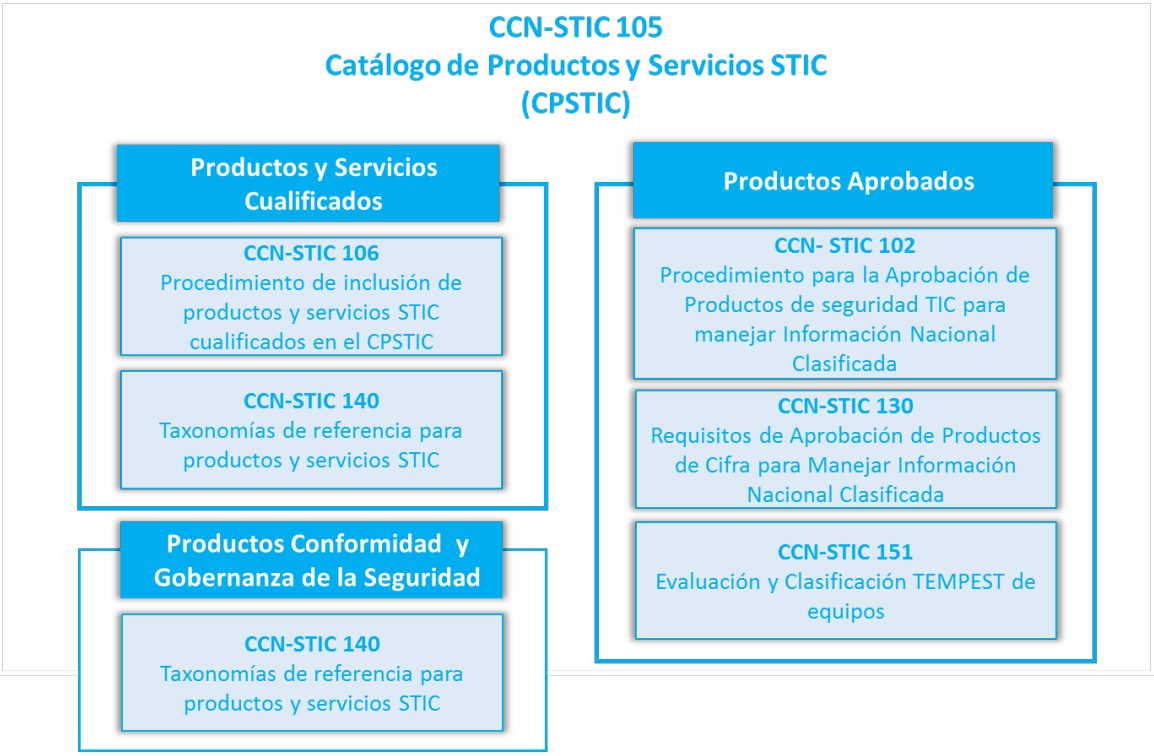


**Figura 1. Clasificación del CPSTIC**

## 2. OBJETIVO

15. El objeto de este documento es establecer una taxonomía para la clasificación de productos de Seguridad en las Tecnologías de Información y la Comunicación (TIC) en torno a diversas familias, e identificar su ámbito y alcance, con el objeto de que sirva como base para clasificar los productos incluidos en el CPSTIC.

16. Además, en cada uno de los Anexos de este documento se incluyen los Requisitos Fundamentales de Seguridad (RFS), definidos para cada familia, que serán exigidos a cada producto que desee ser incluido en el CPSTIC.

## 3. ALCANCE

17. La taxonomía descrita en el presente documento se divide en tres (3) partes. Las dos primeras (**Taxonomía de Productos y Servicios Cualificados y Aprobados**) establecen una clasificación de aquellos productos TIC que forman parte de la arquitectura de seguridad de los sistemas TIC, es decir, aquellos que desarrollan su actividad en el contexto operacional de éste, e implementan funcionalidades que permiten incrementar el nivel de seguridad del sistema en alguna de sus dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad).

18. También se incluirán productos cuya funcionalidad principal no esté relacionada con la seguridad pero que sí implementen funcionalidades de seguridad críticas dentro del sistema, como sería el caso de enrutadores, sistemas operativos, dispositivos móviles, etc.

19. En la tercera parte (**Taxonomía de Productos y Servicios de Conformidad y Gobernanza de la Seguridad**) se incluirán productos que no están contemplados en las dos anteriores, dado que no forman parte de la arquitectura de seguridad del sistema, pero que implementan funcionalidades que facilitan el cumplimiento con la normativa de seguridad. En este grupo estarían, por ejemplo, herramientas de auditoría, análisis de riesgos o bastionado de sistemas/equipos.

20. Los productos incluidos en cada familia de la taxonomía podrán ser implementados, salvo indicación expresa en contra, en equipamiento hardware, aplicación *software* o lógica para circuitos integrados (*firmware*).

# 4. TAXONOMÍA DE PRODUCTOS CUALIFICADOS

## 4.1 TAXONOMÍA: ESTRUCTURA

21. Con objeto de que el Catálogo sirva como instrumento de referencia para cubrir las necesidades por parte de la Administración Pública de cumplir con la normativa de seguridad y, en particular, con el Esquema Nacional de Seguridad (ENS), la estructura de la taxonomía se organiza en base a las medidas de seguridad definidas en el Anexo II del Real Decreto 311/2022 de 3 de mayo por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración electrónica[3].

22. La taxonomía se divide en familias que han sido definidas, con la intención de adaptarse a los futuros cambios que se puedan producir en el mercado de los productos STIC

23. Una familia agrupa productos de seguridad atendiendo a su funcionalidad básica (p.ej.: enrutador, cortafuegos, proxy, herramienta de borrado seguro, etc.). Dichos productos pueden contribuir en la implementación de algunos de los requisitos de seguridad recogidos en las medidas del Anexo II del ENS. Estas medidas se encuentran referenciadas al lado de cada familia mediante su identificador (p.ej.: [op.exp.N] cubre el requisito "N" de las medidas de explotación dentro del marco operacional).

24. De acuerdo a esta estructura, podría darse el caso de que un producto se encuadre en una o en varias familias complementarias siempre que implemente las funcionalidades propias de todas ellas. Esto es cada vez más habitual, dado que las empresas que desarrollan productos de seguridad tienden hacia un enfoque "*todo-en-uno*" mediante paquetes de aplicaciones o equipos dedicados (*suites/appliances*) que cubren varias funcionalidades de seguridad en un único dispositivo o sistema.

25. Para cada familia de productos de la taxonomía se ha definido un documento de Requisitos Fundamentales de Seguridad (RFS), que deberían tomarse como referencia para el desarrollo, evaluación y uso seguro de los productos dentro de cada familia. Estos RFS se incluyen en los anexos de esta guía.

## 4.2 TAXONOMÍA: ESQUEMA

26. La Tabla 2 recoge el esquema de la taxonomía organizada en base a las medidas de seguridad recogidas en el Anexo II del ENS en las que podrían contribuir a su cumplimiento los productos asociados a cada familia, así como la relación de anexos a este documento, donde se recogen los Requisitos Fundamentales de Seguridad (RFS) exigidos para cada familia de productos y en función de la categoría del sistema (MEDIA o ALTA) en el que van a ser utilizados.

