

Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación





Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

NIPO: 083-24-034-4

Fecha de Edición: Diciembre de 2024

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

ÍNDICE.....	3
1. INTRODUCCIÓN	6
2. OBJETIVO.....	7
3. ALCANCE.....	7
4. INCLUSIÓN DE UN PRODUCTO DEL CPSTIC.....	8
5. REVISIÓN DE VALIDEZ DE PRODUCTOS STIC.....	9
6. EXCLUSIÓN DE UN PRODUCTO O SERVICIO DEL CPSTIC.....	10
7. PRODUCTOS CUALIFICADOS	11
7.1 HERRAMIENTAS PARA EL DESARROLLO DE PRODUCTOS DE SEGURIDAD	13
7.2 CONTROL DE ACCESO.....	15
7.2.1 CONTROL DE ACCESO A RED (NAC)	15
7.2.2 SERVIDORES DE AUTENTICACIÓN.....	17
7.2.3 GESTIÓN DE ACCESO PRIVILEGIADO (PAM).....	19
7.2.4 GESTIÓN DE IDENTIDADES (IM).....	20
7.3 SEGURIDAD EN LA EXPLOTACIÓN	25
7.3.1 ANTI-VIRUS / EPP (ENDPOINT PROTECTION PLATFORM).....	25
7.3.2 EDR (ENDPOINT DETECTION AND RESPONSE).....	33
7.3.3 HERRAMIENTAS DE GESTIÓN DE RED.....	41
7.3.4 HERRAMIENTAS DE FILTRADO DE NAVEGACIÓN.....	43
7.3.5 SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM)	44
7.3.6 DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS.....	54
7.4 MONITORIZACIÓN DE LA SEGURIDAD	56
7.4.1 IDS, IPS Y ANTIDDOS	56
7.4.2 CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO.....	68
7.4.3 HERRAMIENTAS DE SANDBOX.....	71
7.5 PROTECCIÓN DE LAS COMUNICACIONES.....	72
7.5.1 ENRUTADORES.....	72
7.5.2 SWITCHES	107
7.5.3 CORTAFUEGOS.....	145
7.5.4 PROXIES	180
7.5.5 DISPOSITIVOS DE RED INALÁMBRICOS.....	184
7.5.6 PASARELAS SEGURAS DE INTERCAMBIO DE DATOS	192
7.5.7 DIODOS DE DATOS.....	193
7.5.8 REDES PRIVADAS VIRTUALES: IPSEC	194
7.5.9 REDES PRIVADAS VIRTUALES: SSL.....	214
7.5.10 REDES PRIVADAS VIRTUALES: OTROS	216
7.5.11 HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA (IM)	217
7.5.12 HERRAMIENTAS VOZ IP	218
7.5.13 HERRAMIENTAS DE VIDEOCONFERENCIA	220

7.5.14	WEB APPLICATION FIREWALL (WAF).....	221
7.5.15	REDES DEFINIDAS POR SOFTWARE (SDN)	222
7.5.16	CIFRADORES IP	223
7.6	PROTECCIÓN DE LA INFORMACIÓN Y LOS SOPORTES DE LA INFORMACIÓN	224
7.6.1	ALMACENAMIENTO CIFRADO DE DATOS	224
7.6.2	CIFRADO Y COMPARTICIÓN SEGURA DE INFORMACIÓN	225
7.6.3	HERRAMIENTAS DE BORRADO SEGURO	229
7.6.4	SISTEMAS PARA PREVENCIÓN DE FUGAS DE DATOS.....	231
7.6.5	HERRAMIENTAS PARA FIRMA ELECTRÓNICA.....	232
7.6.6	HARDWARE SECURITY MODULE (HSM).....	235
7.6.7	GESTIÓN DE METADATOS.....	239
7.7	PROTECCIÓN DE EQUIPOS Y SERVICIOS.....	240
7.7.1	DISPOSITIVOS MÓVILES.....	240
7.7.2	SISTEMAS OPERATIVOS	254
7.7.3	PROTECCIÓN DE CORREO ELECTRÓNICO	256
7.7.4	BALANCEADORES DE CARGA	260
7.7.5	CASB.....	262
7.7.6	HIPERCONVERGENCIA	263
7.7.7	HERRAMIENTAS DE VIDEOIDENTIFICACIÓN	265
7.7.8	CONMUTADORES KVM	275
7.7.9	SISTEMAS DE GESTIÓN DE BASES DE DATOS (DBMS).....	279
7.8	OTRAS HERRAMIENTAS.....	280
7.8.1	OTRAS HERRAMIENTAS	280
7.9	SEGURIDAD OT.....	296
7.9.1	SEGURIDAD OT	296
8.	PRODUCTOS APROBADOS.....	297
8.1	HERRAMIENTAS PARA EL DESARROLLO DE PRODUCTOS DE SEGURIDAD	298
8.2	CONTROL DE ACCESO.....	299
8.2.1	CONTROL DE ACCESO A RED (NAC)	299
8.2.2	GESTIÓN DE IDENTIDADES (IM)	300
8.3	SEGURIDAD EN LA EXPLOTACIÓN	301
8.3.1	ANTI-VIRUS / EPP (ENDPOINT PROTECTION PLATFORM).....	301
8.3.2	EDR (ENDPOINT DETECTION AND RESPONSE).....	302
8.3.3	HERRAMIENTAS DE FILTRADO DE NAVEGACIÓN.....	303
8.3.4	SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM)	304
8.3.5	DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS.....	309
8.4	MONITORIZACIÓN DE LA SEGURIDAD	311
8.4.1	CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO.....	311
8.5	PROTECCIÓN DE LAS COMUNICACIONES.....	313
8.5.1	ENRUTADORES.....	313
8.5.2	SWITCHES	318

8.5.3	CORTAFUEGOS.....	326
8.5.4	PASARELAS SEGURAS DE INTERCAMBIO DE DATOS	327
8.5.5	DIODOS DE DATOS.....	329
8.5.6	HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA (IM)	330
8.5.7	HERRAMIENTAS VOZ IP	331
8.5.8	CIFRADORES IP.....	332
8.6	PROTECCIÓN DE LA INFORMACIÓN Y LOS SOPORTES DE LA INFORMACIÓN	335
8.6.1	CIFRADO Y COMPARTICIÓN SEGURA DE INFORMACIÓN	335
8.6.2	HERRAMIENTAS DE BORRADO SEGURO	337
8.6.3	GESTIÓN DE METADATOS.....	338
8.7	PROTECCIÓN DE EQUIPOS Y SERVICIOS.....	339
8.7.1	DISPOSITIVOS MÓVILES.....	339
8.7.2	SISTEMAS OPERATIVOS	341
8.7.3	PROTECCIÓN DE CORREO ELECTRÓNICO	342
8.7.4	HIPERCONVERGENCIA	343
8.8	OTRAS HERRAMIENTAS.....	344
8.8.1	OTRAS HERRAMIENTAS	344
8.9	COMUNICACIONES TÁCTICAS SEGURAS	346
8.9.1	PLATAFORMAS Y DISPOSITIVOS TÁCTICOS CONFIABLES.....	346
8.9.2	SOLUCIONES PARA PROTECCIÓN DE LAS COMUNICACIONES TÁCTICAS.....	348
8.10	TEMPEST	353
8.10.1	ARMARIOS APANTALLADOS	353
8.10.2	MONITORES.....	356
8.10.3	PERIFÉRICOS	357
8.10.4	CPU	359
8.10.5	IMPRESORAS	360
8.10.6	SERVIDOR	361
9.	PRODUCTOS Y SERVICIOS DE CONFORMIDAD Y GOBERNANZA DE LA	
	SEGURIDAD	362
9.1	GOBERNANZA Y PLANIFICACIÓN DE LA SEGURIDAD	363
9.2	ANÁLISIS Y GESTIÓN DE RIESGOS.....	364
9.3	NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES.....	365
9.4	FORMACIÓN Y CONCENCIACIÓN	366
10.	REFERENCIAS	370
11.	ABREVIATURAS	371

1. INTRODUCCIÓN

1. La adquisición de un producto o la contratación de un servicio 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 o servicio son adecuados para proteger dicha información.
2. La evaluación y certificación de un producto o servicio de seguridad TIC es el único medio objetivo que permite valorar y acreditar su capacidad 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 la comunicación y 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)**. 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 dos (2) partes: **Productos Aprobados** y **Productos y Servicios Cualificados**. En el apartado de **Productos Aprobados** se recogen aquellos productos que se consideran adecuados para el manejo de información clasificada, mientras que en el apartado de **Productos y Servicios 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).

TIPO DE PRODUCTO O SERVICIO	INFORMACIÓN QUE MANEJA
APROBADO	CLASIFICADA
CUALIFICADO	SENSIBLE (ENS)

Tabla 1. Tipos de productos o servicios incluidos en el CPSTIC

2. OBJETIVO

7. El objeto de este documento es el de presentar el Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicación que recoge un listado de productos aprobados para el manejo de información clasificada y de productos y servicios cualificados para el manejo de información sensible, de forma que pueda servir de referencia a la Administración Pública.

3. ALCANCE

8. En el apartado de Productos Cualificados de este documento se incluyen todos aquellos que han superado con éxito el proceso de inclusión en el CPSTIC descrito en la guía CCN-STIC 106 Procedimiento de inclusión de productos y servicios de seguridad TIC cualificados en el CPSTIC [1] y que por lo tanto se consideran cualificados para ser utilizados en sistemas de Categoría Alta en el ENS.
9. Este hecho implica que todos ellos poseen una certificación funcional Common Criteria en la que se incluyen los Requisitos Fundamentales de Seguridad (RFS) descritos en la guía CCN-STIC 140 Taxonomías de referencia para productos de seguridad TIC [2] para la familia en la que se consideran o que, en ausencia de productos que posean la certificación requerida, se han añadido de acuerdo al supuesto de excepcionalidad tras haber superado una evaluación STIC complementaria.
10. En el caso de productos multipropósito, éstos pueden aparecer en una o varias familias, siempre y cuando se haya certificado que cumplen con los RFS correspondientes a cada una de ellas. En estos casos, que un producto se considere cualificado para una determinada familia de productos no implica que lo esté para el resto de las familias en las que pueda encuadrarse, al margen de que implemente la funcionalidad asociada.
11. En el apartado de Productos Aprobados se incluyen todos aquellos que han superado con éxito el proceso de inclusión en el CPSTIC descrito en la guía CCN-STIC 102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada [3] y que por lo tanto se consideran aprobados para manejar información clasificada. El nivel máximo de clasificación de la información para la que se aprueba su uso vendrá especificado en cada producto de manera individual.

