

Taxonomía de referencia para productos y servicios de Seguridad TIC



Julio de 2026



Centro Criptológico Nacional, 2026



CCN
c=ES, l=MADRID, o=CCN, ou=SELLO
ELECTRONICO, 2.5.4.97=VATES-
S2800155J,
serialNumber=S2800155J, cn=CCN
2026.07.22 13:18:06 +02'00'

Fecha de Edición: julio de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

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

ÍNDICE

1. INTRODUCCIÓN	5
2. OBJETIVO	8
3. ALCANCE	9
4. TAXONOMÍA DE PRODUCTOS CUALIFICADOS	10
4.1 TAXONOMÍA: ESTRUCTURA	10
4.2 TAXONOMÍA: ESQUEMA	10
4.3 TAXONOMÍA: DESCRIPCIÓN	16
4.3.1. CONTROL DE ACCESO	16
4.3.1.1. FAMILIA: CONTROL DE ACCESO A RED (NAC)	16
4.3.1.2. FAMILIA: DISPOSITIVOS BIOMÉTRICOS	16
4.3.1.3. FAMILIA: DISPOSITIVOS <i>SINGLE SIGN-ON</i>	16
4.3.1.4. FAMILIA: SERVIDORES DE AUTENTICACIÓN	17
4.3.1.5. FAMILIA: GESTIÓN DE ACCESO PRIVILEGIADO (PAM)	17
4.3.1.6. FAMILIA: GESTIÓN DE IDENTIDADES (IM)	17
4.3.1.7. FAMILIA: AUTENTICACIÓN MULTIFACTOR (MFA)	17
4.3.1.8. FAMILIA: HERRAMIENTAS DE VIDEOIDENTIFICACIÓN	17
4.3.2. PROTECCIÓN DE DISPOSITIVOS	18
4.3.2.1. FAMILIA: ANTI-VIRUS/EPP (ENDPOINT PROTECTION PLATFORM)	18
4.3.2.2. FAMILIA: EDR (ENDPOINT DETECTION AND RESPONSE)	18
4.3.2.3. FAMILIA: HERRAMIENTAS DE GESTIÓN DE DISPOSITIVOS (UEM)	18
4.3.2.4. FAMILIA: HERRAMIENTAS DE SANDBOX	18
4.3.3. PROTECCIÓN DE REDES Y SISTEMAS	18
4.3.3.1. FAMILIA: SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM)	19
4.3.3.2. FAMILIA: SISTEMAS DE ORQUESTACIÓN, AUTOMATIZACIÓN Y RESPUESTA DE SEGURIDAD (SOAR)	19
4.3.3.3. FAMILIA: HERRAMIENTAS DE GESTIÓN DE RED	19
4.3.3.4. FAMILIA: SISTEMAS HONEYBOT / HONEYNET	19
4.3.3.5. FAMILIA: DETECCIÓN Y RESPUESTA DE AMENAZAS EN RED (NDR)	19
4.3.3.6. FAMILIA: HERRAMIENTAS DE ACTUALIZACIÓN DE SISTEMAS	19
4.3.3.7. FAMILIA: CASB	19
4.3.4. PROTECCIÓN DE PERÍMETRO	20
4.3.4.1. FAMILIA: ENRUTADORES	20
4.3.4.2. FAMILIA: <i>SWITCHES</i>	20
4.3.4.3. FAMILIA: CORTAFUEGOS	20
4.3.4.4. FAMILIA: <i>PROXIES</i>	20
4.3.4.5. FAMILIA: DISPOSITIVOS DE RED INALÁMBRICOS	21
4.3.4.6. FAMILIA: PASARELAS SEGURAS DE INTERCAMBIO DE DATOS	21
4.3.4.7. FAMILIA: DIODOS DE DATOS	21
4.3.4.8. FAMILIA: WEB APPLICATION FIREWALL (WAF)	21
4.3.4.9. FAMILIA: REDES DEFINIDAS POR <i>SOFTWARE</i> (SDN)	21
4.3.4.10. FAMILIA: DISPOSITIVOS DE PREVENCIÓN Y DETECCIÓN DE INTRUSIONES	