[3] https://www.boe.es/eli/es/rd/2022/05/03/311

| MEDIDAS DE SEGURIDAD | FAMILIAS | | | |
|---|---|---|---|---|
| | NOMBRE | MEDIDAS | ANEXOS | |
| | | | ENS ALTO | ENS MEDIO |
| **Control de acceso [op.acc]** | Control de Acceso a Red (NAC[4]) | [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7] | A.1 | A.1M |
| | Dispositivos Biométricos | [op.acc.1]; [op.acc.2]; [op.acc.5] | A.2 | |
| | Dispositivos *Single Sign-On* | [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7] | A.3 | |
| | Servidores de Autenticación | [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7] | A.4 | A.4M |
| | Dispositivos *One-Time Password* | [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7] | A.5 (*) | |
| | Gestión de Acceso Privilegiado (PAM[5]) | [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7] | A.6 | A.6M |
| | Gestión de Identidades (IM[6]) | [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7] | A.7 | A.7M |

[4] *Network Access Control*
[5] *Privileged Access Manager*
[6] *Identity Management*

| MEDIDAS DE SEGURIDAD | FAMILIAS | | | |
|---|---|---|---|---|
| | NOMBRE | MEDIDAS | ANEXOS | |
| | | | ENS ALTO | ENS MEDIO |
| **Seguridad en la explotación [op.exp]** | Anti-virus/EPP (*Endpoint Protection Platform*) | [op.exp.6] | B.1 | B.1M |
| | EDR (*Endpoint Detection and Response)* | [op.exp.6] | B.2 | B.2M |
| | Herramientas de gestión de red | [op.exp.3]; [op.exp.7] | B.3 | B.3M |
| | Herramientas de actualización de sistemas | [op.exp.4]; [op.exp.5] | B.4 | |
| | Herramientas de filtrado de navegación | [op.exp.6] | B.5 | B.5M |
| | Sistemas de gestión de eventos de seguridad (SIEM) | [op.exp.8]; [op.exp.9]; [op.exp.10] | B.6 | B.6M |
| | Dispositivos para gestión de claves criptográficas | [op.exp.11] | B.7(*) | NA |
| | Herramientas de gestión de dispositivos (UEM) | [op.exp.3] | B.8 | NA |
| | Sistemas de orquestación, automatización y respuesta de seguridad (SOAR) | [op.exp.8]; [op.exp.9]; | B.9 | B.9M |
| **Monitorización de la seguridad [op.mon]** | IDS, IPS y AntiDDoS | [op.mon.1] | C.1 | C.1M |
| | Sistemas *Honeypot / Honeynet* | [op.mon.1] | C.2 | |
| | Captura, Monitorización y Análisis de Tráfico | [op.mon.1] | C.3 | C.3M |
| | Herramientas de *sandbox* | [op.mon.1] | C.4 | C.4M |

| MEDIDAS DE SEGURIDAD | FAMILIAS | | | | |
|---|---|---|---|---|---|
| | NOMBRE | | MEDIDAS | ANEXOS | |
| | | | | ENS ALTO | ENS MEDIO |
| **Protección de las comunicaciones [mp.com]** | Enrutadores | | [mp.com.3]; [mp.com.4] | D.1 | D.1M |
| | Switches | | [mp.com.4] | D.2 | D.2M |
| | Cortafuegos | | [mp.com.1]; [mp.com.3]; [mp.com.4] | D.3 | D.3M |
| | *Proxies* | | [mp.com.1]; [mp.com.3]; [mp.com.4] | D.4 | D.4M |
| | Dispositivos de Red Inalámbricos | | [mp.com.3]; [mp.com.4] | D.5 | D.5M |
| | Pasarelas seguras de intercambio de datos | | [mp.com.4] | D.6 | NA |
| | Diodos de datos | | [mp.com.4] | D.7 | NA |
| | Redes privadas virtuales | IPSec | [mp.com.2]; [mp.com.3] | D.8A | |
| | | TLS | | D.8B | |
| | Herramientas de voz y vídeo por IP (VVoIP) | | [mp.com.2]; [mp.com.3] | D.9A | D.9AM |
| | Herramientas de mensajería instantánea (IM) | | | D.9B | D.9BM |
| | Herramientas de videoconferencia | | | D.9C | D.9CM |
| | Web Application Firewall (WAF) | | [mp.com.1]; [mp.com.3]; [mp.com.4] | D.10 | D.10M |
| | Redes definidas por *software* (SDN) | | [mp.com.1]; [mp.com.3]; [mp.com.4] | D.11 | |

| MEDIDAS DE SEGURIDAD | FAMILIAS | | | |
|---|---|---|---|---|
| | NOMBRE | MEDIDAS | ANEXOS | |
| | | | ENS ALTO | ENS MEDIO |
| **Protección de la Información [mp.info] y los Soportes de Información [mp.si]** | Almacenamiento cifrado de datos | [mp.si.2]; [mp.info.3] | E.1 | |
| | Cifrado y compartición segura de información | [mp.si.2]; [mp.info.3] | E.2 | |
| | Herramientas de Borrado Seguro | [mp.si.5] | E.3 | E.3M |
| | Sistemas de prevención de fugas de datos | [mp.info.2] | E.4 | |
| | Herramientas para firma electrónica | [mp.info.4]; [mp.info.5] | E.5 | NA |
| | *Hardware Security Module* (HSM) | [mp.si.2]; [mp.info.3] | E.6 | NA |
| | Gestión de metadatos | [mp.si.1]; [mp.info.5] Transversalmente: [op.mon.3] | E.7 | E.7M |
| **Protección de Equipos [mp.eq] y Servicios [mp.s]** | Dispositivos móviles | [mp.eq.3] | F.1 | NA |
| | Sistemas operativos | [mp.eq.2] Transversalmente : [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.exp.8] | F.2 | NA |
| | Protección de correo electrónico | Transversalmente: [op.acc.1]; [op.acc.5]; [mp.si.2] | F.3 | F.3M |
| | Tarjetas inteligentes | [mp.s.1] | F.4 | NA |
| | Copias de seguridad | [mp.info.9] | F.5 | |

| MEDIDAS DE SEGURIDAD | FAMILIAS | | | |
|---|---|---|---|---|
| | NOMBRE | MEDIDAS | ANEXOS | |
| | | | ENS ALTO | ENS MEDIO |
| | Plataformas confiables | [mp.eq.2] Transversalmente : [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.exp.8] | F.6 | |
| | Virtualización | [mp.eq.2] Transversalmente : [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.exp.8] | F.7 | F.7M |
| | Balanceadores de carga | [mp.s.8] | F.8 | F.8M |
| | CASB | [mp.s] Transversalmente : [mp.info]; [mp.acc]; [op.exp.2] | F.9 | F.9M |
| | Hiperconvergencia | [mp.s] Transversalmente : [mp.com]; [op.cont] [mp.info.9] | F.10 | F.10M |
| | Herramientas de videoidentificación | [mp.s.2] | F.11 | F.11M |
| | Infraestructura de escritorio virtual (VDI) | [op.acc.4] [op.acc.6] [mp.eq.3] [mp.si] | F.12 | F.12M |
| | Conmutadores KVM | | F.13 | |

| MEDIDAS DE SEGURIDAD | FAMILIAS | | | |
|---|---|---|---|---|
| | NOMBRE | MEDIDAS | ANEXOS | |
| | | | ENS ALTO | ENS MEDIO |
| | Sistemas de Gestión de Bases de Datos (DBMS) | Control y requisitos de acceso.<br>Configuración de seguridad<br>Inventario de activos<br>Mantenimiento y actualizaciones de seguridad | F.14 | |
| **Protección de las instalaciones e infraestructuras [mp.if]** | Cámaras IP | [mp.if] | I.1 | I.1M |
| | Gestión de vídeo | [mp.if] | I.2 | I.2M |
| **Seguridad OT** | Estaciones de carga de vehículos eléctricos | | | O.1M |
| **Servicios de seguridad en la nube** | | - | G | |
| **Otras herramientas** | | - | - | |
| **Herramientas para el desarrollo de productos de seguridad** | | - | - | |