4. INCLUSIÓN DE UN PRODUCTO DEL CPSTIC

12. Para la inclusión de un producto o servicio en el catálogo, el CCN tendrá en cuenta los siguientes criterios:
- a) En el caso de **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 y Servicios Cualificados**, la máxima categoría del sistema de información en el que puede emplearse (ALTA, MEDIA, BÁSICA¹).
 - c) Las funcionalidades de seguridad que implementa el producto o servicio y las certificaciones aportadas.
 - d) Otros aspectos como el análisis de riesgos del producto o servicio, la necesidad operativa dentro de la Administración, la disponibilidad o no de otros productos o servicios certificados que satisfagan la misma funcionalidad, etc.

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

13. 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** [3]. 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** [4] y para realizar la evaluación TEMPEST se describe en la guía **CCN-STIC 151 Evaluación y Clasificación TEMPEST de equipos** [5]. Ver **Figura 1**.
14. El producto o servicio STIC 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 un procedimiento de empleo seguro. Dicho procedimiento será distribuido por la empresa fabricante junto con el producto y además se publicará como una guía CCN-STIC de la serie 1000.

¹ Clasificación por categorías definida en el ENS.

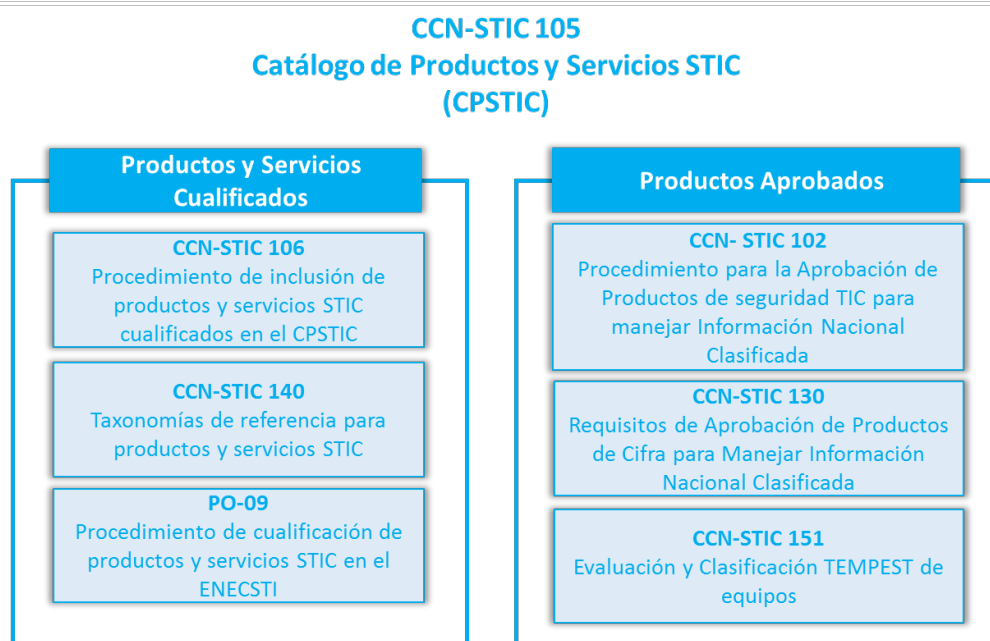


Figura 1. Inclusión de productos y servicios de seguridad en el CPSTIC

5. REVISIÓN DE VALIDEZ DE PRODUCTOS STIC

15. Periódicamente se realizará una revisión de validez de los productos y servicios incluidos en el catálogo con el fin de garantizar que siguen cumpliendo con los requisitos exigidos para formar parte de él. La fecha de revisión de validez se indica en la ficha correspondiente a cada producto.
16. Por esta razón, tras una revisión de validez, un producto o servicio incluido en el catálogo puede bajar el máximo nivel de clasificación que está autorizado a procesar en el caso de los productos aprobados e incluso puede ser excluido cuando se dejen de cumplir los requisitos exigidos para su inclusión.

6. EXCLUSIÓN DE UN PRODUCTO O SERVICIO DEL CPSTIC

17. Un producto o servicio podrá ser excluido del CPSTIC por cualquiera de los siguientes motivos:
 - a) Caducidad del certificado de Producto o Servicio Cualificado STIC. Todos los certificados serán emitidos con una fecha de revisión de validez (que dependerá de la familia considerada), a partir de la cual el solicitante deberá remitir una nueva solicitud de inclusión siguiendo el procedimiento descrito anteriormente. En el caso de que esta solicitud no se lleve a cabo, el CCN podrá excluir el producto o servicio del CPSTIC.
 - b) Revocación o caducidad de alguna de las certificaciones requeridas al producto o servicio para acceder al catálogo: *Common Criteria*, LINCE, conformidad con el ENS, según el caso.
 - c) Pérdida de las condiciones de excepcionalidad. En el caso de que el producto o servicio haya sido incluido en el catálogo por alguno de los supuestos de excepcionalidad, podrá ser excluido una vez deje de cumplirse alguno de ellos: aparición de productos o servicios sustitutivos con la certificación adecuada, pérdida de la consideración de producto o servicio estratégico para la Administración, etc.
 - d) Que no cumpla con los RFS vigentes en el momento de la revisión de validez. Los avances tecnológicos pueden dejar obsoleta la tecnología empleada en unos casos y en otros hacer que se reduzca de forma considerable la seguridad del mismo, lo que implicará una evolución de los RFS.
 - e) Que presente vulnerabilidades críticas no corregidas. En este caso, podrá solicitarse al fabricante un informe de impacto de dichas vulnerabilidades. Si este informe determinase que la vulnerabilidad es explotable siguiendo el PES, este será excluido del catálogo.

7. PRODUCTOS CUALIFICADOS

PRODUCTOS CUALIFICADOS





INFORMACIÓN IMPORTANTE

Todos los productos o servicios incluidos en este apartado han superado un proceso de evaluación/certificación en el que se ha comprobado que implementan, con cierto nivel de garantía, las funcionalidades de seguridad requeridas por los Requisitos Fundamentales de Seguridad definidos en la CCN-STIC-140 para la familia o familias a las que pertenecen.

Esta garantía avala su robustez frente a atacantes con un potencial determinado por el tipo de certificación que presentan, que en ningún caso alcanza el potencial que suelen presentar aquellos ataques motivados por estados.

Asimismo, el proceso de Cualificación no supone, en ningún caso, un posicionamiento del CCN sobre la fiabilidad del fabricante o proveedor de servicio. Esto tendría impacto en aquellos productos o servicios que, por su arquitectura, envían información de usuario a servidores externos a la organización controlados por el fabricante o proveedor de servicio, cuyas malas prácticas podrían derivar en divulgación no autorizada de datos de usuario o en su utilización con fines no declarados.

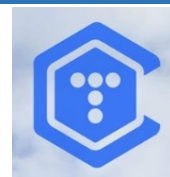
Estos aspectos son riesgos inherentes al producto o servicio que el Responsable de Seguridad del Sistema deberá valorar y, en caso de que resulten inasumibles, mitigar.

INFORMACIÓN IMPORTANTE

7.1 HERRAMIENTAS PARA EL DESARROLLO DE PRODUCTOS DE SEGURIDAD

Módulo criptográfico para aplicaciones móviles Telcryp

Versión	1.11
Fabricante	Cryptographic and Security System (CS2)
Familia	-
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/10/2025



Descripción

Este módulo provee los servicios de cifrado y seguridad para garantizar la comunicación tanto con el servidor IMS como con los terminales remotos con un cifrado extremo a extremo.

Este módulo criptográfico está diseñado como una librería criptográfica e incorporado a aplicaciones de comunicaciones en entorno de movilidad debidamente aprobadas, e instaladas en plataformas confiables.

Observaciones

Procedimiento de empleo pendiente de publicación

Biblioteca Criptográfica BOTAN-CCN

Versión	2.19.3
Fabricante	Centro Criptológico Nacional
Familia	-
Tipo	Producto
Categoría ENS	N/A
Fecha Inclusión	01/10/2020
Revisión de Validez	31/12/2024



Descripción

La biblioteca criptográfica BOTAN-CCN implementa los mecanismos criptográficos aceptados por el CCN para su uso en el desarrollo de productos de seguridad. Incluye código fuente y binarios compatibles con sistemas Windows y Linux. Incluye generadores de ruido y test de todas los mecanismos implementados

Observaciones

No aplica

INFORMACIÓN IMPORTANTE

TRNG-P200 Physical True Random Number Generator

Versión	1.11
Fabricante	BERTEN DSP
Familia	-
Tipo	Producto
Categoría ENS	N/A
Fecha Inclusión	01/10/2020
Revisión de Validez	31/12/2024

**Descripción**

El IP Core TRNG-P200 es un Generador de Números Aleatorios Verdaderos (TRNG, True Random Number Generator) implementable en cualquier diseño criptográfico basado en FPGA, SoC o ASIC. Utiliza una fuente física de entropía no determinista basada en osciladores multifase, que genera números aleatorios de alta calidad estadística en un área mínima. Genera simultáneamente la secuencia aleatoria de la fuente de entropía, y dos salidas post procesadas con un filtro de paridad y un codificador polinómico configurable. Es portable a cualquier dispositivo Xilinx, Intel o Microsemi y cumple con los requisitos definidos en las baterías de test Diehard, NIST 800-22 y AIS-31 PTG.2. Además, implementa un conjunto de pruebas de integridad (health tests), de acuerdo con NIST 800-90B, FIPS 140-2 y AIS-31. La generación de secuencias es monitorizada continuamente, activando alarmas en caso de fallos. El TRNG-P200 incluye interfaces AMBA-AXI y un mapa de registros con parámetros programables para configurar la velocidad de salida, el codificador polinómico, las pruebas de integridad, y la gestión de las alarmas. El producto incluye funciones ANSI C para la configuración de estos registros en el sistema criptográfico. <https://www.bertendsp.com/products/trng-p200/>