4.3.4.11. FAMILIA: SISTEMAS ANTIDDOS	22
4.3.4.12. FAMILIA: HERRAMIENTAS DE FILTRADO DE NAVEGACIÓN	22
4.3.4.13. FAMILIA: PROTECCIÓN DE CORREO ELECTRÓNICO	22
4.3.4.14. FAMILIA: BALANCEADORES DE CARGA	22
4.3.5. PROTECCIÓN DE LAS COMUNICACIONES	22
4.3.5.1. FAMILIA: HERRAMIENTAS DE VOZ Y VÍDEO POR IP (VOIP)	22
4.3.5.2. FAMILIA: HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA (IM)	22
4.3.5.3. FAMILIA: HERRAMIENTAS DE VIDEOCONFERENCIA	23
4.3.5.4. FAMILIA: REDES PRIVADAS VIRTUALES (IPSEC)	23
4.3.5.5. FAMILIA: REDES PRIVADAS VIRTUALES (TLS).....	23
4.3.5.6. FAMILIA: REDES PRIVADAS VIRTUALES (OTRAS)	23
4.3.5.7. FAMILIA: ACCESO A RED DE CONFIANZA CERO (ZTNA)	23
4.3.6. PROTECCIÓN DE LA INFORMACIÓN	24
4.3.6.1. FAMILIA: ALMACENAMIENTO CIFRADO DE DATOS	24
4.3.6.2. FAMILIA: CIFRADO Y COMPARTICIÓN SEGURA DE INFORMACIÓN	24
4.3.6.3. FAMILIA: HERRAMIENTAS DE BORRADO SEGURO.....	24
4.3.6.4. FAMILIA: SISTEMAS DE PREVENCIÓN DE FUGAS DE DATOS	24
4.3.6.5. FAMILIA: GESTIÓN DE METADATOS	24
4.3.6.6. FAMILIA: COPIAS DE SEGURIDAD	24
4.3.6.7. FAMILIA: SISTEMAS DE GESTIÓN DE BASES DE DATOS (DBMS).....	25
4.3.7. SOPORTE CRIPTOGRÁFICO	25
4.3.7.1. FAMILIA: HERRAMIENTAS PARA FIRMA ELECTRÓNICA	25
4.3.7.2. FAMILIA: <i>HARDWARE SECURITY MODULE</i> (HSM).....	25
4.3.7.3. FAMILIA: <i>INFRAESTRUCTURA PKI</i>	25
4.3.7.4. FAMILIA: DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS.....	25
4.3.8. PROTECCIÓN DE PLATAFORMAS	25
4.3.8.1. FAMILIA: DISPOSITIVOS MÓVILES	26
4.3.8.2. FAMILIA: SISTEMAS OPERATIVOS.....	26
4.3.8.3. FAMILIA: TARJETAS INTELIGENTES	26
4.3.8.4. FAMILIA: PLATAFORMAS CONFIABLES	26
4.3.8.5. FAMILIA: VIRTUALIZACIÓN	26
4.3.8.6. FAMILIA: HIPERCONVERGENCIA.....	26
4.3.8.7. FAMILIA: INFRAESTRUCTURAS DE ESCRITORIO VIRTUAL (VDI).....	27
4.3.8.8. FAMILIA: CONMUTADORES KVM	27
4.3.9. PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS	27
4.3.9.1. FAMILIA: CAMARAS IP	27
4.3.9.2. FAMILIA: HERRAMIENTAS DE GESTIÓN DE VÍDEO.....	27
4.3.9.3. FAMILIA: CONTROL DE ACCESO FÍSICO	27
4.3.10. SEGURIDAD OT	28
4.3.10.1. FAMILIA: ESTACIONES DE CARGA DE VEHÍCULOS ELÉCTRICOS	28
4.3.11. ESPACIO	28
4.3.11.1. FAMILIA: PRODUCTOS CRIPTOGRÁFICOS PARA ACCESO A SERVICIOS GNSS	28
4.3.12. OTRAS HERRAMIENTAS.....	28
5. TAXONOMÍA DE PRODUCTOS APROBADOS	29