**Tabla 2. Taxonomía de Productos y Servicios Cualificados**

**Nota:** Los anexos marcados con (*) se encuentran en elaboración en la fecha de publicación de la presente guía. Los RFS correspondientes a estas familias serán publicados en futuras versiones.

## 4.3 TAXONOMÍA: DESCRIPCIÓN

### 4.3.1. CONTROL DE ACCESO

27. Todo organismo necesita la capacidad de disponer de distintos perfiles de usuario y que, a su vez, cada usuario cuente con unas credenciales de acceso

personalizadas. Estas capacidades, unidas a unas políticas de seguridad adecuadas para cada tipo de usuario, permiten controlar el acceso a los recursos disponibles. Abarca todas las familias de productos que facilitan dichas capacidades.

#### 4.3.1.1. FAMILIA: CONTROL DE ACCESO A RED (NAC)

28. Engloba todos los productos que cuentan con mecanismos destinados a la administración y el acceso de un conjunto de usuarios a una red concreta. Entre sus opciones de configuración cuentan con soluciones específicas de seguridad para aumentar o disminuir la disponibilidad de la red y lograr así el cumplimiento normativo de la empresa u organismo.

#### 4.3.1.2. FAMILIA: DISPOSITIVOS BIOMÉTRICOS

29. Permiten la autenticación e identificación de usuarios mediante la presentación de atributos físicos únicos como por ejemplo la huella dactilar, el iris del ojo, etc.

#### 4.3.1.3. FAMILIA: DISPOSITIVOS *SINGLE SIGN-ON*

30. Habilitan el acceso a varios sistemas dentro de una organización realizando únicamente una autenticación, es decir, no es necesario repetir el proceso de autenticación para cada servicio, sino que basta con un sólo acceso/cuenta.

#### 4.3.1.4. FAMILIA: SERVIDORES DE AUTENTICACIÓN

31. Los productos asociados a esta familia están orientados fundamentalmente a verificar la identidad de un usuario o dispositivo dentro de una arquitectura de red protegida en función de uno o varios factores. Estos productos suelen situarse justo delante de los servicios de una organización para asegurar que estos son solamente utilizados por aquellas identidades autorizadas de acuerdo a la política de seguridad de la organización.

#### 4.3.1.5. FAMILIA: DISPOSITIVOS *ONE-TIME PASSWORD*

32. Los productos asociados a esta familia están orientados fundamentalmente a proporcionar un medio para generar claves de acceso de un solo uso, conocidos como *tokens*, que sirven para reforzar cualquier sistema o procedimiento de autenticación, evitando diversos ataques como los de fuerza bruta y permitiendo implementar estrategias de autenticación fuerte o multi-factor.

#### 4.3.1.6. FAMILIA: GESTIÓN DE ACCESO PRIVILEGIADO (PAM)

33. Los productos asociados a esta familia permiten el acceso privilegiado seguro a los activos críticos de un sistema de acuerdo a las políticas de una organización. Para ello, gestionan y monitorizan cuentas privilegiadas y accesos: descubren cuentas, dispositivos o aplicaciones privilegiadas; gestionan y protegen credenciales; controlan el acceso a cuentas privilegiadas y aíslan y monitorizan sesiones de acceso privilegiado.

#### 4.3.1.7. FAMILIA: GESTIÓN DE IDENTIDADES (IM)

34. Los productos asociados a la familia de Gestión de Identidades (*IM, Identity Management)* proporcionan a las organizaciones servicios centralizaos y sincronizados de identidades digitales. Generan una identidad única para cada usuario, de manera que se le pueda identificar de manera unívoca, y a la que asociar el resto de atributos para la autenticación (credenciales) y autorización (permisos), junto con otros atributos de interés.

### 4.3.2. SEGURIDAD EN LA EXPLOTACIÓN

35. Abarca las familias de productos que facilitan la gestión de la seguridad durante la explotación de un sistema informático, desde su implantación y puesta en funcionamiento hasta su fin de servicio, permitiendo mantener una correcta configuración de las medidas de protección y los niveles de seguridad en su día a día.

#### 4.3.2.1. FAMILIA: ANTI-VIRUS/EPP (ENDPOINT PROTECTION PLATFORM)

36. Se centran en la prevención, detección y desinfección de virus informáticos. Conforme Internet ha ido creciendo y ganando en popularidad, estas herramientas han avanzado en consonancia y actualmente son productos muy avanzados, centrados en prevenir e impedir la propagación buscando que los sistemas donde se ejecutan no se vean comprometidos por códigos dañinos de diferente naturaleza.

#### 4.3.2.2. FAMILIA: EDR (ENDPOINT DETECTION AND RESPONSE)

37. Debido a que las herramientas anti-virus o EPP no aportan una protección completa, ha surgido una nueva familia de aplicaciones llamadas EDR (*Endpoint Detection and Response*) que añaden características de seguridad enfocadas a detectar y bloquear el malware desconocido.

38. La funcionalidad de los EDR ha evolucionado a lo largo del tiempo. En su concepto original se trataba de herramientas para monitorizar y observar la ejecución de procesos. Actualmente las herramientas EDR han evolucionado abarcando parte de las características EPP e incorporando funcionalidades IR (*Incident Response*), hacia una nueva familia llamada *Next Generation Endpoint Protection Platform (NGEPP).*

#### 4.3.2.3. FAMILIA: HERRAMIENTAS DE GESTIÓN DE RED

39. Permiten centralizadamente, gestionar y configurar la infraestructura de dispositivos que conforman una red, monitorizar su rendimiento y el consumo de recursos, así como la resolución de problemas en la red.

#### 4.3.2.4. FAMILIA: HERRAMIENTAS DE ACTUALIZACIÓN DE SISTEMAS

40. Permiten actualizar los componentes software de un sistema en respuesta a las modificaciones y actualizaciones facilitadas por los proveedores, fundamentalmente con el fin de corregir fallos de seguridad o vulnerabilidades

existentes, así como también para añadir nuevas funcionalidades a los sistemas afectados.

