GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

GUÍA DE SEGURIDAD DE LAS TIC
CCN-STIC 140

Taxonomía de referencia para productos de Seguridad TIC

Julio 2018

Edita:

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.07.10 12:08:14 +02'00'

NIPO: 785-18-034-0.
Publicación incluida en el programa editorial del suprimido Ministerio de la Presidencia y para la Administraciones Territoriales (de acuerdo con la reestructuración ministerial establecida por Real Decreto 355/2018, de 6 de junio).

Fecha de Edición: julio 2018
ISDEFE ha participado en el desarrollo del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y la comunicación (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y la comunicación (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

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. El CCN recibe múltiples consultas de los diferentes organismos de la Administración sobre qué productos deben emplear para proteger sus sistemas de las Tecnologías de la Información y la Comunicación (TIC).
4. Para tratar de dar respuesta a estas consultas, el CCN publica la guía CCN-STIC 105 Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC) que ofrece un listado de productos STIC de referencia con el propósito de satisfacer las necesidades y demandas actuales de empleo de productos seguros en las redes de la Administración. El CPSTIC incluye los Productos Aprobados para manejar información nacional clasificada y los Productos Cualificados de Seguridad TIC.
5. La finalidad del CPSTIC es disponer de un listado de referencia de productos de seguridad TIC supervisado por el CCN que proporcione un nivel mínimo de confianza al usuario final en los productos adquiridos, con las mejoras de seguridad derivadas del proceso de evaluación y certificación, y en su empleo seguro en las redes del sector público garantizado por un Procedimiento de Empleo.
6. Se recogerán en el apartado de Productos Aprobados de seguridad TIC en entornos clasificados aquellos que manejen información clasificada y en Productos Cualificados de Seguridad TIC para entornos sensibles o en aquellos sistemas de información de categoría alta en aplicación del ENS.
7. Para la inclusión de un producto en el catálogo, el CCN tendrá en cuenta una serie de criterios, como, la clasificación de la información que puede manejar (Difusión Limitada, Confidencial, Reservado, Secreto), las características de seguridad del producto, la categoría del sistema de información en el que puede emplearse (alta, media, básica[1]), las certificaciones aportadas, el entorno donde se vaya a emplear, etc. En función de esta información, se determinarán las

1 Clasificación por categorías definida en el ENS.

pruebas o evaluaciones que deberá superar el producto de seguridad TIC correspondiente.

8. 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 [REF1]. La relación de la documentación y 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 [REF3] y para realizar la evaluación TEMPEST se describe en la guía CCN-STIC 151 Evaluación y Clasificación TEMPEST de equipos [REF4]. Ver Figura 1.

9. Así mismo, el procedimiento de inclusión de un producto de seguridad TIC cualificado en el CPSTIC se describe en la guía CCN-STIC 106 Procedimiento de inclusión de productos de seguridad TIC cualificados en el CPSTIC [REF6], los requisitos fundamentales de seguridad o los perfiles de protección que deben cumplir los productos de seguridad TIC en función de su taxonomía se detallan en la presente guía CCN-STIC 140 [REF7] y la descripción detallada del flujo, así como los tiempos máximos del proceso se describen en el Procedimiento de cualificación de productos STIC en el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) PO-09 Procedimiento de cualificación de productos STIC en el ENECSTI [REF5]. Ver Figura 1.

10. El producto de seguridad TIC cualificado 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 el procedimiento de empleo. Dicho procedimiento, basado en la guía de uso, será distribuido por la empresa fabricante junto con el producto.