5.1 CATEGORÍA: PROTECCIÓN EN ENTORNOS TÁCTICOS	29
5.1.1. FAMILIA: PLATAFORMAS Y DISPOSITIVOS TÁCTICOS CONFIABLES	30
5.1.2. FAMILIA: SOLUCIONES PARA PROTECCIÓN DE LAS COMUNICACIONES TÁCTICAS.....	31
5.1.3. FAMILIA: SISTEMAS DE INFORMACIÓN PARA ENTORNOS TÁCTICOS.....	31
6. TAXONOMÍA DE PRODUCTOS Y SERVICIOS DE CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD	32
6.1 FAMILIA: GOBERNANZA Y PLANIFICACIÓN DE LA SEGURIDAD	32
6.2 FAMILIA: NORMATIVA DE SEGURIDAD Y CONFORMIDAD	32
6.3 FAMILIA: ANÁLISIS Y GESTIÓN DE RIESGOS	32
6.4 FAMILIA: NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES	33
6.5 FAMILIA: INTERCAMBIO DE CIBERINTELIGENCIA.....	33
6.6 FAMILIA: FORMACIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD	33
7. PRODUCTOS DESPLEGADOS EN LA NUBE	34
8. REFERENCIAS	35
9. ABREVIATURAS	36

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 Seguridad¹.
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, BÁSICA²).
 - 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**

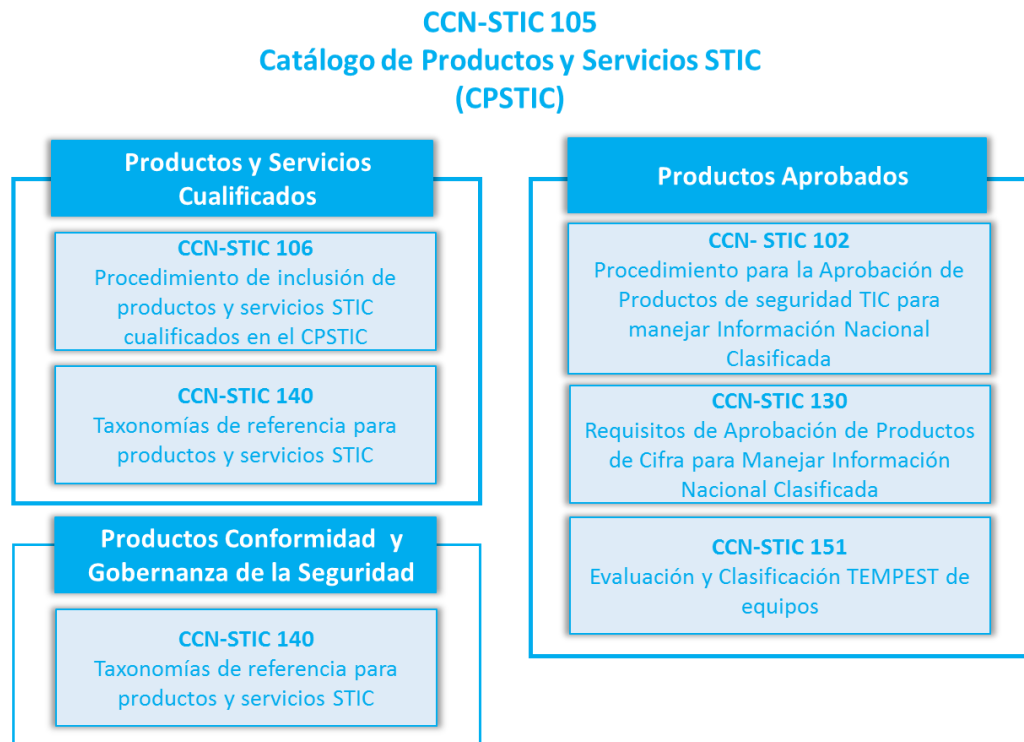
² Clasificación por categorías definida en el ENS.