#### 4.3.2.5. FAMILIA: HERRAMIENTAS DE FILTRADO DE NAVEGACIÓN

41. Protegen al usuario durante la navegación por Internet. Controlan los sitios web y servicios que pueden ser vistos o accedidos. Para lograrlo, hacen uso de listas de confianza o reputación basadas en direcciones URL[7], así como pueden limitar todo acceso a sitios no confiables o potencialmente peligrosos.

#### 4.3.2.6. FAMILIA: SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM)

42. Sirven de apoyo a la monitorización de la seguridad facilitando el proceso de recopilar, analizar y cotejar, así como salvaguardar la información sobre eventos de seguridad y anomalías que puedan indicar un compromiso de la seguridad en los sistemas, pudiendo proporcionar adicionalmente funcionalidades para la detección y notificación de los incidentes de seguridad, y facilitando la trazabilidad lo más rápida y sencilla posible de los eventos.

#### 4.3.2.7. FAMILIA: DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS

43. Permiten llevar a cabo el necesario control y salvaguarda de las claves criptográficas utilizadas para la protección de las comunicaciones, así como de la información almacenada, durante todo su ciclo de vida, incluyendo su generación, transporte, custodia durante su explotación, archivo posterior una vez retiradas y destrucción final.

#### 4.3.2.8. FAMILIA: HERRAMIENTAS DE GESTIÓN DE DISPOSITIVOS (UEM)

44. Permiten gestionar de forma eficiente la diversidad y el despliegue masivo, dinámico y a gran escala de dispositivos en una organización. Las herramientas de gestión de dispositivos permiten aplicar políticas de seguridad y configuraciones a los dispositivos de una organización de manera que éstos puedan ser utilizados para procesar información conforme a los criterios establecidos.

#### 4.3.2.9. FAMILIA: SISTEMAS DE ORQUESTACIÓN, AUTOMATIZACIÓN Y RESPUESTA DE SEGURIDAD (SOAR)

45. Los productos o servicios asociados a esta familia están orientados a la gestión de incidentes, la automatización de tareas y la coordinación de respuestas. Adicionalmente, proporcionan capacidades de correlación y procesado de alertas, lo que en conjunto permite a las organizaciones una detección y respuesta más rápida a los incidentes de seguridad, minimizando el impacto y mejorando la postura de seguridad global.

[7]**URL (*Uniform Resource Locator*):** Localización Uniforme del Recurso. Es la forma en que se identifica un sitio en internet. Ej www.ccn.cni.es

### 4.3.3. MONITORIZACIÓN DE LA SEGURIDAD

46. La reacción efectiva frente a los incidentes de seguridad se basa en la rápida detección y correcta identificación de las actividades que indican un compromiso de la seguridad en los sistemas. Abarca las familias de productos que permiten una continua monitorización de la seguridad automatizando el análisis de los eventos de seguridad, la recopilación y notificación de información al respecto, así como la posible reacción frente a los incidentes detectados.

#### 4.3.3.1. FAMILIA: DISPOSITIVOS IPS, IDS Y ANTIDDOS

47. Su función principal es conseguir detectar y evitar accesos no autorizados, ya sea a una red concreta o a un equipo en el que se instalen. Para lograr su objetivo, realizan funciones de monitorización del tráfico de red con el fin de determinar y prevenir comportamientos sospechosos.

#### 4.3.3.2. FAMILIA: SISTEMAS HONEYPOT / HONEYNET

48. Atraen y detectan actividad dañina en una red o aplicación simulada que emula sistemas de interés para un atacante, permitiendo la monitorización de sus actividades para mejorar posteriormente los mecanismos de protección de las redes reales de la organización.

#### 4.3.3.3. FAMILIA: CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO

49. Permiten recopilar, mostrar y analizar el tráfico de una red facilitando la detección e investigación de posibles eventos de seguridad, principalmente relacionados con el uso no adecuado o no autorizado de protocolos de red.

#### 4.3.3.4. FAMILIA: HERRAMIENTAS DE SANDBOX

50. Permiten la ejecución de aplicaciones de forma aislada y controlada con el objetivo de analizar su ejecución y detectar si contienen código dañino. En el caso de que la aplicación ejecutada contenga *malware* se garantiza que el sistema en el que está desplegada la herramienta de *sandbox* no es infectado.

### 4.3.4. PROTECCIÓN DE LAS COMUNICACIONES

51. Englobaas familias de productos cuyo propósito principal es el de la protección de las comunicaciones establecidas entre sistemas y/o dispositivos conectados dentro de una red. Entre sus principales funciones están las de establecer un perímetro de seguridad, garantizar comunicaciones seguras y prevenir ataques provenientes de otras redes externas.

#### 4.3.4.1. FAMILIA: ENRUTADORES

52. Proporcionan conectividad a nivel de red del modelo OSI[8], permitiendo gestionar el enrutamiento o encaminamiento de paquetes de datos entre diferentes

[8] **OSI (Open System Interconnection):** modelo de Interconexión de Sistemas Abiertos.

subredes. Para ello, será necesario que el dispositivo almacene los paquetes recibidos, procese su información de origen y destino, y finalmente los reenvíe. Cuentan con funcionalidades específicas para la configuración y monitorización del tráfico, ya sea local o remotamente.

#### 4.3.4.2. FAMILIA: *SWITCHES*

53. Permiten interconectar, a nivel de enlace de datos del modelo OSI, dos o más segmentos de red con objeto de fusionarlos en una sola red, pasando datos de un segmento a otro de acuerdo con la dirección MAC[9] de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.

#### 4.3.4.3. FAMILIA: CORTAFUEGOS

54. Controlan los flujos de información entre redes permitiendo el bloqueo de aquellos accesos que no hayan sido autorizados. También impiden la propagación de software malintencionado entre los equipos miembros de la red que protegen. Pueden trabajar a diferentes niveles de la capa OSI e implementarse como equipos dedicados (*appliances*) o como aplicaciones software.

#### 4.3.4.4. FAMILIA: *PROXIES*

55. Actúan como intermediarios en las comunicaciones a través de interconexiones entre redes internas y externas, aceptando peticiones de clientes de la red protegida y actuando en su nombre ante los dispositivos externos, enmascarando y protegiendo así al usuario frente a posibles atacantes.

#### 4.3.4.5. FAMILIA: DISPOSITIVOS DE RED INALÁMBRICOS

56. Permiten la conectividad de equipos y dispositivos móviles a una red por medios inalámbricos (p.ej.: WiFi), a través de ondas electromagnéticas y sin necesidad de acceso a una red cableada. Deben aplicar mecanismos para que las comunicaciones a distancia entre el dispositivo de red inalámbrico y el nodo que se conecta a éste no se vean comprometidas.

#### 4.3.4.6. FAMILIA: PASARELAS SEGURAS DE INTERCAMBIO DE DATOS

57. Permiten la interconexión de redes evitando la filtración de información no autorizada, tanto en sentido de entrada como de salida, mediante la ruptura de la continuidad de los protocolos de comunicaciones y la configuración de una interfaz para determinadas tipologías de servicios de intercambio de datos, tales como correo electrónico, ficheros informáticos, etc. permitiendo el tránsito de la información en los dos sentidos, pero sin utilizar simultáneamente los mismos recursos.