Observaciones

No aplica

INFORMACIÓN IMPORTANTE

7.2 CONTROL DE ACCESO

7.2.1 CONTROL DE ACCESO A RED (NAC)

Aruba ClearPass Policy Manager	
Versión	6.11
Fabricante	HPE Aruba Networking
Familia	Control de acceso a red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	06/05/2024
Revisión de Validez	31/12/2024
Descripción La familia de productos ClearPass de seguridad para el control de acceso a la red ofrece elaboración de perfiles, autenticación y autorización para usuarios, sistemas y dispositivos que intentan acceder a los recursos de TI. ClearPass se ha diseñado para abordar los retos de seguridad asociados con una organización TI: Acceso seguro a la red (802.1X y Radius), funciones de NAC, Implementación de portal de Invitados e interno, soporte de funcionalidades BYOD, integración con Firewalls (PaloAlto, CheckPoint, Fortinet y mas) todo ello mediante la integración múltiples fuentes de autenticación (Directorios activos, LDAP, BBDD y proveedores externos de identidad)	
Observaciones Procedimiento de Empleo Seguro pendiente de publicación	



Forescout 8.3 (CT-R, CT-100, CT-1000, CT-2000, CT-4000, CT-10000, CEM-5, CEM-10, CEM-25, CEM-50, CEM-100, CEM-150, CEM-200, 4130, 5110, 5120, 5140, 5160)	
Versión	8.4
Fabricante	Forescout
Familia	Control de acceso a red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2023
Revisión de Validez	01/04/2025
Descripción La plataforma Forescout es una plataforma unificada de seguridad que permite a las empresas y organismos oficiales obtener información completa sobre el estado de sus entornos empresariales ampliados y orquestar medidas destinadas a reducir el riesgo operativo y de ciberseguridad. Se despliega de forma rápida y segura en entornos de campus, centros de datos, la nube y redes de OT. Ofrece descubrimiento, clasificación en tiempo real y evaluación continua de estado, sin necesidad de agentes. Para más información, véase: https://forescouttechnologies.es	
Observaciones CCN-STIC-1106 Procedimiento de empleo seguro Forescout	



INFORMACIÓN IMPORTANTE

Cisco Identity Services Engine (ISE) 3500 series (SNS-3595), 3600 series (SNS-3615, SNS-3655, SNS-3695), ISE-VM

Versión	V 3.1
Fabricante	Cisco Systems
Familia	Control de acceso a red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2024
Revisión de Validez	31/08/2026

**Descripción**

Cisco® Identity Services Engine (ISE) es la solución integral para optimizar la administración de las políticas de seguridad. Con ISE, puede ver los usuarios y los dispositivos y controlar el acceso a la red corporativa a través de conexiones cableadas, inalámbricas, VPN y 5G.

Cisco Identity Services Engine potencia la resiliencia de la seguridad con la flexibilidad y las opciones necesarias para alojar el software de Cisco como cargas de trabajo en varias nubes más allá del soporte local y mantener la continuidad empresarial en medio de la incertidumbre. Esto permite a los clientes obtener un enfoque más modernizado para implementar los servicios de NAC desde la nube. Al pasar de administrar la infraestructura en una caja a aprovechar la infraestructura como código (IaC) en las implementaciones híbridas. Los equipos ganan agilidad con el aprovisionamiento Zero Trust y la flexibilidad a la hora de automatizar su entorno durante todo el ciclo de vida de la administración de Cisco ISE. ISE es el elemento central para un acceso de confianza cero al lugar de trabajo (infraestructura autogestionada) con el objetivo de reducir el riesgo, proteger la integridad y acelerar el acceso seguro a la red a través de la red distribuida.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

OpenNac Enterprise

Versión	1.2
Fabricante	Cipherbit – Grupo Oesia
Familia	Control de acceso a red (NAC)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2020
Revisión de Validez	31/12/2024

**Descripción****Observaciones**

CCN-STIC-1105 Procedimiento de empleo seguro EMMA

INFORMACIÓN IMPORTANTE

7.2.2 SERVIDORES DE AUTENTICACIÓN

Aruba ClearPass Policy Manager

Versión	6.11
Fabricante	HPE Aruba Networking
Familia	Servidores de Autenticación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	06/05/2024
Revisión de Validez	31/12/2024

aruba

a Hewlett Packard
Enterprise company



Descripción

La familia de productos ClearPass de seguridad para el control de acceso a la red ofrece elaboración de perfiles, autenticación y autorización para usuarios, sistemas y dispositivos que intentan acceder a los recursos de TI. ClearPass se ha diseñado para abordar los retos de seguridad asociados con una organización TI: Acceso seguro a la red (802.1X y Radius), funciones de NAC, Implementación de portal de Invitados e interno, soporte de funcionalidades BYOD, integración con Firewalls (PaloAlto, CheckPoint, Fortinet y mas) todo ello mediante la integración múltiples fuentes de autenticación (Directorios activos, LDAP, BBDD y proveedores externos de identidad)

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Location-Based Identity Platform

Versión	N/A
Fabricante	Ironchip Telco, S.L.
Familia	Servidores de Autenticación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/04/2026

**Descripción**

La solución de Ironchip Location-Based Identity Platform (LBAuth) representa una avanzada plataforma de gestión de accesos y protección de identidades basada en inteligencia artificial de localización. Esta plataforma permite la configuración de políticas de seguridad innovadoras, con el objetivo de evitar la suplantación de identidades y el acceso no autorizado a los servicios protegidos.

La plataforma centralizada Ironchip LBAuth incluye integraciones preconfiguradas que el administrador puede completar siguiendo pasos sencillos, protegiendo de esta manera todos los servicios de tecnología de la información de la empresa.

Los usuarios son integrados dinámicamente en la plataforma, lo que posibilita la gestión de permisos tanto individuales como grupales, mediante la aplicación de diversos métodos de acceso y políticas de seguridad. Esto asegura una protección sólida para los servicios más críticos de la organización.

Las características clave de esta solución incluyen:

- Gestión de privilegios basada en roles: Esta característica permite establecer diferentes niveles de privilegios de usuario, previniendo así el acceso no autorizado al resto del sistema.
- Restricción de acceso desde lugares no autorizados: La plataforma genera acceso habilitado únicamente desde áreas autorizadas, llevando la seguridad de la empresa al siguiente nivel y garantizando que solo personas autorizadas tengan acceso a los recursos protegidos.
- Monitorización de accesos en tiempo real: La plataforma documenta la actividad de los usuarios, permitiendo a los administradores visualizar el acceso en una línea de tiempo. Además, ofrece la posibilidad de generar informes detallados que pueden ser descargados para un control completo del sistema.

Observaciones

CCN-STIC 1633 Procedimiento de Empleo Seguro Location-Based Identity Platform IRONCHIP

INFORMACIÓN IMPORTANTE

7.2.3 GESTIÓN DE ACCESO PRIVILEGIADO (PAM)

Safeguard for Privileged Passwords	
Versión	7.0
Fabricante	One Identity
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2024
Revisión de Validez	31/07/2026
Descripción	  Safeguard for Privileged Passwords (SPP) es una solución de seguridad de gestión de cuentas privilegiadas cuya función principal es prevenir el mal uso potencial de las cuentas privilegiadas en los sistemas IT locales, híbridos o en la nube, así como las aplicaciones de las organizaciones, permitiendo almacenar, gestionar y monitorizar el uso de estas cuentas por parte de los usuarios. SPP automatiza, controla y asegura la gestión de credenciales privilegiadas con un acceso basado en roles y flujos automatizados. - Arquitectura escalable basada en dispositivos físicos o virtuales en alta disponibilidad escalable en modelo Activo-Activo-Activo. - Gestión del acceso basado en un motor de políticas, flujos de aprobación y revisión, etc. - Informes de auditoría de la actividad registrada en los dispositivos. - Importar, descubrir y rotado automático de cuentas privilegiadas y contraseñas de los sistemas y aplicaciones. - Gestión de cuentas de servicio, IIS, tareas programadas y COM+ en entornos Microsoft. - Integración con Safeguard for Sessions para extender las capacidades del SPP para la grabación de sesiones, análisis de comportamiento y detección. - Gestión de secretos en entornos DevOps y RPA. - Integración con sistemas externos mediante RestAPI Observaciones CCN-STIC-1110 Procedimiento de Empleo Seguro Safeguard for Privileged Passwords (SPP)

INFORMACIÓN IMPORTANTE

7.2.4 GESTIÓN DE IDENTIDADES (IM)

AWS Cognito

Versión
Fabricante AWS

Familia Gestión de identidades (IM)

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 17/09/2024

Revisión de Validez 28/02/2025


Amazon Cognito


Descripción

Amazon Cognito permite añadir registro de usuarios, inicio de sesión y control de acceso a sus aplicaciones web y móviles de forma rápida y sencilla. Con Amazon Cognito, se pueden escalar a millones de usuarios y admite el inicio de sesión con proveedores de identidad social como Apple, Facebook, Twitter o Amazon, con soluciones de identidad SAML 2.0 o utilizando su propio sistema de identidad. Además, Amazon Cognito permite guardar datos localmente en los dispositivos de los usuarios, lo que permite que sus aplicaciones funcionen incluso cuando los dispositivos están desconectados. A continuación, se pueden sincronizar los datos entre los dispositivos de los usuarios para que la aplicación siga siendo coherente independientemente del dispositivo que utilicen. Con Amazon Cognito, puede centrarse en las aplicaciones y despreocuparse de la administración de usuarios, la autenticación y la sincronización entre dispositivos.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

AWS Identity Access Management (IAM) + AWS STS

Versión**Fabricante** AWS**Familia** Gestión de identidades (IM)**Tipo** Servicio**Categoría ENS** ALTA**Fecha Inclusión** 01/08/2022**Revisión de Validez** 31/12/2024**Descripción**

AWS Identity and Access Management (IAM) permite controlar de forma segura el acceso a los servicios y recursos de AWS para sus usuarios, grupos y roles de AWS. Se pueden crear y administrar controles de acceso de grano fino con permisos, especificar quién puede acceder a qué servicios y recursos, y bajo qué condiciones.

Suministra la capacidad de administrar los permisos de AWS para sus usuarios y cargas de trabajo en el Centro de Identidad de AWS IAM. Permite administrar el acceso de los usuarios en varias cuentas de AWS, habilitar un servicio de alta disponibilidad, gestionar fácilmente el acceso a varias cuentas y los permisos de todas sus cuentas en las organizaciones de AWS de forma centralizada. El Centro de Identidades de IAM incluye integraciones SAML incorporadas a muchas aplicaciones empresariales, como Salesforce, Box y Microsoft Office 365.

Permite especificar el acceso a los recursos de AWS mediante permisos. Las entidades de IAM (usuarios, grupos y roles) comienzan por defecto sin permisos. A estas identidades se les pueden conceder permisos adjuntando una política de IAM que especifique el tipo de acceso, las acciones que se pueden realizar y los recursos en los que se pueden realizar las acciones.