de

equipos

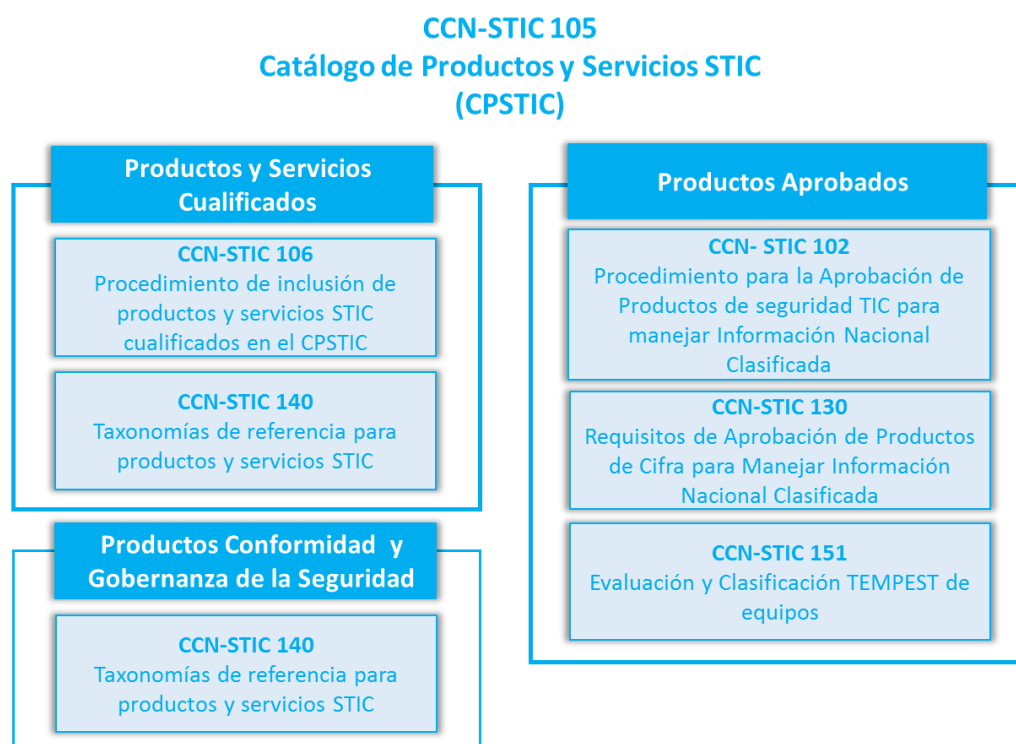
[4].

Ver



13. Figura 1. Clasificación del CPSTIC

14. 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].
15. 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

16. 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.
17. 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

18. 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).
19. 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.
20. 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.
21. 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

22. 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 electrónica³.
23. 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
24. 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).
25. 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.
26. 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

27. La Tabla 2 recoge el esquema de la taxonomía organizada en base a las categorías 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.

³ <https://www.boe.es/eli/es/rd/2022/05/03/311>

CATEGORÍA	FAMILIAS			
	NOMBRE	MEDIDAS	ANEXOS	
			ENS ALTO	ENS MEDIO
Control de accesos	Control de Acceso a Red (NAC ⁴)	[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 <i>Single Sign-On</i>	[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	
	Gestión de Acceso Privilegiado (PAM ⁵)	[op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7]	A.5	
	Gestión de Identidades (IM ⁶)	[op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7]	A.6	
	Autenticación Multi-Factor (MFA)	[op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6];	A.7	
	Herramientas de Videoidentificación	[mp.s.2]	A.8	A.8M