[9] **MAC (*Media Access Control*):** se conoce también como la dirección física de una tarjeta o dispositivo de red y es única para cada uno de ellos. Consiste en seis grupos de dos caracteres hexadecimales separadas por dos puntos.

#### 4.3.4.7. FAMILIA: DIODOS DE DATOS

58. Limitan la conectividad entre equipos/redes, permitiendo el flujo de información en un único sentido, haciendo así inviable la comunicación en el sentido opuesto. De este modo y según la necesidad, se puede transferir la información de una red a otra más protegida sin que se pueda aprovechar dicha conexión para la fuga de información de la red protegida, o por el contrario permitir el envío de información desde la red protegida sin que se abra una canal de acceso desde el exterior.

#### 4.3.4.8. FAMILIA: REDES PRIVADAS VIRTUALES

59. Destinados al cifrado de los canales de comunicación, entre emisor y receptor, mediante los que se intercambia la información en tránsito con el fin de preservar su confidencialidad e integridad. Incluye desde dispositivos hardware con capacidad de cifrado de las comunicaciones a aplicaciones software para el establecimiento de redes privadas virtuales (VPN), permitiendo crear una conexión segura con otra red a través de internet mediante la creación de túneles cifrados.

#### 4.3.4.9. FAMILIA: HERRAMIENTAS DE VOZ Y VÍDEO POR IP (VVOIP)

60. Suministran a las organizaciones servicios que permiten conectar en tiempo real a dos o más personas desde diferentes localizaciones, a través de la red, mediante el uso de un dispositivo móvil, ordenador o *tablet*. Permiten la realización de llamadas de audio y vídeo, entre dos (2) o más dispositivos, protegiendo la confidencialidad de las comunicaciones entre ambos extremos.

#### 4.3.4.10. FAMILIA: HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA (IM)

61. Suministran a las organizaciones servicios que permiten conectar en tiempo real a dos o más personas desde diferentes localizaciones, a través de la red, mediante el uso de un dispositivo móvil, ordenador o *tablet*. Permiten el envío de mensajes de texto y ficheros en tiempo real, entre dos (2) o más dispositivos, protegiendo la confidencialidad de las comunicaciones entre ambos extremos.

#### 4.3.4.11. FAMILIA: HERRAMIENTAS DE VIDEOCONFERENCIA

62. Los productos asociados a la familia de Herramientas de Videoconferencia suministran a las organizaciones servicios que permiten conectar en tiempo real a dos o más personas desde diferentes localizaciones, a través de la red, mediante el uso de un dispositivo móvil, ordenador o *tablet*. Permiten el establecimiento de una comunicación de audio y vídeo en tiempo real, entre dos (2) o más dispositivos. Disponen de opciones de compartir la pantalla, para realizar presentaciones, enviar documentos, programar reuniones y enviar convocatorias.

#### 4.3.4.12. FAMILIA: WEB APPLICATION FIREWALL (WAF)

63. Analizan y filtran el tráfico dirigido a aplicaciones web específicas. La protección tiene lugar dentro de la capa 7 del modelo OSI (Capa de Aplicación). Son un tipo especializado de cortafuegos o firewall que se instalan por delante de los servidores web, para proteger las aplicaciones web contra ataques internos y externos.

#### 4.3.4.13. FAMILIA: REDES DEFINIDAS POR *SOFTWARE* (SDN)

64. 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. 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

### 4.3.5. PROTECCIÓN DE LA INFORMACIÓN Y SOPORTES DE INFORMACIÓN

65. Engloba las familias de productos cuyo propósito es reforzar las medidas de protección de la información, así como de aquellos soportes en los que ésta se maneje, con el fin de asegurar alguna (o todas) las dimensiones de seguridad incluyendo su disponibilidad, integridad y confidencialidad, así como el no repudio de la información.

#### 4.3.5.1. FAMILIA: ALMACENAMIENTO CIFRADO DE DATOS

66. Destinadas al cifrado y descifrado de todo tipo de archivos de datos, así como soportes de almacenamiento tales como discos duros o memorias extraíbles, con el fin de proteger su confidencialidad y habilitar sólo a usuarios autorizados el acceso a la información contenida.

#### 4.3.5.2. FAMILIA: CIFRADO Y COMPARTICIÓN SEGURA DE INFORMACIÓN

67. Las herramientas de cifrado y compartición segura de información son productos que permiten intercambiar de forma segura información o ficheros.

#### 4.3.5.3. FAMILIA: HERRAMIENTAS DE BORRADO SEGURO

68. Permiten eliminar la información en formato electrónico (archivos, carpetas, unidades lógicas, etc.) de forma segura, es decir, de un modo que los contenidos eliminados sean irrecuperables posteriormente.

#### 4.3.5.4. FAMILIA: SISTEMAS DE PREVENCIÓN DE FUGAS DE DATOS

69. Los productos de control de contenidos, conocidos generalmente en inglés como *Data Loss/Leak Prevention* (DLP), son aquellos que impiden y evitan la transferencia de datos no autorizados y la fuga de información con nivel alto de confidencialidad. Pueden controlar el acceso físico a puertos y otros dispositivos extraíbles para evitar el robo de información, así como manejar el acceso a la información según roles y perfiles de usuarios.

#### 4.3.5.5. FAMILIA: HERRAMIENTAS PARA FIRMA ELECTRÓNICA

70. Engloban dispositivos y herramientas que forman parte de un sistema de firma electrónica. Mediante la combinación de estos elementos se permite la generación y validación de firmas mediante mecanismos digitales permitiendo, según el

contexto, salvaguardar la confidencialidad, la integridad, y el no repudio de la información firmada.

71. Se indicará en las observaciones aquellos productos que cumplan con el Reglamento UE 910/2014 (eIDAS) para dispositivos cualificados de creación de firma electrónica.

#### 4.3.5.6. FAMILIA: *HARDWARE SECURITY MODULE* (HSM)

72. Esta familia engloba dispositivos criptográficos basados en *hardware* que generan, almacenan y protegen claves criptográficas y suelen aportar aceleración *hardware* para operaciones criptográficas.

#### 4.3.5.7. FAMILIA: GESTIÓN DE METADATOS

73. Comprende las herramientas que gestionan los metadatos que contienen ficheros, como documentos ofimáticos o archivos multimedia (imagen, audio, video), conforme a la política de tratamiento de metadatos establecida en un organismo.

### 4.3.6. PROTECCIÓN DE EQUIPOS Y SERVICIOS

74. La seguridad en las TIC recae en gran medida en la correcta protección de los equipos sobre los que se procesa la información, así como de los servicios que se ejecutan en estos. Abarca las familias de productos que proporcionan un nivel de seguridad a nivel de plataforma, y que en ocasiones ofrecen también una seguridad transversal con otras medidas de seguridad de las recogidas en la presente taxonomía, así como mecanismos de protección para servicios TIC específicos.

#### 4.3.6.1. FAMILIA: DISPOSITIVOS MÓVILES

75. Comprenden los dispositivos hardware, equipados con software de sistema, que facilitan la conectividad a redes móviles facilitando los mecanismos para establecer comunicaciones de voz y datos por diferentes medios con otras redes o dispositivos móviles.