Los roles de IAM permiten delegar el acceso a usuarios o servicios que normalmente no tienen acceso a los recursos de AWS de su organización. Los usuarios de IAM o los servicios de AWS pueden asumir un rol para obtener una credencial de seguridad temporal que se utilizará para realizar llamadas a la API de AWS. AWS Security Token Service (STS) se integra junto a AWS IAM para proporcionar un servicio web que permite solicitar credenciales temporales (tokens) con privilegios limitados a los usuarios. Estos tokens son los encargados de proporcionar a las identidades de AWS IAM los diferentes permisos de acceso a los recursos de AWS.

Para más información: https://aws.amazon.com/iam/?nc1=h_ls

Observaciones

CCN-STIC-887A Guía de configuración segura AWS

**INFORMACIÓN IMPORTANTE**

One Identity Manager

Versión v 9.0

Fabricante One Identity

Familia Gestión de identidades (IM)

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/01/2024

Revisión de Validez 30/06/2026

**Descripción**

One Identity Manager es una solución de gobierno y gestión de identidades (IAM) que permite automatizar la gestión de los accesos de los usuarios, permitiendo que accedan a las aplicaciones y a los datos estrictamente necesarios para desempeñar su trabajo. La solución permite que la administración de los usuarios, sus identidades digitales y sus accesos puedan ser impulsadas por otros departamentos como RRHH. Permite:

- Gestionar el acceso a recursos en las instalaciones, en la nube e híbridos desde cualquier departamento de la organización.
- Reducir el riesgo al asegurarse de que los usuarios tengan solo los accesos que necesitan.
- Satisfacer auditorías e iniciativas de cumplimiento con políticas de confirmación/recertificación.
- Otorgar derechos de acceso en función de roles, reglas y políticas definidas.
- Establecer procesos estándares de aprovisionamiento y desaproveccionamiento para sus empleados y proveedores.
- Administrar de forma rápida y fácil el acceso a recursos a medida que las responsabilidades del usuario evolucionen con la empresa.

Observaciones

CCN-STIC-1107 Procedimiento de Empleo Seguro One Identity Manager

INFORMACIÓN IMPORTANTE

SailPoint IdentityIQ

Versión	V8.3p2
Fabricante	Sailpoint
Familia	Gestión de identidades (IM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2023
Revisión de Validez	31/12/2025

**Descripción**

Sailpoint es una plataforma de Gestión de Identidades y Accesos que ofrece una amplia gama de funcionalidades, lo que lo convierte en una solución integral para la gestión de las identidades en las organizaciones.

- Provisionamiento: onboarding de nuevos usuarios, cambios y desprovisionamiento, automatización en los procesos. Para usuarios internos, colaboradores y/o proveedores.
- Gobierno de acceso: Visibilidad completa de los accesos de la organización, certificación de acceso, cumplimiento de acceso según políticas de usuarios a aplicaciones y datos.
- Gestión de contraseñas.
- Segregación de funciones.
- Gobierno de nube.

Observaciones

CCN-STIC-1111 SAILPOINT IdentityIQ

INFORMACIÓN IMPORTANTE

AWS IAM Identity Center

Versión**Fabricante** AWS**Familia** Gestión de identidades (IM)**Tipo** Servicio**Categoría ENS** ALTA**Fecha Inclusión** 01/06/2023**Revisión de Validez** 31/12/2024**Descripción**

AWS IAM Identity Center (sucesor de AWS Single Sign-On) es un servicio en la nube que facilita la administración centralizada del acceso a varias cuentas de AWS y aplicaciones empresariales.

Con AWS IAM Identity Center, puede administrar fácilmente el acceso centralizado y los permisos de usuario para todas sus cuentas de AWS Organizations. AWS IAM Identity Center también incluye integraciones incorporadas con aplicaciones de AWS, y muchas aplicaciones empresariales, como Salesforce, Box y Microsoft Office 365. Además, mediante el asistente de configuración de aplicaciones de AWS IAM Identity Center, puede crear integraciones de Security Assertion Markup Language (SAML) 2.0 y ampliar el acceso SSO a cualquiera de sus aplicaciones compatibles con SAML.

Sus usuarios solo tienen que iniciar sesión en un portal de usuario con las credenciales que configuren en AWS IAM Identity Center o utilizando sus credenciales corporativas existentes para acceder a todas sus cuentas y aplicaciones asignadas desde un único lugar.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

**INFORMACIÓN IMPORTANTE**

7.3 SEGURIDAD EN LA EXPLOTACIÓN

7.3.1 ANTI-VIRUS / EPP (ENDPOINT PROTECTION PLATFORM)

GravityZone	
Versión	
Fabricante	Bitdefender
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/06/2024
Revisión de Validez	31/01/2025
Descripción	La plataforma Bitdefender GravityZone es una plataforma integral de ciberseguridad que protege a toda la organización, brindando capacidades de prevención, protección, detección y respuesta (EDR/XDR/MDR) para organizaciones de todos los tamaños en servidores, cargas de trabajo y sistemas de usuario final de múltiples nubes híbridas, incluidas PC, portátiles y dispositivos móviles. La arquitectura de defensa en profundidad de GravityZone integra conocimiento y control de seguridad en una consola de administración unificada desde la cual los administradores monitorean y administran de manera centralizada el riesgo de ciberseguridad. Además, la consola de administración brinda capacidades para que los equipos de seguridad investiguen y solucionen incidentes. El rendimiento está optimizado específicamente para entornos de nube y virtualización, para minimizar el impacto de seguridad en la computación en la nube y los recursos virtualizados Observaciones Procedimiento de Empleo Seguro pendiente de publicación.

Bitdefender



Stormshield Endpoint Security Evolution	
Versión	2.5.3
Fabricante	Stormshield
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2024
Revisión de Validez	30/11/2026
Descripción	Stormshield Endpoint Security Evolution ofrece una ciberseguridad de nueva generación para garantizar la protección completa de terminales y servidores. Basado en la tecnología de análisis de comportamiento sin firmas, el agente reconoce las técnicas de ataque, como la explotación de las vulnerabilidades de las aplicaciones o las acciones características del ransomware. Una vez identificada la amenaza, se puede tomar cualquier acción deseada, como el cierre de procesos o el bloqueo de las conexiones de red (cuarentena de equipos infectados, restricción de túnel VPN o de uso de redes Wi-Fi). Observaciones CCN-STIC-1221 Procedimiento de empleo seguro Stormshield Endpoint Security Evolution



STORMSHIELD


INFORMACIÓN IMPORTANTE

Deep Security (Manager y Agente/Relay Linux/Windows)

Versión	11
Fabricante	Trend Micro
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/03/2025

**Descripción**

Deep Security es la respuesta de Trend Micro para proteger el cloud híbrido ya sean servidores físicos o virtuales.

Gracias a su agente ligero, el cual incorpora funcionalidades: EDR (con respuesta frente a amenazas conocidas, zero-day), envío de telemetría a la plataforma XDR de Trend Micro (VisionOne), reputación web, control de aplicaciones, supervisión de logs, Supervisión de Integridad (FIM), Firewall de Host y Host IPS (que incorpora la tecnología de parchado virtual), ayuda a mejorar la postura de seguridad proporcionando seguridad, visibilidad y control. La cualificación abarca los siguientes componentes: Manager, Agente/Relay Linux y el Agente/Relay Windows. El Virtual Appliance no está cualificado.

Observaciones

CCN-STIC-1216 PES Trendmicro Deep Security

Trellix Endpoint Solution

Versión	Trellix Endpoint Security 10.7.x with ePolicy Orchestrator 5.10.x
Fabricante	Trellix
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	20/09/2024
Revisión de Validez	28/02/2025

Trellix

**Descripción**

Trellix Endpoint Security es una solución flexible y unificada que protege los dispositivos corporativos, lo que permite a las organizaciones abordar problemas de seguridad complejos y distribuidos de forma exhaustiva, eficiente y rápida. Utiliza análisis y aprendizaje automático para lograr una eficacia líder en el sector, al tiempo que ofrece la flexibilidad de integrarse fácilmente con terceros. La solución le ayuda a unificar su seguridad contra amenazas desde el dispositivo hasta el Cloud.

La solución implementa un modelo de futuro en el que la seguridad es un sistema integrado, más simple e inteligente.

Previene, detecta, investiga y responde a las amenazas mientras gestiona eficazmente la infraestructura. Permite simplificar las investigaciones, y realizar investigaciones guiadas por IA.

Respuesta eficaz a las amenazas mediante servicios integrados de detección y respuesta ampliadas (XDR), detección y respuesta gestionadas (MDR), API abiertas y aplicaciones de terceros.

Trellix Endpoint Security es un conjunto integrado de tecnologías que utiliza análisis y aprendizaje automático para proporcionar una protección eficaz.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

WatchGuard EPDR/Advanced EPDR

Versión	4.2 (Protection Agent v8.0)
Fabricante	WatchGuard Technologies
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/03/2023
Revisión de Validez	31/03/2025

**Descripción**

WatchGuard EDR/EPP integra en una única solución un conjunto completo de tecnologías preventivas en el endpoint, con capacidades EDR y el Servicio Zero-Trust Application. Extiende las capacidades de prevención, detección y respuesta con una gama completa de capacidades de protección del endpoint necesarias para evitar que las amenazas lleguen a los dispositivos y servidores y reducir la superficie de ataque. Sus capacidades de protección avanzada cubren todas las fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicio de Threat Hunting y Análisis Forense, que permite un reforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1213 PES Panda Adaptive Defense 360

Cytomic EDR/EPDR

Versión	4.2 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	31/03/2025

**Descripción**

Cytomic EPDR integra en una única solución un conjunto completo de tecnologías preventivas en el endpoint, con capacidades EDR y el Servicio Zero-Trust Application. Extiende las capacidades de prevención, detección y respuesta con una gama completa de capacidades de protección del endpoint necesarias para evitar que las amenazas lleguen a los dispositivos y servidores y reducir la superficie de ataque. Sus capacidades de protección avanzada cubren todas las fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicio de Threat Hunting y Análisis Forense, que permite un reforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1211 Procedimiento de empleo seguro Cytomic EPDR

INFORMACIÓN IMPORTANTE

ESET Endpoint Security

Versión	11.0.2044.0
Fabricante	ESET, spol. s r.o.
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	08/10/2024
Revisión de Validez	31/03/2025



Digital Security
Progress. Protected.