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

Protección de dispositivos	Anti-virus/EPP (<i>Endpoint Protection Platform</i>)	[op.exp.6]	B.1
	EDR (<i>Endpoint Detection and Response</i>)	[op.exp.6]	B.2
	Herramientas de gestión de dispositivos	[op.exp.3]	B.3
	Herramientas de sandbox	[op.mon.1]	B.4
Protección de redes y sistemas	Sistemas de gestión de eventos de seguridad (SIEM)	[op.exp.8]; [op.exp.9]; [op.exp.10]	C.1
	Sistemas de orquestación, automatización y respuesta de seguridad (SOAR)	[op.exp.8]; [op.exp.9];	C.2
	Herramientas de gestión de red	[op.exp.3]; [op.exp.7]	C.3
	Sistemas <i>Honeypot</i> / <i>Honeynet</i>	[op.mon.1]	C.4
	Detección y respuesta de amenazas en red (NDR)	[op.mon.1]	C.5
	Herramientas de actualización de sistemas	[op.exp.4]; [op.exp.5]	C.6
	CASB	[mp.s] Transversalmente: [mp.info]; [mp.acc]; [op.exp.2]	C.7
Protección de perímetro	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
	<i>Proxies</i>	[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
	Web Application Firewall (WAF)	[mp.com.1]; [mp.com.3]; [mp.com.4]	D.8
	Redes definidas por <i>software</i> (SDN)	[mp.com.1]; [mp.com.3]; [mp.com.4]	D.9
	Dispositivos de prevención y detección de intrusiones (IDS e IPS)	[mp.com.1]; [mp.com.2]; [mp.com.3];	D.10A
	Sistemas AntiDDoS	[mp.com.1]; [mp.com.2]; [mp.com.3];	D.10B
	Herramientas de filtrado de navegación	[op.exp.6]	D.11
	Protección de correo electrónico	Transversalmente: [op.acc.1]; [op.acc.5]; [mp.si.2]	D.12
	Balanceadores de carga	[mp.s.8]	D.13
Protección de comunicaciones	Herramientas de voz por IP (VoIP)	[mp.com.2]; [mp.com.3]	E.1
	Herramientas de mensajería instantánea (IM)		E.2
	Herramientas de videoconferencia		E.3
	Redes privadas virtuales: IPsec	[mp.com.2]; [mp.com.3]	E.4
	Redes privadas virtuales: TLS	[mp.com.2]; [mp.com.3]	E.5

	Redes privadas virtuales: Otras	[mp.com.2]; [mp.com.3]	E.6	
	Acceso a red de confianza cero (ZTNA)	[mp.com.2]; [mp.com.3]	E.7	
Protección de la información	Almacenamiento cifrado de datos	[mp.si.2]; [mp.info.3]	F.1	
	Cifrado y compartición segura de información	[mp.si.2]; [mp.info.3]	F.2	
	Herramientas de Borrado Seguro	[mp.si.5]	F.3	
	Sistemas de prevención de fugas de datos	[mp.info.2]	F.4	
	Gestión de metadatos	[mp.si.1]; [mp.info.5] Transversalmente: [op.mon.3]	F.5	
	Copias de seguridad	[mp.info.9]	F.6	
	Sistemas de Gestión de Bases de Datos (DBMS)	Control y requisitos de acceso. Configuración de seguridad Inventario de activos Mantenimiento y actualizaciones de seguridad	F.7	
Soporte criptográfico	Herramientas para firma electrónica	[mp.info.4]; [mp.info.5]	L.1	
	Módulo de Seguridad Hardware (HSM)	[mp.si.2]; [mp.info.3]	L.2	
	Infraestructura PKI	[mp.si.2]; [mp.info.3]	L.3	
	Dispositivos para gestión de claves criptográficas	[op.exp.11]	L.4	
	Dispositivos móviles	[mp.eq.3]	M.1	

Protección de plataformas	Sistemas operativos	[mp.eq.2] Transversalmente: [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.exp.8]	M.2	
	Tarjetas inteligentes	[mp.s.1]	M.3	
	Plataformas confiables	[mp.eq.2] Transversalmente: [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.exp.8]	M.4	
	Virtualización	[mp.eq.2] Transversalmente: [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.exp.8]	M.5	M.5M
	Hiperconvergencia	[mp.s] Transversalmente: [mp.com]; [op.cont] [mp.info.9]	M.6	M.6M
	Infraestructura de escritorio virtual (VDI)	[op.acc.4] [op.acc.6] [mp.eq.3] [mp.si]	M.7	M.7M
	Conmutadores KVM	[mp.com.3]; [mp.com.4]	M.8	
Protección de instalaciones e infraestructuras	Cámaras IP	[mp.if]	I.1	
	Herramientas de Gestión de vídeo	[mp.if]	I.2	
	Control de Acceso Físico	[mp.if]	I.3	
Seguridad OT	Estaciones de carga de vehículos eléctricos	-		O.1M

Espacio	Productos criptográficos para acceso a servicios GNSS	[mp.si.2]; [mp.info.3]	K.1	
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

28. Engloba las soluciones cuyo objetivo es garantizar que únicamente los usuarios, dispositivos o procesos autorizados puedan acceder a recursos, sistemas o datos, de acuerdo con las políticas de seguridad establecidas.