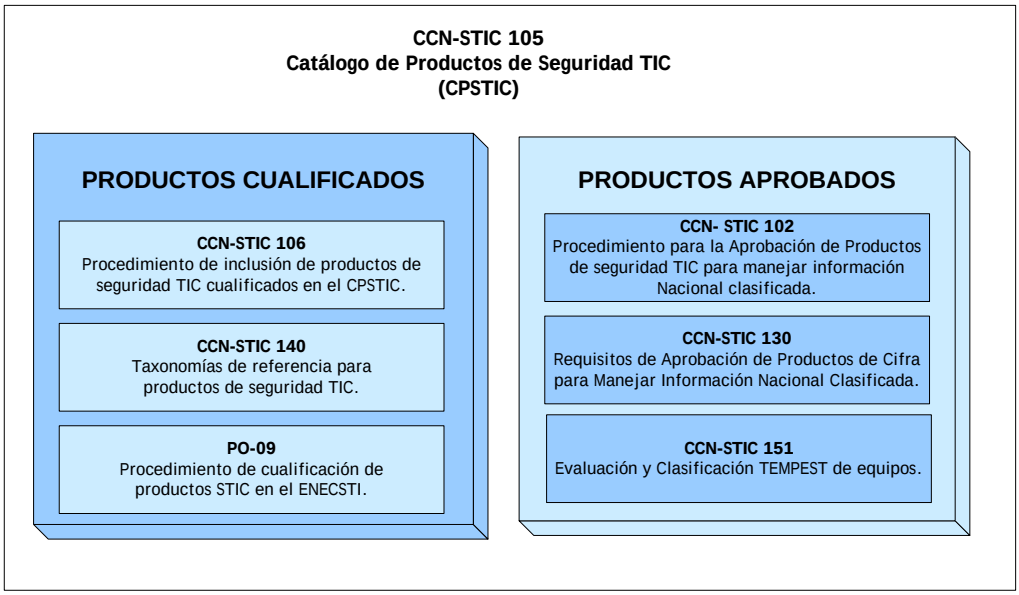

Figura 1. Inclusión de productos de seguridad en el CPSTIC.

2. OBJETIVO

11. El objeto de este documento es el de establecer una taxonomía para la clasificación de productos de Seguridad en las Tecnologías de Información y la Comunicación (TIC) en torno a diversas categorías y familias, identificando su ámbito y alcance, con el objeto de servir como base para la clasificación de productos incluidos en el apartado de Productos Cualificados del CPSTIC, de referencia en la Administración Pública.

12. 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 apartado de Productos Cualificados del CPSTIC.

3. ALCANCE

13. La taxonomía descrita en el presente documento pretende categorizar aquellos productos de seguridad TIC que forman parte activa del sistema TIC, y desarrollan su actividad en el contexto operacional de éste, implementando funcionalidades que permiten incrementar el nivel de seguridad del sistema en alguna de sus dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad).

14. Por lo tanto, no se incluirían dentro de esta taxonomía productos de seguridad cuya función sea, por ejemplo, de auditoría, análisis de riesgos o bastionado de sistemas/equipos. Por el contrario, sí se incluirán productos cuya funcionalidad principal no esté relacionada con la seguridad pero que sí implementen funcionalidades de seguridad, como sería el caso de enrutadores, sistemas operativos, dispositivos móviles, etc.

15. 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

16. 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 al Anexo II sobre Medidas de seguridad del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica[2].

17. La taxonomía cuenta con un conjunto de categorías de productos que, a su vez, se dividen en familias y que han sido definidas, con la intención de adaptarse a los futuros cambios que se puedan producir en el mercado de los productos STIC, conforme a los siguientes criterios:

    - **Categoría**: Tipo de producto de acuerdo a las medidas de seguridad que aporte (p.ej.: control de acceso, protección de las comunicaciones, etc.). Coincidirán con las categorías que componen el marco operacional [op.XXX] y de medidas de protección [mp.XXX] recogidas en el Anexo II del ENS, siempre y cuando éstas resulten aplicables a productos.

    - **Familia**: Tipo de producto de acuerdo a su funcionalidad principal (p.ej.: enrutador, cortafuegos, proxy, herramienta de borrado seguro, etc.). Los productos incluidos en estas familias pueden implementar diversas medidas recogidas en el Anexo II del ENS. Estas medidas se encuentran referenciadas al lado de cada familia mediante su identificador (p.ej.: [op.exp.N] para el requisito número N de las medidas de explotación dentro del marco operacional).

18. 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.

19. 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.

[2]https://www.ccn-cert.cni.es/ens/fe-de-erratas-ens.html y http://www.boe.es/buscar/act.php?id=BOE-A-2010-1330

4.2 TAXONOMÍA: ESQUEMA

20. La Tabla 1 recoge el esquema de la taxonomía, cuyas categorías y familias se definen más adelante, las medidas de seguridad recogidas en el Anexo II del ENS asociadas a cada categoría y familia de productos, así como la relación de anexos a este documento, donde se recogen los Requisitos Fundamentales de Seguridad (RFS) exigidos para cada familia de productos.