**Descripción**

ESET Endpoint Security ofrece una protección integral para empresas de todos los tamaños mediante un enfoque de seguridad multicapa que garantiza la protección de los sistemas frente a una amplia variedad de amenazas. Las principales funciones de seguridad incluyen:

- Antivirus y Antiespía: Elimina amenazas como virus, rootkits, gusanos y software espía, protegiendo los dispositivos de ataques conocidos y emergentes.
- Sistema Avanzado de Prevención de Intrusiones (HIPS): Controla los procesos del sistema, archivos y claves de registro a través de reglas personalizables. Protege contra modificaciones no autorizadas y detecta amenazas según su comportamiento.
- Análisis Avanzado de Memoria: Monitoriza y analiza los procesos activos en memoria para prevenir infecciones, incluso aquellas diseñadas para evitar la detección.
- Firewall Bidireccional: Supervisa y controla todo el tráfico de red entrante y saliente, evitando accesos no autorizados y ataques dirigidos. Esta capa de seguridad avanzada bloquea conexiones maliciosas y protege los recursos de la empresa de ataques externos.
- Protección Antiransomware: Bloquea cualquier intento de cifrado malicioso en archivos y resguarda los activos críticos de la empresa.
- Protección contra Botnets: Impide que los equipos sean usados para ataques distribuidos o envío masivo de spam, asegurando que los dispositivos permanezcan fuera del control de redes maliciosas.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Autonomous AI Endpoint Security Platform

Versión	Console Tokyo#19, agent 23.1.1
Fabricante	SentinelOne
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2023
Revisión de Validez	30/04/2025

**Descripción**

SentinelOne es una plataforma de ciberseguridad que utiliza inteligencia artificial y aprendizaje automático para detectar y prevenir amenazas avanzadas y malware. La plataforma proporciona una visibilidad completa de la red y es capaz de analizar el comportamiento del sistema en tiempo real para detectar patrones anómalos. También ofrece características de gestión de puntos finales y una respuesta automatizada a las amenazas. La plataforma es fácil de implementar y personalizar, escalable y se adapta a empresas de cualquier tamaño. SentinelOne también ofrece servicios de soporte técnico y gestión de incidentes.

Observaciones

CCN-STIC 1226 Procedimiento de Empleo Seguro SentinelOne

Kaspersky Endpoint Security for Windows

Versión	12.1.0.506 AES256
Fabricante	KASPERSKY LAB, S.L.U.
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2024
Revisión de Validez	30/06/2026

**Descripción**

Kaspersky Endpoint Security es una solución de protección avanzada que proporciona una protección integral mediante componentes de control (Control de dispositivos, Control Web, Control de anomalías adaptable) y de protección (Detección de comportamiento, Prevención de vulnerabilidades, Prevención de intrusiones en el host, Motor de reparación, Protección frente a amenazas en archivos, Protección frente a amenazas web, Protección frente a amenazas en el correo, Protección frente a amenazas en la red, Firewall, Prevención de ataques de BadUSB, Proveedor de protección AMSI). Este enfoque de protección multicapa permite detectar y bloquear amenazas como Ransomware, ataques sin archivos (Fileless), ataques de día cero, ataques de red o ataques mediante el uso de Exploits o técnicas Phishing. Sus capacidades de protección avanzada cubren las fases de Seguridad Adaptativa de Prevención, Detección y Respuesta (Remediación). Cuenta con capacidades avanzadas de detección y respuesta inteligentes que permiten hacer investigaciones, análisis forense y Threat Hunting para ser proactivo a la hora de identificar amenazas e investigar eventos maliciosos, así como buscar los indicadores de amenazas en toda la red. Todo ello desde una única consola de gestión.

La integración con Kaspersky Security Center (KSC) está excluida de la cualificación.

Observaciones

CCN-STIC-1209 Procedimiento de Empleo Seguro Kaspersky Endpoint Security 12.1.0.506 for Windows

INFORMACIÓN IMPORTANTE

Cortex XDR Agente Windows

Versión	7.5CE
Fabricante	Palo Alto
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/07/2022
Revisión de Validez	31/12/2024

**Descripción**

Cortex XDR es una solución de prevención, detección y respuesta que integra de forma nativa la telemetría desde la red, los endpoints y la nube para detener los ataques más sofisticados. El agente Windows, que es el componente cualificado, se fundamenta en una estrategia de detección, prevención y aprendizaje continuo.

Es capaz de detectar las amenazas con precisión gracias al análisis de comportamiento, revelando la causa original de cada incidente para acelerar las investigaciones. Además, se integra perfectamente con las diferentes soluciones de seguridad que aplican las políticas, de modo que se pongan en marcha los mecanismos de contención lo antes posible.

En cuanto a la prevención, ofrece una estrategia multidisciplinar con el fin de prevenir no solamente las amenazas conocidas, sino también las que no lo son. En el caso de los exploits, es posible prevenir los día cero en base a la detección de las técnicas que se utilizan para aprovecharse de las vulnerabilidades. En cuanto al malware, cada archivo se examina con un motor de análisis local adaptativo, basado en inteligencia artificial, que aprende constantemente para combatir las nuevas técnicas. Además, un motor de análisis dinámico observa cómo se comportan los procesos para detectar al instante cualquier ataque.

Cortex XDR permite que los equipos de seguridad puedan detener rápidamente la propagación del malware tanto en el endpoint como en la red, habilitándoles además para las tareas de hunting o respuesta a incidentes.

Observaciones

CCN-STIC-1222 Procedimiento de empleo seguro Agente Cortex XDR

INFORMACIÓN IMPORTANTE

Falcon Sensor con Falcon Console Cloud

Versión	7.05 (Falcon Sensor)
Fabricante	CrowdStrike
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2022
Revisión de Validez	30/04/2025

**Descripción**

La plataforma CrowdStrike Falcon®, construida sobre conocimiento de adversarios (Inteligencia de amenazas) ofrece y unifica la higiene de TI, el antivirus de nueva generación, la detección y respuesta de puntos finales (EDR), threat hunting y la inteligencia de amenazas, todo ello a través de un único agente ligero de despliegue rápido y sencillo sin requerir reinicio ni impacto significativo en el rendimiento de los sistemas protegidos. El agente de Falcon registra todas las actividades de interés en un punto final (puestos de trabajo, servidores, movilidad y cloud) para una inspección más profunda, incluso aquellas que evaden las medidas de prevención estándar, aplicando técnicas de Deep Machine Learning e IA, Protección basada en el comportamiento del Indicador de Ataque (IOA), protección antiexploit y gestión de IOCs.

Observaciones

CCN-STIC-1217 PES FALCON SENSOR

Intercept X Advanced with EDR

Versión	2023.2.0.47/2023.1.1
Fabricante	Sophos
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/03/2020
Revisión de Validez	31/12/2024

**Descripción**

Sophos Intercept X Advanced con EDR es una solución que ofrece protección avanzada de puesto de trabajo y servidores. Está especialmente diseñada para detener la gran mayoría de ataques y hacer frente a nuevas amenazas como ransomware, fileless, o ataques zero-day. Con diferentes capas de protección, las primeras están diseñadas para reducir la superficie de ataque a través del control de USBs, control de aplicaciones, control de navegación y DLP. Posteriormente tiene capas que detectan, primero lo malo conocido a través de las firmas que desarrollan los Sophos LABS y, segundo, lo malo desconocido, como el ransomware, gracias a la monitorización de procesos, el control de comportamiento, utilizando la tecnología única de Deep Learning que permite detectar malware no identificado previamente, y la detección de técnicas de explotación/ataque y de post compromiso. Además, la solución cuenta con capacidades avanzadas de detección y respuesta inteligentes (EDR) que permiten a la organización hacer investigaciones y threat hunting para ser proactivo a la hora de identificar amenazas e investigar posibles eventos maliciosos, así como comprender el alcance y el impacto o buscar los indicadores de amenazas en toda la red. Todo ello desde una única consola de gestión en la nube y un único agente.

Observaciones

CCN-STIC 1207 Procedimiento de Empleo Seguro Sophos Central Intercept X

INFORMACIÓN IMPORTANTE

Panda Adaptive Defense 360

Versión	4.2 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	31/03/2025

**Descripción**

Panda Adaptive Defense 360 es una solución de seguridad completa para los puestos de trabajo, portátiles y servidores que además de proteger contra amenazas conocidas, avanzadas y zero-day, ransomware y ataques de seguridad fileless (en memoria) y malwareless, incluye firewall personal, IPS/IDS, anti-spam, anti-spam en correo, filtrado y categorización en navegación web y control de dispositivos, entre otras técnicas de seguridad y control de productividad. Sus capacidades de protección avanzada cubren todas fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicio de Threat Hunting y Análisis Forense, que permite una enforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1213 PES Panda Adaptive Defense 360

INFORMACIÓN IMPORTANTE

7.3.2 EDR (ENDPOINT DETECTION AND RESPONSE)

GravityZone	
Versión	
Fabricante	Bitdefender
Familia	EDR (Endpoint Detection and Response)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/06/2024
Revisión de Validez	31/01/2025
Descripción	La plataforma Bitdefender GravityZone es una plataforma integral de ciberseguridad que protege a toda la organización, brindando capacidades de prevención, protección, detección y respuesta (EDR/XDR/MDR) para organizaciones de todos los tamaños en servidores, cargas de trabajo y sistemas de usuario final de múltiples nubes híbridas, incluidas PC, portátiles y dispositivos móviles. La arquitectura de defensa en profundidad de GravityZone integra conocimiento y control de seguridad en una consola de administración unificada desde la cual los administradores monitorean y administran de manera centralizada el riesgo de ciberseguridad. Además, la consola de administración brinda capacidades para que los equipos de seguridad investiguen y solucionen incidentes. El rendimiento está optimizado específicamente para entornos de nube y virtualización, para minimizar el impacto de seguridad en la computación en la nube y los recursos virtualizados
Observaciones	Procedimiento de Empleo Seguro pendiente de publicación.

Bitdefender.



INFORMACIÓN IMPORTANTE

TEHTRIS Endpoint Detection and Response

Versión	1.8.1
Fabricante	TEHTRI-SECURITY SPAIN, SOCIEDAD LIMITADA
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/06/2024
Revisión de Validez	31/01/2025

**Descripción**

Los agentes EDR detectan y neutralizan automáticamente las amenazas avanzadas o desconocidas en tiempo real en cada estación de trabajo y servidor donde se despliega. Para reforzar el control y la seguridad, nuestra solución ofrece una visibilidad y un análisis completo de los endpoints con capacidades de investigación avanzada (Threat Hunting, compliance, análisis de vulnerabilidades, etc.).