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

29. 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

30. 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

31. 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

32. 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: 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.

4.3.1.6. FAMILIA: GESTIÓN DE IDENTIDADES (IM)

34. Los productos asociados a la familia de Gestión de Identidades (*IM, Identity Management*) proporcionan a las organizaciones servicios centralizados 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.

4.3.1.7. FAMILIA: AUTENTICACIÓN MULTIFACTOR (MFA)

35. Los productos asociados a la familia de Autenticación Multi-Factor (*MFA, Multi-Factor Authentication*) surgen para dar respuesta a la necesidad que tienen las organizaciones de proteger las credenciales de los usuarios y los recursos a los que estos pueden acceder. Ayudan a implementar la autenticación de una forma centralizada, aportando distintos factores de autenticación⁷ que se ajustan a las diferentes situaciones y servicios de las organizaciones.

4.3.1.8. FAMILIA: HERRAMIENTAS DE VIDEOIDENTIFICACIÓN

36. 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.

⁷ Un *Factor de autenticación* es una evidencia que sirve para demostrar al usuario su identidad y, por lo tanto, superar la autenticación.

4.3.2. PROTECCIÓN DE DISPOSITIVOS

37. Engloba las soluciones que permiten registrar y supervisar la actividad de usuarios y procesos en los dispositivos finales, detectar comportamientos maliciosos o anómalos y, en algunos casos, reaccionar de forma automática o centralizada para prevenir, contener y responder ante incidentes de seguridad.

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

38. 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)

39. 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.
40. 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 DISPOSITIVOS (UEM)

41. 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.

4.3.2.4. FAMILIA: HERRAMIENTAS DE SANDBOX

42. 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.

4.3.3. PROTECCIÓN DE REDES Y SISTEMAS

43. Engloba las soluciones orientadas a proteger, supervisar, analizar y administrar la infraestructura de una organización, centrándose en la red en su conjunto y el tráfico que se transmite por la misma.

4.3.3.1. FAMILIA: SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM)

44. 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.

4.3.3.2. 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 procesamiento 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.

4.3.3.3. FAMILIA: HERRAMIENTAS DE GESTIÓN DE RED

46. 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.

4.3.3.4. FAMILIA: SISTEMAS HONEYPOT / HONEYNET

47. 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.

4.3.3.5. FAMILIA: DETECCIÓN Y RESPUESTA DE AMENAZAS EN RED (NDR)

48. Permiten monitorizar, capturar y analizar el tráfico y comportamiento de la red con el objetivo de identificar anomalías que representen posibles amenazas, utilizando para ello protocolos que capturan el comportamiento de los flujos de tráfico (telemetría) y, por extensión, el comportamiento de la red.

4.3.3.6. FAMILIA: HERRAMIENTAS DE ACTUALIZACIÓN DE SISTEMAS

49. 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.

4.3.3.7. FAMILIA: CASB

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

4.3.4. PROTECCIÓN DE PERÍMETRO

51. Engloba equipos de red o soluciones situados en los límites de una red, cuya función principal es controlar, filtrar y proteger el tráfico de datos que entra o sale de la red.
52. Su objetivo es establecer una primera línea de defensa frente a amenazas externas, asegurando que solo el tráfico legítimo, autorizado y conforme a las políticas de seguridad pueda atravesar el perímetro.

4.3.4.1. FAMILIA: ENRUTADORES

53. Proporcionan conectividad a nivel de red del modelo OSI⁸, 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

54. 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 MAC⁹ de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.

4.3.4.3. FAMILIA: CORTAFUEGOS

55. 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

56. 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.

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

⁹MAC (**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 separados por dos puntos.

4.3.4.5. FAMILIA: DISPOSITIVOS DE RED INALÁMBRICOS

57. 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

58. 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

59. 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: WEB APPLICATION FIREWALL (WAF)

60. 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.