CATEGORÍAS	FAMILIAS		
	NOMBRE	MEDIDAS	ANEXOS
Control de acceso [op.acc]	Dispositivos de Control de Acceso a Red	[op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7]	A.1
	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
	Dispositivos *One-Time Password*	[op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7]	A.5 (*)
Seguridad en la explotación [op.exp]	Anti-virus/EPP (*Endpoint Protection Platform*)	[op.exp.6]	B.1
	EDR (*Endpoint Detection and Response)*	[op.exp.6]	B.2
	Herramientas de gestión de red	[op.exp.3]; [op.exp.7]	B.3
	Herramientas de actualización de sistemas	[op.exp.4]; [op.exp.5]	B.4
	Herramientas de filtrado de navegación	[op.exp.6]	B.5
	Sistemas de gestión de eventos de seguridad	[op.exp.8]; [op.exp.9]; [op.exp.10]	B.6
	Dispositivos para gestión de claves criptográficas	[op.exp.11]	B.7(*)
	Herramientas de gestión de dispositivos móviles (MDM)	[op.exp.3]	B.8
	Otras herramientas		

CATEGORÍAS	FAMILIAS		
	NOMBRE	MEDIDAS	ANEXOS
Monitorización de la seguridad [op.mon]	Dispositivos de prevención y detección de intrusiones	[op.mon.1]	C.1
	Sistemas *Honeypot / Honeynet*	[op.mon.1]	C.2
	Captura, Monitorización y Análisis de Tráfico	[op.mon.1]	C.3
Protección de las comunicaciones [mp.com]	Enrutadores	[mp.com.3]; [mp.com.4]	D.1
	Switches	[mp.com.4]	D.2
	Cortafuegos	[mp.com.1]; [mp.com.3]; [mp.com.4]	D.3
	Proxies	[mp.com.1]; [mp.com.3]; [mp.com.4]	D.4
	Dispositivos de Red Inalámbricos	[mp.com.3]; [mp.com.4]	D.5
	Pasarelas seguras de intercambio de datos	[mp.com.4]	D.6
	Diodos de datos	[mp.com.4]	D.7 (*)
	Redes privadas virtuales	[mp.com.2]; [mp.com.3]	D.8
	Herramientas para comunicaciones móviles seguras	[mp.com.2]; [mp.com.3]	D.9
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 *offline*	[mp.si.2]; [mp.info.3]	E.2
	Herramientas de Borrado Seguro	[mp.si.5]	E.3
	Sistemas de prevención de fugas de datos	[mp.info.2]	E.4

CATEGORÍAS	FAMILIAS		
	NOMBRE	MEDIDAS	ANEXOS
	Firma Electrónica	[mp.info.4]; [mp.info.5]	E.5(*)
Protección de Equipos [mp.eq] y Servicios [mp.s]	Dispositivos móviles	[mp.eq.3]	F.1
	Sistemas operativos	[mp.eq.2] Transversalmente se asociaría a: [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.exp.8]	F.2
	anti-spam	Transversalmente se asociaría a: [op.acc.1]; [op.acc.5]; [mp.si.2]	F.3
	Tarjetas inteligentes	[mp.s.1]	F.4
	Copias de seguridad	[mp.info.9]	F.5

Tabla 1. Esquema de Taxonomía para Catálogo de Productos STIC

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. CATEGORÍA: CONTROL DE ACCESO

21. 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. Esta categoría abarca todas las familias de productos que facilitan dichas capacidades.

4.3.1.1. FAMILIA: DISPOSITIVOS DE CONTROL DE ACCESO A RED

22. 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

23. 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*

24. 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

25. 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*

26. 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.

4.3.2. CATEGORÍA: SEGURIDAD EN LA EXPLOTACIÓN

27. Esta categoría 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*)

28. 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)*

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

30. 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 categoría llamada *Next Generation Endpoint Protection Platform (NGEPP).*

4.3.2.3. FAMILIA: HERRAMIENTAS DE GESTIÓN DE RED

31. 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

32. 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

33. 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[3], 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

34. 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

35. Permiten llevar a cabo el necesario control y salvaguarda de las claves criptográficas utilizas para la protección de las comunicaciones, así como de la

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

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 MÓVILES (MDM)

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

4.3.2.9. FAMILIA: OTRAS HERRAMIENTAS

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

4.3.3. CATEGORÍA: MONITORIZACIÓN DE LA SEGURIDAD

38. 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. Esta categoría 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 DE PREVENCIÓN Y DETECCIÓN DE INTRUSIONES (IPS/IDS)[4]

39. 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*

40. 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] **IPS (*Intrusion Prevention System*):** Sistema de Prevención de Intrusiones.
IDS (*Intrusion Detection System*): Sistema de Detección de Intrusiones.