TEHTRIS EDR puede ser gestionado desde la consola única TEHTRIS XDR Platform 11.0 que permite mejorar la prevención, acelerar la detección y la remediación de ciberataques en tiempo real, sin intervención humana. Incluye inteligencia de amenazas robusta y fiable, sandboxes, SOAR integrado con playbooks de remediación pre-construidos y paneles de control fáciles de usar. Desde esta consola única se puede gestionar otros productos de ciberseguridad creados por TEHTRIS como son MTD, SIEM, Honeypots, NTA y DNS Firewall.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Stormshield Endpoint Security Evolution

Versión	2.5.3
Fabricante	Stormshield
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2024
Revisión de Validez	30/11/2026

**STORMSHIELD****Descripción**

Stormshield Endpoint Security Evolution ofrece una ciberseguridad de nueva generación para garantizar la protección completa de terminales y servidores. Basado en la tecnología de análisis de comportamiento sin firmas, el agente reconoce las técnicas de ataque, como la explotación de las vulnerabilidades de las aplicaciones o las acciones características del ransomware. Una vez identificada la amenaza, se puede tomar cualquier acción deseada, como el cierre de procesos o el bloqueo de las conexiones de red (cuarentena de equipos infectados, restricción de túnel VPN o de uso de redes Wi-Fi).

Observaciones

CCN-STIC-1221 Procedimiento de empleo seguro Stormshield Endpoint Security Evolution

INFORMACIÓN IMPORTANTE

Deep Security (Manager y Agente/Relay Linux/Windows)

Versión	11
Fabricante	Trend Micro
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/03/2025

**Descripción**

Deep Security es la respuesta de Trend Micro para proteger el cloud híbrido ya sean servidores físicos o virtuales.

Gracias a su agente ligero, el cual incorpora funcionalidades: EDR (con respuesta frente a amenazas conocidas, zero-day), envío de telemetría a la plataforma XDR de Trend Micro (VisionOne), reputación web, control de aplicaciones, supervisión de logs, Supervisión de Integridad (FIM), Firewall de Host y Host IPS (que incorpora la tecnología de parchado virtual), ayuda a mejorar la postura de seguridad proporcionando seguridad, visibilidad y control. La cualificación abarca los siguientes componentes: Manager, Agente/Relay Linux y el Agente/Relay Windows. El Virtual Appliance no está cualificado.

Observaciones

CCN-STIC-1216 PES Trendmicro Deep Security

Microsoft Defender for Endpoint

Versión	
Fabricante	Microsoft Iberica SRL
Familia	EDR (Endpoint Detection and Response)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	30/11/2024

**Descripción**

Microsoft Defender for Endpoint es una solución EDR en la nube que protege a las organizaciones públicas y/o privadas contra amenazas en línea y en toda clase de dispositivos. Utiliza tecnologías en tiempo real para prevenir, detectar, investigar y responder a amenazas avanzadas. Entre sus funcionalidades proporciona técnicas para la reducción de la superficie de ataque, protección contra amenazas y vulnerabilidades incluyendo el uso de Inteligencia Artificial, detección y respuesta mediante la monitorización de comportamientos y técnicas de los atacantes, capacidades de investigación avanzada y automatización de respuestas, así como acceso a los expertos en ciber-amenazas de Microsoft.

Microsoft Defender for Endpoint puede controlar y monitorizar el acceso a todos los recursos de una organización pública y/o privada de forma centralizada, lo que permite detectar y resolver problemas de seguridad de manera rápida y eficiente además de estar integrada con otros productos de Microsoft, como Office 365 y Azure.

Observaciones

CCN-STIC -1228-Procedimiento de empleo seguro Microsoft Defender for Endpoint.

INFORMACIÓN IMPORTANTE

WatchGuard EPDR/Advanced EPDR

Versión	4.2 (Protection Agent v8.0)
Fabricante	WatchGuard Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/03/2023
Revisión de Validez	31/03/2025

**Descripción**

WatchGuard EDR/EPP integra en una única solución un conjunto completo de tecnologías preventivas en el endpoint, con capacidades EDR y el Servicio Zero-Trust Application. Extiende las capacidades de prevención, detección y respuesta con una gama completa de capacidades de protección del endpoint necesarias para evitar que las amenazas lleguen a los dispositivos y servidores y reducir la superficie de ataque. Sus capacidades de protección avanzada cubren todas las fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicio de Threat Hunting y Análisis Forense, que permite un reforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1213 PES Panda Adaptive Defense 360

Cytomic EDR/EPDR

Versión	4.2 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	31/03/2025

**Descripción**

Cytomic EPDR integra en una única solución un conjunto completo de tecnologías preventivas en el endpoint, con capacidades EDR y el Servicio Zero-Trust Application. Extiende las capacidades de prevención, detección y respuesta con una gama completa de capacidades de protección del endpoint necesarias para evitar que las amenazas lleguen a los dispositivos y servidores y reducir la superficie de ataque. Sus capacidades de protección avanzada cubren todas las fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicio de Threat Hunting y Análisis Forense, que permite un reforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1211 Procedimiento de empleo seguro Cytomic EPDR

INFORMACIÓN IMPORTANTE

Autonomous AI Endpoint Security Platform

Versión	Console Tokyo#19, agent 23.1.1
Fabricante	SentinelOne
Familia	EDR (Endpoint Detection and Response)
Tipo	Servicio
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2023
Revisión de Validez	30/04/2025

**Descripción**

SentinelOne es una plataforma de ciberseguridad que utiliza inteligencia artificial y aprendizaje automático para detectar y prevenir amenazas avanzadas y malware. La plataforma proporciona una visibilidad completa de la red y es capaz de analizar el comportamiento del sistema en tiempo real para detectar patrones anómalos. También ofrece características de gestión de puntos finales y una respuesta automatizada a las amenazas. La plataforma es fácil de implementar y personalizar, escalable y se adapta a empresas de cualquier tamaño. SentinelOne también ofrece servicios de soporte técnico y gestión de incidentes.

Observaciones

CCN-STIC 1226 Procedimiento de Empleo Seguro SentinelOne

Kaspersky Endpoint Security for Windows

Versión	12.1.0.506 AES256
Fabricante	KASPERSKY LAB, S.L.U.
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2024
Revisión de Validez	30/06/2026

**Descripción**

Kaspersky Endpoint Security es una solución de protección avanzada que proporciona una protección integral mediante componentes de control (Control de dispositivos, Control Web, Control de anomalías adaptable) y de protección (Detección de comportamiento, Prevención de vulnerabilidades, Prevención de intrusiones en el host, Motor de reparación, Protección frente a amenazas en archivos, Protección frente a amenazas web, Protección frente a amenazas en el correo, Protección frente a amenazas en la red, Firewall, Prevención de ataques de BadUSB, Proveedor de protección AMSI). Este enfoque de protección multicapa permite detectar y bloquear amenazas como Ransomware, ataques sin archivos (Fileless), ataques de día cero, ataques de red o ataques mediante el uso de Exploits o técnicas Phishing. Sus capacidades de protección avanzada cubren las fases de Seguridad Adaptativa de Prevención, Detección y Respuesta (Remediación). Cuenta con capacidades avanzadas de detección y respuesta inteligentes que permiten hacer investigaciones, análisis forense y Threat Hunting para ser proactivo a la hora de identificar amenazas e investigar eventos maliciosos, así como buscar los indicadores de amenazas en toda la red. Todo ello desde una única consola de gestión.

La integración con Kaspersky Security Center (KSC) está excluida de la cualificación.

Observaciones

CCN-STIC-1209 Procedimiento de Empleo Seguro Kaspersky Endpoint Security 12.1.0.506 for Windows

INFORMACIÓN IMPORTANTE

Cortex XDR Agente Windows

Versión	7.5CE
Fabricante	Palo Alto
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/07/2022
Revisión de Validez	31/12/2024

**Descripción**

Cortex XDR es una solución de prevención, detección y respuesta que integra de forma nativa la telemetría desde la red, los endpoints y la nube para detener los ataques más sofisticados. El agente Windows, que es el componente cualificado, se fundamenta en una estrategia de detección, prevención y aprendizaje continuo.

Es capaz de detectar las amenazas con precisión gracias al análisis de comportamiento, revelando la causa original de cada incidente para acelerar las investigaciones. Además, se integra perfectamente con las diferentes soluciones de seguridad que aplican las políticas, de modo que se pongan en marcha los mecanismos de contención lo antes posible.

En cuanto a la prevención, ofrece una estrategia multidisciplinar con el fin de prevenir no solamente las amenazas conocidas, sino también las que no lo son. En el caso de los exploits, es posible prevenir los día cero en base a la detección de las técnicas que se utilizan para aprovecharse de las vulnerabilidades. En cuanto al malware, cada archivo se examina con un motor de análisis local adaptativo, basado en inteligencia artificial, que aprende constantemente para combatir las nuevas técnicas. Además, un motor de análisis dinámico observa cómo se comportan los procesos para detectar al instante cualquier ataque.

Cortex XDR permite que los equipos de seguridad puedan detener rápidamente la propagación del malware tanto en el endpoint como en la red, habilitándoles además para las tareas de hunting o respuesta a incidentes.

Observaciones

CCN-STIC-1222 Procedimiento de empleo seguro Agente Cortex XDR

INFORMACIÓN IMPORTANTE

Falcon Sensor con Falcon Console Cloud

Versión	7.05 (Falcon Sensor)
Fabricante	CrowdStrike
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2022
Revisión de Validez	30/04/2025

**Descripción**

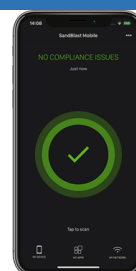
La plataforma CrowdStrike Falcon®, construida sobre conocimiento de adversarios (Inteligencia de amenazas) ofrece y unifica la higiene de TI, el antivirus de nueva generación, la detección y respuesta de puntos finales (EDR), threat hunting y la inteligencia de amenazas, todo ello a través de un único agente ligero de despliegue rápido y sencillo sin requerir reinicio ni impacto significativo en el rendimiento de los sistemas protegidos. El agente de Falcon registra todas las actividades de interés en un punto final (puestos de trabajo, servidores, movilidad y cloud) para una inspección más profunda, incluso aquellas que evaden las medidas de prevención estándar, aplicando técnicas de Deep Machine Learning e IA, Protección basada en el comportamiento del Indicador de Ataque (IOA), protección antiexploit y gestión de IOCs.