4.3.4.9. FAMILIA: REDES DEFINIDAS POR SOFTWARE (SDN)

61. 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

4.3.4.10. FAMILIA: DISPOSITIVOS DE PREVENCIÓN Y DETECCIÓN DE INTRUSIONES

62. 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.

4.3.4.11. FAMILIA: Sistemas AntiDDoS

63. Los sistemas antiDDoS proporcionan detección, clasificación y mitigación de tráfico malicioso, orientada a garantizar la disponibilidad de los servicios de las organizaciones frente a ataques masivos. Principalmente, lleva a cabo estas funciones a través de análisis de tráfico, detección de anomalías y activación de mecanismos de mitigación.

4.3.4.12. FAMILIA: HERRAMIENTAS DE FILTRADO DE NAVEGACIÓN

64. 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 URL¹⁰, así como pueden limitar todo acceso a sitios no confiables o potencialmente peligrosos.

4.3.4.13. FAMILIA: PROTECCIÓN DE CORREO ELECTRÓNICO

65. 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.

4.3.4.14. FAMILIA: BALANCEADORES DE CARGA

66. 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.

4.3.5. PROTECCIÓN DE LAS COMUNICACIONES

4.3.5.1. FAMILIA: HERRAMIENTAS DE VOZ Y VÍDEO POR IP (VOIP)

67. 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.

4.3.5.2. FAMILIA: HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA (IM)

68. 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

¹⁰**URL (Uniform Resource Locator):** Localización Uniforme del Recurso. Es la forma en que se identifica un sitio en internet. Ej www.ccn.cni.es

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.

4.3.5.3. FAMILIA: HERRAMIENTAS DE VIDEOCONFERENCIA

69. 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.

4.3.5.4. FAMILIA: REDES PRIVADAS VIRTUALES (IPsec)

70. Destinados al cifrado de los canales de comunicación empleando IPsec, 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.

4.3.5.5. FAMILIA: REDES PRIVADAS VIRTUALES (TLS)

71. Destinados al cifrado de los canales de comunicación empleando TLS, 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.

4.3.5.6. FAMILIA: REDES PRIVADAS VIRTUALES (OTRAS)

72. 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.

4.3.5.7. FAMILIA: ACCESO A RED DE CONFIANZA CERO (ZTNA)

73. Los productos o servicios asociados a esta familia están orientados a definir condiciones específicas, así como garantizar el cumplimiento de las mismas por parte de los usuarios finales, a la hora de acceder a los recursos, aplicaciones o servicios de una organización. Este tipo de herramientas surgen con la motivación de segregar los recursos de una organización, de forma que solamente puedan

acceder aquellos usuarios que cumplan ciertos permisos específicos previamente definidos.

4.3.6. PROTECCIÓN DE LA INFORMACIÓN

74. Engloba las soluciones centradas en garantizar la confidencialidad e integridad de la información, tanto en reposo como en tránsito o en uso. Estos productos permiten prevenir accesos no autorizados, fugas de información y pérdidas de datos, garantizando su correcto ciclo de vida.

4.3.6.1. FAMILIA: ALMACENAMIENTO CIFRADO DE DATOS

75. 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.

4.3.6.2. FAMILIA: CIFRADO Y COMPARTICIÓN SEGURA DE INFORMACIÓN

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

4.3.6.3. FAMILIA: HERRAMIENTAS DE BORRADO SEGURO

77. 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.

4.3.6.4. FAMILIA: SISTEMAS DE PREVENCIÓN DE FUGAS DE DATOS

78. 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.

4.3.6.5. FAMILIA: GESTIÓN DE METADATOS

79. 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.

4.3.6.6. FAMILIA: COPIAS DE SEGURIDAD

80. 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.

4.3.6.7. FAMILIA: SISTEMAS DE GESTIÓN DE BASES DE DATOS (DBMS)

81. 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. SOPORTE CRIPTOGRÁFICO

4.3.7.1. FAMILIA: HERRAMIENTAS PARA FIRMA ELECTRÓNICA

82. 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.
83. Se indicará en las observaciones aquellos productos que cumplan con el Reglamento UE 910/2014 (eIDAS) para dispositivos cualificados de creación de firma electrónica.