4.3.3.3. FAMILIA: CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO

41. 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.

4.3.4. CATEGORÍA: PROTECCIÓN DE LAS COMUNICACIONES

42. En esta categoría se encuentran las 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

43. Proporcionan conectividad a nivel de red del modelo OSI[5], permitiendo gestionar el enrutamiento o encaminamiento de paquetes de datos entre diferentes 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*

44. 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[6] de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.

4.3.4.3. FAMILIA: CORTAFUEGOS

45. 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*

46. Actúan como intermediarios en las comunicaciones a través de interconexiones entre redes internas y externas, aceptando peticiones de clientes de la red

[5] **OSI (Open System Interconnection):** modelo de Interconexión de Sistemas Abiertos.
[6] **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.

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

47. 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

48. 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.

4.3.4.7. FAMILIA: DIODOS DE DATOS

49. 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

50. 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 PARA COMUNICACIONES MÓVILES SEGURAS

51. Proveen canales seguros de comunicación entre dispositivos móviles a través de redes externas o entre un dispositivo móvil y otras redes de comunicación, protegiendo la confidencialidad de las comunicaciones entre ambos extremos.

4.3.5. CATEGORÍA: PROTECCIÓN DE LA INFORMACIÓN Y SOPORTES DE INFORMACIÓN

52. Esta categoría 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

53. 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 *OFFLINE*

54. Los dispositivos o herramientas de cifrado *offline* son productos que permiten el cifrado de información para su posterior almacenamiento o transporte cuando no se dispone de una infraestructura de comunicaciones o de intercambio de información segura.

4.3.5.3. FAMILIA: HERRAMIENTAS DE BORRADO SEGURO

55. Permiten eliminarla 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

56. 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: FIRMA ELECTRÓNICA

57. Engloban dispositivos y sistemas para la generación, ejecución y validación de firmas mediante mecanismos digitales, asociadas a la información o documentos informáticos, permitiendo salvaguardar según el contexto la confidencialidad e integridad, así como el no repudio de la información firmada.

4.3.6. CATEGORÍA: PROTECCIÓN DE EQUIPOS Y SERVICIOS

58. 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. Esta categoría abarca las familias de productos que

proporcionan un nivel de seguridad a nivel de plataforma, y que en ocasiones ofrecen también una seguridad transversal a otras categorías de las recogidas en la presente taxonomía, así como mecanismos de protección para servicios TIC específicos.

4.3.6.1. FAMILIA: DISPOSITIVOS MÓVILES

59. 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

60. 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: *ANTI-SPAM*

61. Previenen la llegada a la bandeja de entrada de un usuario del correo basura también conocido como *spam*. Estas herramientas analizan los mensajes mirando en su contenido en busca de palabras y patrones de mensajes que sugieren que son correo basura y que por tanto deben ser filtrados y no ser remitidos al usuario.

4.3.6.4. FAMILIA: TARJETAS INTELIGENTES

62. 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

63. 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.

5. REFERENCIAS

REF1	CCN-STIC-102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada.
REF2	CCN-STIC-105Catálogo de Productos de Seguridad TIC (CPSTIC).
REF3	CCN-STIC-130Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada.
REF4	CCN-STIC-151Evaluación y Clasificación TEMPEST de equipos.
REF5	PO-09Procedimiento de cualificación de productos STIC en el ENECSTI.
REF6	CCN-STIC 106 Procedimiento de inclusión de productos de seguridad TIC cualificados en el CPSTIC.
REF7	CCN-STIC 140 Taxonomía de referencia para productos de Seguridad TIC.

6. 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*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
MAC	*Media Access Control.*
OSI	*Open Systems Interconection.*
RD	*Real Decreto.*
RFS	*Requisitos Fundamentales de Seguridad.*
STIC	*Seguridad de las Tecnologías de la Información y la Comunicación.*
TIC	*Tecnologías de la Información y la Comunicación.*
VPN	*Virtual Private Network*