Observaciones

CCN-STIC-1217 PES FALCON SENSOR

Sandblast (Harmony) Mobile para iOS y Android

Versión	3.8
Fabricante	Check Point Software Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2024

**Descripción**

Harmony Mobile es una completa solución de defensa contra amenazas móviles para las plataformas de iOS y Android. Mantiene sus datos corporativos seguros porque protege los dispositivos móviles de los empleados de todos los vectores de ataque: aplicaciones, red y sistema operativo. Diseñada para reducir los gastos generales de los administradores y aumentar la adopción del usuario, se adapta perfectamente a su entorno móvil existente, se implementa y escala rápidamente, y protege los dispositivos sin afectar la experiencia ni la privacidad del usuario.

Observaciones

CCN-STIC-1212 Procedimiento de empleo seguro Harmony Sandblast Mobile

INFORMACIÓN IMPORTANTE

Intercept X Advanced with EDR

Versión	2023.2.0.47/2023.1.1
Fabricante	Sophos
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/03/2020
Revisión de Validez	31/12/2024

SOPHOS
Cybersecurity made simple.

**Descripción**

Sophos Intercept X Advanced con EDR es una solución que ofrece protección avanzada de puesto de trabajo y servidores. Está especialmente diseñada para detener la gran mayoría de ataques y hacer frente a nuevas amenazas como ransomware, fileless, o ataques zero-day. Con diferentes capas de protección, las primeras están diseñadas para reducir la superficie de ataque a través del control de USBs, control de aplicaciones, control de navegación y DLP. Posteriormente tiene capas que detectan, primero lo malo conocido a través de las firmas que desarrollan los Sophos LABS y, segundo, lo malo desconocido, como el ransomware, gracias a la monitorización de procesos, el control de comportamiento, utilizando la tecnología única de Deep Learning que permite detectar malware no identificado previamente, y la detección de técnicas de explotación/ataque y de post compromiso. Además, la solución cuenta con capacidades avanzadas de detección y respuesta inteligentes (EDR) que permiten a la organización hacer investigaciones y threat hunting para ser proactivo a la hora de identificar amenazas e investigar posibles eventos maliciosos, así como comprender el alcance y el impacto o buscar los indicadores de amenazas en toda la red. Todo ello desde una única consola de gestión en la nube y un único agente.

Observaciones

CCN-STIC 1207 Procedimiento de Empleo Seguro Sophos Central Intercept X

Panda Adaptive Defense 360

Versión	4.2 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	31/03/2025

**Descripción**

Panda Adaptive Defense 360 es una solución de seguridad completa para los puestos de trabajo, portátiles y servidores que además de proteger contra amenazas conocidas, avanzadas y zero-day, ransomware y ataques de seguridad fileless (en memoria) y malwareless, incluye firewall personal, IPS/IDS, anti-spam, anti-spam en correo, filtrado y categorización en navegación web y control de dispositivos, entre otras técnicas de seguridad y control de productividad. Sus capacidades de protección avanzada cubren todas las fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicio de Threat Hunting y Análisis Forense, que permite una enforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1213 PES Panda Adaptive Defense 360

INFORMACIÓN IMPORTANTE

7.3.3 HERRAMIENTAS DE GESTIÓN DE RED

NetinDS		 
Versión	2.0.2	
Fabricante	Netin Systems SL	
Familia	Herramientas de gestión de red	
Tipo	Producto	
Categoría ENS	ALTA	
Fecha Inclusión	20/11/2024	
Revisión de Validez	30/04/2025	
Descripción		
NetinDS es un sistema avanzado de monitorización y diagnóstico para instalaciones industriales y OT, enfocado en optimizar la disponibilidad y productividad. Sus principales características incluyen la monitorización en tiempo real de dispositivos como PLCs, RTUs y SCADA, la auditoría constante y la integración de protocolos IT y OT, y el análisis forense. NetinDS cuenta con tres componentes principales: Agentes (captura de datos), Servidor (almacenamiento y gestión), y WebUI (visualización personalizable). Soporta protocolos como OPC UA y MODBUS, y permite la configuración de alarmas con notificaciones detalladas.		
Observaciones		
Procedimiento de Empleo Seguro pendiente de publicación		

FortiManager (FMG-200G, FMG-400G, FMG-3000G, FMG-3700G, FMG-VM)		 
Versión	6.4	
Fabricante	Fortinet	
Familia	Herramientas de gestión de red	
Tipo	Producto	
Categoría ENS	ALTA	
Fecha Inclusión	01/03/2024	
Revisión de Validez	31/08/2026	
Descripción		
Gestión centralizada mediante interfaz gráfica de dispositivos Fortinet incluyendo: FortiGate, FortiSwitches, FortiAP, FortiClient. Facilita la descarga de firmas FortiGuard para entornos estancos sin conexión a internet. Revisión, aprobación y auditoría de políticas de seguridad y/o gestión de las comunicaciones, proceso automatizado para facilitar el cumplimiento de las políticas y gestión del ciclo de vida de las mismas. Diseño de flujos de trabajo para reducir el riesgo o impacto sobre el servicio. API para la automatización y orquestación. Capacidad de configuración colectiva de los dispositivos, los objetos y las políticas desde una única interfaz de usuario, con posibilidad de creación de distintos roles de gestión o aprobación, llegando a poder distinguir perfiles o grado de aplicación en función de las garantías de seguridad, acceso, momento o ubicación del mismo. Agrupación y gestión flexible lógica o geográfica de dispositivos. Facilita el despliegue y auto-provisión en modo "Zero Touch".		
Observaciones		
CCN-STIC-1443 Procedimiento de empleo seguro FortiManager		

INFORMACIÓN IMPORTANTE

FortiManager (FMG-200F, FMG-300E, FMG-2000E, FMG-3000F, FMG-3700F)

Versión	6.4
Fabricante	Fortinet
Familia	Herramientas de gestión de red
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2024
Revisión de Validez	31/08/2025

FORTINET®**Descripción**

Gestión centralizada mediante interfaz gráfica de dispositivos Fortinet incluyendo: FortiGate, FortiSwitches, FortiAP, FortiClient. Facilita la descarga de firmas FortiGuard para entornos estancos sin conexión a internet. Revisión, aprobación y auditoría de políticas de seguridad y/o gestión de las comunicaciones, proceso automatizado para facilitar el cumplimiento de las políticas y gestión del ciclo de vida de las mismas. Diseño de flujos de trabajo para reducir el riesgo o impacto sobre el servicio. API para la automatización y orquestación. Capacidad de configuración colectiva de los dispositivos, los objetos y las políticas desde una única interfaz de usuario, con posibilidad de creación de distintos roles de gestión o aprobación, llegando a poder distinguir perfiles o grado de aplicación en función de las garantías de seguridad, acceso, momento o ubicación del mismo. Agrupación y gestión flexible lógica o geográfica de dispositivos. Facilita el despliegue y auto-provisión en modo ""Zero Touch".

Observaciones

CCN-STIC-1443 Procedimiento de empleo seguro FortiManager

FortiManager (FMG-300F y FMG-1000F)

Versión	6.4
Fabricante	Fortinet
Familia	Herramientas de gestión de red
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

FORTINET®**Descripción**

Gestión centralizada mediante interfaz gráfica de dispositivos Fortinet incluyendo: FortiGate, FortiSwitches, FortiAP, FortiClient. Facilita la descarga de firmas FortiGuard para entornos estancos sin conexión a internet. Revisión, aprobación y auditoría de políticas de seguridad y/o gestión de las comunicaciones, proceso automatizado para facilitar el cumplimiento de las políticas y gestión del ciclo de vida de las mismas. Diseño de flujos de trabajo para reducir el riesgo o impacto sobre el servicio. API para la automatización y orquestación. Capacidad de configuración colectiva de los dispositivos, los objetos y las políticas desde una única interfaz de usuario, con posibilidad de creación de distintos roles de gestión o aprobación, llegando a poder distinguir perfiles o grado de aplicación en función de las garantías de seguridad, acceso, momento o ubicación del mismo. Agrupación y gestión flexible lógica o geográfica de dispositivos. Facilita el despliegue y auto-provisión en modo ""Zero Touch".

Observaciones

CCN-STIC-1443 Procedimiento de empleo seguro FortiManager

INFORMACIÓN IMPORTANTE

7.3.4 HERRAMIENTAS DE FILTRADO DE NAVEGACIÓN

Cisco Web Security Appliance (S690, S690X, S695, S695F, S680, S390, S380, S395, S190, S195)

Versión	AsyncOS 11.8
Fabricante	Cisco Systems
Familia	Herramientas de filtrado de navegación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	31/05/2025



Descripción

Cisco Secure Web Appliance proxy protege a las organizaciones en cuanto a navegación se refiere, evaluando las webs desconocidas antes de permitir que los usuarios accedan a ellas y bloqueando automáticamente las páginas de riesgo. Utilizando funciones de alto rendimiento, Cisco Secure Web Appliance mantiene seguros a los usuarios.

Observaciones

CCN-STIC-1625 Procedimiento de Empleo Seguro Cisco Web Security Appliance

INFORMACIÓN IMPORTANTE

7.3.5 SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM)

MONICA

Versión	7.1
Fabricante	Grupo ICA Sistemas y Seguridad
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2024
Revisión de Validez	31/12/2024



Descripción

La plataforma española Mónica permite a los analistas de ciberseguridad recopilar logs e información ilimitada de seguridad, detectar ataques basados en anomalías y comportamientos desconocidos así como automatizar la respuesta ante incidentes en entornos IT, OT e IoT. Mónica recopila información de cualquier fuente interna y externa a la empresa (comercial, propietaria, aplicaciones, cloud), correlando y analizando en tiempo real esa información, permitiendo contextualizar y priorizar los incidentes de seguridad tanto internos como externos. Combina los casos de uso de detección más sofisticados con la información más precisa de amenazas y vulnerabilidades zero day gracias a la información de fuentes externas de inteligencia, threat hunting y anomalías de red/usuario.

Observaciones

CCN-STIC-1206 PES NGSIEM LogICA

INFORMACIÓN IMPORTANTE

Microsoft Sentinel

Versión**Fabricante**

Microsoft Iberica SRL

Familia

Sistemas de gestión de eventos de seguridad (SIEM)

Tipo

Servicio

Categoría ENS

ALTA

Fecha Inclusión

01/02/2023

Revisión de Validez

31/01/2025

**Descripción**

Microsoft Sentinel es una plataforma SIEM/SOAR de seguridad en la nube diseñada para ayudar a las organizaciones a detectar, investigar y responder a amenazas de seguridad. Incorpora capacidades de automatización y una visión completa de la seguridad de una organización.