#### 4.3.6.2. FAMILIA: SISTEMAS OPERATIVOS

76. Componen el software básico usado en plataformas hardware (ordenadores, teléfonos móviles, tabletas, etc.) para la administración de los recursos de la máquina, la gestión de los recursos hardware y la provisión de servicios a programas de aplicación software.

#### 4.3.6.3. FAMILIA: PROTECCIÓN DE CORREO ELECTRÓNICO

77. Analizan el flujo de correos electrónicos para evitar que aquellos considerados dañinos lleguen a los usuarios finales. Estas herramientas analizan el contenido de los mensajes en busca de palabras y patrones sospechosos que indiquen que estos deben ser filtrados o etiquetados para no ser remitidos a la bandeja de entrada de correo.

#### 4.3.6.4. FAMILIA: TARJETAS INTELIGENTES

78. Permiten la ejecución de lógica programada en sus circuitos integrados para muy distintos fines, a la vez que proporcionan interfaces para la comunicación con los sistemas con que deben interactuar. Además, las tarjetas inteligentes pueden estar equipadas con diferentes mecanismos de protección para salvaguardar los datos que contienen o los datos intercambiados para llevar a cabo la funcionalidad a la que se destinen.

#### 4.3.6.5. FAMILIA: COPIAS DE SEGURIDAD

79. Permiten aplicar las políticas de copias de seguridad definidas por la organización. Estas herramientas permiten realizar copias de seguridad de sistemas de almacenamiento, equipos o sistemas completos.

#### 4.3.6.6. FAMILIA: PLATAFORMAS CONFIABLES

80. Productos o sistemas que sirven como base o soporte para la ejecución de determinados módulos software.

#### 4.3.6.7. FAMILIA: VIRTUALIZACIÓN

81. Los productos asociados a la familia de Virtualización están orientados fundamentalmente a aprovechar una misma infraestructura hardware que se compartirá con múltiples entornos aislados cada uno con su propio sistema operativo, posibilitando la mejora en la eficiencia y flexibilidad de los recursos TIC. El **hipervisor, o Gestor de Máquinas Virtuales (VMM[10])**, es el componente del producto que permite al equipo físico soportar los distintos entornos virtuales con sus configuraciones. Cada entorno virtual se encapsula en **una máquina virtual (VM[11])** que tiene asignados unos recursos virtuales, como memoria, procesador, sistema operativo invitado y aplicaciones.

#### 4.3.6.8. FAMILIA: BALANCEADORES DE CARGA

82. Los productos asociados a la familia de Balanceadores de Carga o Controladores de Entrega de Aplicación están orientados al control del ancho de banda entre diferentes elementos del sistema, principalmente entre equipos cliente (internos o externos) que realizan peticiones a servidores que las atienden. Los balanceadores son productos *software* o *hardware* que tienen como objetivo evitar la saturación de los servicios, optimizando la asignación de recursos entre diferentes servidores independientes o en clúster.

#### 4.3.6.9. FAMILIA: CASB

83. Los productos CASB (*Cloud Access Security Broker*) dan respuesta a la necesidad de visibilidad y control sobre el uso que hacen los usuarios de una organización de las aplicaciones y servicios en la nube. Representan un punto central en el que la

[10] *Virtual Machine Management*
[11] *Virtual Machine*

organización puede implementar políticas de seguridad que regulen el uso que realizan usuarios y dispositivos, de aplicaciones y servicios en la nube.

#### 4.3.6.10. FAMILIA: HIPERCONVERGENCIA

84. La infraestructura hiperconvergente (HCI) es un enfoque de arquitectura basada en *software* que proporciona recursos de almacenamiento, cómputo y redes de forma transparente al *hardware* que se utilice, con grandes capacidades de escalado horizontal y todo ello gestionado desde un único punto centralizado. Los productos asociados a esta familia integran las capacidades de cómputo, de almacenamiento y de red en una misma capa de funcionamiento y centralizan todas las tareas de gestión propias de los centros de datos, a nivel *software*.

#### 4.3.6.11. FAMILIA: HERRAMIENTAS DE VIDEOIDENTIFICACIÓN

85. Los productos asociados a esta familia surgen para dar respuesta a la necesidad de establecer mecanismos de autenticación e identificación remota, con el fin de contribuir en la reducción de los desplazamientos de los ciudadanos para realizar trámites, sin mermar sus derechos. Estas herramientas realizan comparaciones entre una persona y su foto del documento de identidad e implementan controles de seguridad en tiempo real, como la detección de hologramas, distintivos, patrones y otros elementos de seguridad del documento de identidad.

#### 4.3.6.12. FAMILIA: INFRAESTRUCTURAS DE ESCRITORIO VIRTUAL (VDI)

86. VDI es una tecnología que permite a los usuarios disponer de un entorno de escritorio, accesible de forma remota a través de un dispositivo cliente. El usuario puede manejar un escritorio completo o una aplicación, de la misma forma que si se estuviese ejecutando en su propio. VDI proporciona flexibilidad y eficiencia a las organizaciones a la hora de gestionar los recursos TI. También da facilidades a los empleados a la hora de desarrollar su trabajo, independientemente de su ubicación física.

#### 4.3.6.13. FAMILIA: CONMUTADORES KVM

87. Los Conmutadores KVM (Keyboard-Video-Mouse), son dispositivos hardware que permiten al usuario controlar múltiples ordenadores desde uno o más conjuntos de teclados, monitores de video y ratones. Permiten seleccionar qué ordenador se desea activar, mostrando así su salida de vídeo y siendo controlado por el teclado y ratón.

#### 4.3.6.14. FAMILIA: SISTEMAS DE GESTIÓN DE BASES DE DATOS (DBMS)

88. Los Sistemas de Gestión de Bases de Datos (DBMS) facilitan el uso y manipulación de las bases de datos de forma segura, sencilla y ordenada. Proporciona a los usuarios una forma sistemática de crear, recuperar, actualizar y administrar los datos, asegurando que los datos estén organizados de manera consistente y permanezcan fácilmente accesibles.

### 4.3.7. PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS

89. Engloba las familias de productos y servicios cuyo propósito es reforzar las medidas de protección las instalaciones e infraestructuras.

#### 4.3.7.1. FAMILIA: CAMARAS IP

90. Los productos pertenecientes a esta familia permiten la captura vídeo y audio y la transmisión de forma segura de forma digital, ya sea para su visualización, almacenamiento local o remoto, o tratamiento en una herramienta de gestión de video.

#### 4.3.7.2. FAMILIA: GESTIÓN DE VÍDEO

91. Los productos pertenecientes a esta familia permiten la visualización, el almacenamiento, la gestión y análisis de eventos y el envío de alertas de una o varias fuentes de captura de captura de vídeo. También permiten la administración centralizada del sistema de videovigilancia.

### 4.3.8. SEGURIDAD OT

92. Incluye herramientas especializadas en proteger sistemas de tecnologías de las Operaciones (OT), utilizados en entornos industriales o en infraestructuras críticas.