4.3.7.2. FAMILIA: *HARDWARE SECURITY MODULE (HSM)*

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

4.3.7.3. FAMILIA: *INFRAESTRUCTURA PKI*

85. Una Infraestructura de Clave Pública (PKI) es un conjunto organizado de elementos, procedimientos y políticas que, mediante el uso de criptografía asimétrica, permite la gestión de certificados digitales y claves criptográficas.

4.3.7.4. FAMILIA: DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS

86. 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.

4.3.8. PROTECCIÓN DE PLATAFORMAS

87. Engloba las soluciones que proporcionan seguridad a nivel de plataforma (equipos sobre los que se procesa la información), y que en ocasiones ofrecen también una seguridad transversal, así como mecanismos de protección para servicios TIC específicos.

4.3.8.1. FAMILIA: DISPOSITIVOS MÓVILES

88. 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.

4.3.8.2. FAMILIA: SISTEMAS OPERATIVOS

89. 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.

4.3.8.3. FAMILIA: TARJETAS INTELIGENTES

90. 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.

4.3.8.4. FAMILIA: PLATAFORMAS CONFIABLES

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

4.3.8.5. FAMILIA: VIRTUALIZACIÓN

92. 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 (VMM¹¹)**, 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 (VM¹²)** que tiene asignados unos recursos virtuales, como memoria, procesador, sistema operativo invitado y aplicaciones.

4.3.8.6. FAMILIA: HIPERCONVERGENCIA

93. 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

¹¹ Virtual Machine Management

¹² Virtual Machine

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*.

4.3.8.7. FAMILIA: INFRAESTRUCTURAS DE ESCRITORIO VIRTUAL (VDI)

94. 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.

4.3.8.8. FAMILIA: CONMUTADORES KVM

95. 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.

4.3.9. PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS

96. Engloba las soluciones cuyo propósito es reforzar las medidas de protección física de las instalaciones e infraestructuras.

4.3.9.1. FAMILIA: CAMARAS IP

97. 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 vídeo.

4.3.9.2. FAMILIA: HERRAMIENTAS DE GESTIÓN DE VÍDEO

98. 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 vídeo. También permiten la administración centralizada del sistema de videovigilancia.

4.3.9.3. FAMILIA: CONTROL DE ACCESO FÍSICO

99. El sistema de control de acceso físico es un sistema centralizado formado por un conjunto de diferentes elementos que proporcionan una funcionalidad de autorización segura. Los componentes esenciales de un sistema de control de acceso físico son los lectores RFID, las unidades de control de acceso (UCA) y el software de gestión de todos los sistemas de seguridad.

4.3.10. SEGURIDAD OT

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

4.3.10.1. FAMILIA: ESTACIONES DE CARGA DE VEHÍCULOS ELÉCTRICOS

101. 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.

4.3.11. ESPACIO

4.3.11.1. FAMILIA: PRODUCTOS CRIPTOGRÁFICOS PARA ACCESO A SERVICIOS GNSS

102. Los productos pertenecientes a esta familia proporcionan los servicios criptográficos necesarios para el acceso a determinados servicios de navegación por satélite.

4.3.12. OTRAS HERRAMIENTAS

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

5. TAXONOMÍA DE PRODUCTOS APROBADOS

104. 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.
105. 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.
106. 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

107. 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.
108. 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.
109. 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:
110. 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.
111. 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 allá de los mecanismos COMSEC también cobran especial importancia otros aspectos como los mecanismos TRANSEC y NETSEC.
112. 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

113. 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).
114. En general, serán de aplicación los mismos Requisitos Fundamentales de Seguridad aplicables a la familia Plataformas Confiables.
115. 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

116. 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.
117. 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.
118. 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).
119. 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.
120. 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

121. 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.
122. 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

123. 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

124. 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

125. 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

126. 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

127. 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

128. 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

129. 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. PRODUCTOS DESPLEGADOS EN LA NUBE

130. Todos los productos y servicios que se implementen, desplieguen o estén disponibles en entornos de la nube deberán cumplir con las disposiciones establecidas en el Anexo G.

8. 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.

9. ABREVIATURAS

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