#### 4.3.8.1. FAMILIA: ESTACIONES DE CARGA DE VEHÍCULOS ELÉCTRICOS

93. Los productos pertenecientes a esta familia permiten proveer la recarga rápida de las baterías de los vehículos eléctricos mediante la conexión directa a la red eléctrica.

### 4.3.9. SERVICIOS DE SEGURIDAD CLOUD

94. Incluye los servicios *cloud* que suministren funcionalidades de seguridad. Dicha funcionalidad de seguridad debe estar asociada a alguna de las familias incluidas en la taxonomía detallada en este documento.

### 4.3.10. OTRAS HERRAMIENTAS

95. Recoge herramientas cuya funcionalidad principal de seguridad no se encuadran dentro de ninguna otra de las publicadas.

### 4.3.11. HERRAMIENTAS PARA EL DESARROLLO DE PRODUCTOS DE SEGURIDAD

96. Incluye aquellos componentes *software* y firmware que han sido evaluados por el Centro Criptológico Nacional para el desarrollo de productos de seguridad.

97. Dado que en esta clasificación aparecen componentes de diversa índole, no se creará un anexo a esta guía que contenga los Requisitos Fundamentales de Seguridad asociados a la misma.

# 5. TAXONOMÍA DE PRODUCTOS APROBADOS

98. La taxonomía de productos aprobados para el manejo de información clasificada será la misma que para productos cualificados junto con las familias que se detallan en los siguientes apartados.

99. Los Requisitos Fundamentales de Seguridad (RFS) serán los mismos que los establecidos en la presente guía para los productos cualificados, actualizados con los específicos de mecanismos criptográficos descritos en el Anexo H. Además, según el caso podrá requerirse una evaluación TEMPEST y/o una evaluación criptológica del producto.

100. En caso de que sea necesaria una evaluación criptológica del producto, se deberán considerar los requisitos establecidos en la guía CCN-STIC-130 "Requisitos de los Productos de Cifra para Superar la Evaluación Criptológica" [3]. El procedimiento detallado de Aprobación de Productos de Seguridad TIC se incluye en la guía CCN-STIC-102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada [2].

## 5.1 CATEGORÍA: PROTECCIÓN EN ENTORNOS TÁCTICOS

101. En esta categoría se encuentran las familias de productos cuyo propósito principal es la protección de la información y las comunicaciones en entornos tácticos o desplegados.

102. Esta categoría también incluye una familia específica que identifica diferentes sistemas de información para uso en entornos tácticos que, bajo determinadas condiciones de configuración, y siempre empleando productos de las otras familias de esta categoría, se aprueban para procesar información clasificada nacional hasta un nivel determinado. Esta aprobación no exime del procedimiento para la acreditación de los sistemas que manejan información clasificada, definido en la Guía CCN-STIC-101 Acreditación de Sistemas de las TIC que manejan Información Clasificada [5]; la aprobación de un sistema de información táctico únicamente pretende facilitar la propia acreditación del sistema.

103. Las comunicaciones en entornos tácticos o desplegados presentan ciertas particularidades que difieren notablemente de las comunicaciones a través de redes e infraestructuras fijas. Entre ellas, cabe citar las siguientes:

- El tiempo durante el cual la información es relevante, normalmente es menor que en otros entornos. Por ejemplo, la posición de una unidad militar generalmente solo tiene importancia durante el periodo de tiempo que la unidad está en un emplazamiento determinado.
- El impacto asociado al compromiso de la confidencialidad de la información puede incluir otros daños asociados que trascienden la criticidad de la propia información. Siguiendo con el ejemplo anterior, la posición de una unidad militar podría no tener un nivel de clasificación muy alto, pero su compromiso puede poner en riesgo vidas humanas.

- Las redes usadas son generalmente desplegables y de carácter propietario, aunque en determinadas situaciones puntuales también pueden usarse infraestructuras de red pertenecientes a operadores públicos.
- Las redes de carácter propietario generalmente no están conectadas a Internet.
- Los medios de transmisión empleados son generalmente inalámbricos tales como radios militares, equipos de *trunking* digital (TETRA, TETRAPOL…), equipos *Wi-Fi* y LTE, etc. Estos medios de transmisión en muchas ocasiones son de naturaleza *half-duplex*, presentan un reducido ancho de banda, una tasa de errores que puede llegar a ser elevada, no existe una garantía de conectividad, etc. Por todo ello, no es factible emplear ciertas soluciones de cifra habitualmente usadas en infraestructuras de red fijas (p.ej.: cifradores IP clásicos con negociación de claves de sesión), y resulta necesario emplear soluciones de cifra específicas adaptadas a los medios de transmisión empleados.
- Ciertas características de los despliegues tácticos en ocasiones pueden permitir asumir que el nivel de la amenaza para determinados medios de transmisión de corto alcance es menor que en otro tipo de entornos. Entre estas características se incluyen el establecimiento de perímetros de seguridad y vigilancia (p.ej. en puestos de mando), la corta estancia de un nodo móvil en un mismo emplazamiento, etc.
- En este tipo de productos, más alá de los mecanismos COMSEC también cobran especial importancia otros aspectos como los mecanismos TRANSEC y NETSEC.

104. Dada la multiplicidad de escenarios tácticos posibles, las limitaciones en la utilización de los productos pertenecientes a las familias de esta categoría, quedarán perfectamente delimitadas en el correspondiente procedimiento de empleo del producto.

### 5.1.1. FAMILIA: PLATAFORMAS Y DISPOSITIVOS TÁCTICOS CONFIABLES

105. Plataformas y dispositivos para entornos tácticos que se consideran como un contenedor seguro donde ejecutar aplicaciones software de forma protegida (p.ej.: aplicaciones de mando y control).

106. En general, serán de aplicación los mismos Requisitos Fundamentales de Seguridad aplicables a la familia Plataformas Confiables.

107. Esta familia no contempla la protección de la información en tránsito, cuyo cifrado deberá ser realizado por una solución para la protección de las comunicaciones tácticas (p.ej. una aplicación de cifrado que se ejecute en la propia plataforma o dispositivo táctico confiable). Por tanto, las aprobaciones de estas plataformas y dispositivos de forma aislada únicamente serán válidas para procesamiento de información clasificada de forma local, pero no para la transmisión de ésta por redes no seguras.

### 5.1.2. FAMILIA: SOLUCIONES PARA PROTECCIÓN DE LAS COMUNICACIONES TÁCTICAS

108. Permiten la protección de las comunicaciones en entornos tácticos en una o varias dimensiones de seguridad (confidencialidad, integridad, autenticidad, disponibilidad y/o trazabilidad), adecuándose a las particularidades de los medios de transmisión empleados.

109. Incluirá diferentes tipos de productos adecuados para diferentes niveles de clasificación que se indicarán de forma explícita: cifradores tácticos, radios militares, aplicaciones software de cifrado, etc.

110. En el caso de las aplicaciones *software* de cifrado, éstas deberán ejecutarse en plataformas o dispositivos tácticos que sean considerados confiables y que pertenezcan a la anterior familia (se identificarán en el procedimiento de empleo seguro de la aplicación de cifrado).

111. En el caso de las radios militares, teniendo en cuenta su naturaleza reconfigurable, la aprobación de cada una de ellas identificará de forma inequívoca las formas de onda y los juegos de algoritmos COMSEC, NETSEC y TRANSEC incluidos en dicha aprobación. Sólo se incluirán aquellas formas de onda cuyos mecanismos COMSEC hayan sido aprobados tras superar la correspondiente evaluación criptológica.

112. Esta familia también particularizará la aprobación de ciertos productos pertenecientes a otras familias para su empleo en entornos tácticos, permitiendo su uso para proteger información clasificada de mayor grado de clasificación que el que figura en su aprobación general (p.ej. ver CCN-STIC-497 sobre empleo de Wi-Fi en redes clasificadas). Las condiciones bajo las que se particulariza la aprobación de un producto existente vendrán definidas en un procedimiento de empleo exclusivo y dedicado para esas condiciones de uso.

### 5.1.3. FAMILIA: SISTEMAS DE INFORMACIÓN PARA ENTORNOS TÁCTICOS

113. Sistemas de información para uso en entornos tácticos, como por ejemplo sistemas de mando y control, que emplean productos aprobados pertenecientes a las anteriores familias de esta categoría y que se aprueban para el procesamiento de información clasificada nacional.

114. Para incluir un sistema de información en esta categoría también se comprobará el grado de cumplimiento de los requisitos STIC recogidos en la CCN-STIC-301 Requisitos STIC [6].

# 6. TAXONOMÍA DE PRODUCTOS Y SERVICIOS DE CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD

115. La Tabla 3 recoge el esquema de la taxonomía de **Productos de Conformidad y Gobernanza de la Seguridad**, así como la relación de anexos a este documento, donde se recogen los requisitos exigidos para cada una de las familias que componen esta taxonomía.

| FAMILIA | ANEXOS |
|---|---|
| **Gobernanza y Planificación de la Seguridad** | CG.1 |
| **Normativa de Seguridad y Conformidad** | CG.2 |
| **Análisis y Gestión de Riesgos** | CG.3 |
| **Notificación y Gestión de Ciberincidentes** | CG.4 |
| **Intercambio de Ciberinteligencia** | CG.5 |
| **Formación Y Concienciación en Ciberseguridad** | CG.6 |

**Tabla 3. Taxonomía de Productos de Conformidad y Gobernanza de la Seguridad**

## 6.1 FAMILIA: GOBERNANZA Y PLANIFICACIÓN DE LA SEGURIDAD

116. A esta familia pertenecen aquellas soluciones que ofrecen asistencia a los usuarios en la obtención de información acerca del estado de seguridad de los sistemas de los organismos, en base a un estándar de medición, proporcionando índices que permiten evaluar los datos obtenidos, interpretarlos y tomar decisiones estratégicas. Asimismo, podrían facilitar la elaboración de Planes de Adecuación y la obtención del correspondiente conjunto de medidas técnicas a aplicar a sistemas en base a una categoría pre-establecida.

## 6.2 FAMILIA: NORMATIVA DE SEGURIDAD Y CONFORMIDAD

117. Esta familia se compone de aquellas soluciones que ofrecen asistencia a los usuarios en la ejecución de tareas de preparación de auditorías, de la gestión del cumplimiento y certificaciones y de la gestión de la seguridad del sistema en su conjunto. Además, ofrece asistentes orientados a apoyar a auditores y organismos de auditoría, a través de capacidades de recopilación de evidencias de auditoría, listas de comprobación y cuadernos de auditoría, generación de informes y cualquier otra tarea necesaria en las diferentes fases de la auditoría.

## 6.3 FAMILIA: ANÁLISIS Y GESTIÓN DE RIESGOS

118. A esta familia pertenecen aquellas soluciones que ofrecen asistencia a los usuarios en la elaboración del Análisis de Riesgos asociado a los sistemas, en base a un estándar establecido, mediante la identificación de las amenazas a las que están

sometidos los activos esenciales del sistema y el análisis de la probabilidad y el impacto de su materialización. Asimismo, ofrecerán la posibilidad de mitigar o reducir los riesgos asociados a través de salvaguardas.

## 6.4 FAMILIA: NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES

119. A esta familia pertenecen aquellas soluciones que automatizan procesos, clasifican incidentes, facilitan el seguimiento de su gestión y permiten la coordinación entre los diferentes actores implicados. Pueden ofrecer asistencia tanto a operadores que gestionan incidentes como o a usuarios que notifican incidentes de seguridad a un organismo o entidad central.

## 6.5 FAMILIA: INTERCAMBIO DE CIBERINTELIGENCIA

120. A esta familia pertenecen aquellas soluciones destinadas a la gestión e intercambio de ciberinteligencia, proporcionando medios para mejorar las capacidades de prevención, análisis y detección de ciberamenazas.

## 6.6 FAMILIA: FORMACIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD

121. Se incluyen en esta familia aquellas soluciones dedicadas a evaluar, capacitar, reforzar y/o medir los niveles de formación y concienciación en ciberseguridad de los empleados de un organismo.

## 7. REFERENCIAS

[1] CCN-STIC-105 Catálogo de Productos de Seguridad TIC (CPSTIC).

[2] CCN-STIC-102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada.

[3] CCN-STIC-130 Requisitos de los Productos de Cifra para Superar la Evaluación Criptológica.

[4] CCN-STIC-151 Evaluación y Clasificación TEMPEST de equipos.

[5] CCN-STIC-101 Acreditación de Sistemas de las TIC que manejan Información Clasificada.

[6] CCN-STIC-301 Requisitos STIC.

[7] CCN-STIC-106 Procedimiento de inclusión de productos de seguridad TIC cualificados en el CPSTIC.

## 8. ABREVIATURAS

| | |
|---|---|
| **CCN** | *Centro Criptológico Nacional* |
| **CPSTIC** | *Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación* |
| **DLP** | *Data Loss/Leak Prevention* |
| **EDR** | *Endpoint Detection and Response* |
| **ENS** | *Esquema Nacional de Seguridad* |
| **EPP** | *Endpoint Protection Platform* |
| **HSM** | *Hardware Security Module* |
| **IDS** | *Intrusion Detection System* |
| **IM** | *Identity Management* |
| **IPS** | *Intrusion Prevention System* |
| **IPSec** | *Internet Protocol Security* |
| **IR** | *Incident Response* |
| **MAC** | *Media Access Control* |
| **NA** | No Aplica |
| **NAC** | *Network Access Control* |
| **NGEPP** | *Next Generation Endpoint Protection Platform* |
| **OSI** | *Open Systems Interconection* |
| **PAM** | *Privileged Access Manager* |
| **RD** | Real Decreto |
| **RFS** | Requisitos Fundamentales de Seguridad |
| **SIEM** | *Security Information and Event Management* |
| **STIC** | Seguridad de las Tecnologías de la Información y la Comunicación |
| **TIC** | Tecnologías de la Información y la Comunicación |
| **TLS** | *Tranport Layer Security* |
| **UEM** | *Unified Endpoint Management* |
| **URL** | *Uniform Resource Locator* |
| **VM** | *Virtual Machine* |
| **VMM** | *Virtual Machine Manager* |
| **VPN** | *Virtual Private Network* |

PUBLICACIONES DE DEFENSA

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