Permite agilizar y modernizar las operaciones de cualquier centro de seguridad (SOC) eliminando la configuración y el mantenimiento de la infraestructura de seguridad, aprovechando la elasticidad y la escalabilidad de la nube, al tiempo que reduce los costes. Es una solución enfocada en detectar rápidamente las amenazas reales, reduciendo los falsos positivos gracias al uso del aprendizaje automático integrado y a conocimientos basados en el análisis diario de billones de señales.

Permite además acelerar la búsqueda proactiva de amenazas con consultas predefinidas basadas en años de experiencia en seguridad, dispone de listas priorizadas de alertas, análisis de correlacionados de miles de eventos de seguridad de forma rápida y visualización del alcance completo de cada ataque. Permite simplificar las operaciones de seguridad y acelerar la respuesta a las amenazas con la automatización integrada y la orquestación de tareas y flujos de trabajo.

Puede conectar y recopilar datos de diferentes fuentes, incluidos usuarios, aplicaciones, servidores y dispositivos que se ejecutan en una infraestructura on-premise o en cualquier nube. Y tiene la capacidad de integrarse con herramientas existentes, ya sean aplicaciones empresariales, u otros productos de análisis de seguridad o herramientas propias, y crear y utilizar sus propios modelos de aprendizaje automático.

Observaciones

CCN-STIC 1229 Procedimiento de Empleo Seguro MS Sentinel

INFORMACIÓN IMPORTANTE

IBM QRadar Security Intelligence Platform

Versión	7.5
Fabricante	IBM
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/12/2026

**Descripción**

La familia de productos QRadar, plataforma de seguridad inteligente líder en el mercado SIEM, ofrece una visibilidad absoluta y unificada de la seguridad en tiempo real. QRadar recolecta, consolida y correlaciona información de todos los endpoints, dispositivos de red, entornos de las nubes, aplicaciones e incluso de diferentes data-lakes. Aplica análisis avanzado para priorizar las amenazas y clasificarlas con mayor precisión. Adicionalmente, esta tecnología ofrece capacidades de búsquedas avanzadas para ayudar a encontrar nuevas amenazas de forma proactiva y proporciona todas las funcionalidades que una organización necesita para abordar los desafíos de seguridad más importantes.

Observaciones

CCN-STIC-1203 Procedimiento de empleo seguro IBM QRadar Security Intelligence Platform

Chronicle SIEM

Versión	N/A
Fabricante	Google
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	16/02/2024
Revisión de Validez	31/01/2025

**Descripción**

Chronicle SIEM, una solución de gestión de eventos e información de seguridad (SIEM) nativa de la nube, permite a los clientes recopilar y analizar la telemetría de seguridad de toda su empresa para potenciar la detección, investigación y remediación de amenazas.

Como parte del servicio, Chronicle SIEM normaliza, correlaciona y enriquece los datos de seguridad para proporcionar análisis y contexto sobre actividades sospechosas.

Chronicle SIEM incluye Google Cloud Threat Intelligence, que es un servicio de inteligencia de amenazas agregado para clientes de Chronicle SIEM que aprovecha la inteligencia de amenazas de Google para resaltar amenazas en sus entornos de nube y on-premise.

Está respaldado por analistas de amenazas de Google que verifican los indicadores maliciosos en la telemetría de seguridad y revelan alertas contextualizadas a los clientes, lo que les permite dar una respuesta informada.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Gloria

Versión	v6.6.1
Fabricante	S2 GRUPO / CCN
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2021
Revisión de Validez	30/06/2026



Descripción

Gloria es una plataforma para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos. Basado en los sistemas SIEM, va un paso más allá de las capacidades de monitorización, almacenamiento e interpretación de los datos relevantes. Así, mediante técnicas de correlación compleja de varias fuentes de eventos o análisis de patrones para la identificación de anomalías, permite una orientación muy flexible hacia la vigilancia del mundo IP. La plataforma permite las siguientes funcionalidades a través de distintos módulos:

- Monitorización de entornos tecnológicos (IT/OT).
 - Inteligencia.
 - Gestión del servicio.
 - Automatización, orquestación y reducción de tiempos de respuesta.
- Para más información, (<https://ccn-cert.cni.es/soluciones-seguridad/gloria.html>)

Observaciones

CCN-STIC-1215 Procedimiento de empleo seguro GLORIA

INFORMACIÓN IMPORTANTE

ASIP (AIUKEN SECURITY INTELLIGENCE PLATFORM)

Versión	Delfos Linux Agent v0.8.10
Fabricante	AIUKEN SOLUTIONS
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Servicio
Categoría ENS	MEDIA
Fecha Inclusión	01/03/2023
Revisión de Validez	28/02/2025

**Descripción**

ASIP (Aiuken Security Intelligence Platform), es una Plataforma completa de gestión SOC, que aúna capacidades avanzadas de correlación y detección temprana de eventos de seguridad, mejorándolas a través de aprendizaje e Inteligencia Artificial e integración de los framework de seguridad MITRE Attack para ataques, CAPEC para detección de vulnerabilidades y NIST para la gestión de los controles de seguridad de las compañías, permitiendo no tener una dependencia tan alta del modelo tradicional de casos de uso.

Integra a su vez, portal de servicio, gestión de casos y ticketing, motor de generación de paneles informativos y KPIs, Threat Intelligence propia y herramientas para Threat Hunting y detección temprana. La automatización es otra de las ventajas de ASIP, orquestación y SOAR para el modelado de procesos autogestionado y generación de informes de servicio de forma automática, permitiendo a los técnicos enfocarse en las tareas importantes.

De igual forma es posible integrar cualquier fuente disponible en la compañía e incluso aprovechar las capacidades de integración nativa de la herramienta con Azure, Google Cloud y AWS para poder tener una visibilidad completa de todas las fuentes de la compañía, tanto externas como internas.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

MONSE

Versión	Probe 1.0, Agente 8.3.2
Fabricante	GRUPO CIES
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	01/11/2024

**Descripción**

MONSE (Monitorización de la Seguridad) es una solución SIEM que permite recopilar y correlacionar de forma centralizada múltiples fuentes de eventos de seguridad. La solución permite analizar eventos basados en logs, procesos, comportamiento e IOCs. Dispone de técnicas de Inteligencia Artificial que facilitan la detección de anomalías, integración de fuentes de inteligencia de amenazas, posibilidad de definir reglas de alerta adaptadas a la particularidad de cada organización, así como la posibilidad de crear cuadros de mando personalizables. La plataforma permite un despliegue modular en función del tipo de madurez de la organización. Dispone de múltiples funcionalidades orientadas a la mejora en el cumplimiento del Esquema Nacional de Seguridad.

Observaciones

CCN-STIC 1223 Procedimiento de empleo seguro MONSE

Splunk Enterprise

Versión	9.2
Fabricante	Splunk Inc.
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2024
Revisión de Validez	31/01/2026

**Descripción**

Splunk Enterprise es una plataforma de gestión de eventos e información de seguridad (SIEM) que proporciona una visibilidad completa de su postura de seguridad. Splunk Enterprise permite gestionar el ciclo completo en una organización, incluyendo capacidades de Detección, Monitorización, Investigación y Respuesta ante incidentes de Seguridad. Incorpora capacidades de búsqueda y generación de informes sin precedentes, análisis avanzados, inteligencia artificial integrada y contenido de seguridad predefinido y dinámico para acelerar la detección e investigación de amenazas. Splunk permite clasificar por prioridad los incidentes, priorizando los incidentes que afecten a activos o identidades críticos. Permite generar alertas basadas en riesgo, identificando anomalías y amenazas tanto externas como internas. Las más de 2500 reglas de detección abarcan todos los ámbitos de seguridad: IT, OT, IoT, IoMT y las nubes públicas en cualquiera de sus formatos.

Observaciones

Procedimiento de empleo pendiente de actualización. Existe un PES de una versión anterior del producto: CCN-STIC-1225

INFORMACIÓN IMPORTANTE

NetWitness Platform

Versión	11.6
Fabricante	Netwitness, an RSA Business.
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	31/12/2024

**Descripción**

La plataforma XDR de Netwitness (an RSA Business), es la solución de SIEM evolucionado o XDR (eXtended Detection and Response), con capacidades de visibilidad completa gracias a su modelo de datos unificado pudiendo capturar logs, netflows, tráfico de red, actividad en los end points, además de información de inteligencia de seguridad, de forma integrada, bajo un único motor de análisis y correlación avanzada. Además, incluye funcionalidades necesarias por un SOC para hacer frente a amenazas complejas. Netwitness Platform XDR cuenta además con componentes adicionales como UEBA (User and Entity Behaviour Analytics) y SOAR (Security Orchestration and Automation Response). La solución permite capturar todo tipo de información, permitiendo el análisis avanzado de amenazas, priorización en base al contexto de negocio y haciendo más eficiente el trabajo del analista. Es una plataforma que, gracias a su capacidad de análisis, muestra el alcance completo de un ataque a los analistas. Además, gracias a su estrategia Run Anywhere, la plataforma se puede desplegar en cualquier entorno (virtual, cloud, físico o híbrido), así como hacer frente a arquitecturas altamente distribuidas. RSA Netwitness incluye en todos sus clientes +50 feeds de inteligencia, agente para endpoints ilimitados, así como el despliegue ilimitado de dispositivos para cubrir cualquier forma de despliegue. <https://www.netwitness.com/en-us/solutions/evolved-siem/>

Observaciones

CCN-STIC-1210 Procedimiento de Empleo Seguro RSA Netwitness Platform

INFORMACIÓN IMPORTANTE

NetWitness Platform

Versión 11.7**Fabricante** Netwitness, an RSA Business.**Familia** Sistemas de gestión de eventos de seguridad (SIEM)**Tipo** Producto**Categoría ENS** ALTA**Fecha Inclusión** 01/11/2024**Revisión de Validez** 31/12/2025**Descripción**

La plataforma XDR de Netwitness (an RSA Business), es la solución de SIEM evolucionado o XDR (eXtended Detection and Response), con capacidades de visibilidad completa gracias a su modelo de datos unificado pudiendo capturar logs, netflows, tráfico de red, actividad en los end points, además de información de inteligencia de seguridad, de forma integrada, bajo un único motor de análisis y correlación avanzada. Además, incluye funcionalidades necesarias por un SOC para hacer frente a amenazas complejas. Netwitness Platform XDR cuenta además con componentes adicionales como UEBA (User and Entity Behaviour Analytics) y SOAR (Security Orchestration and Automation Response). La solución permite capturar todo tipo de información, permitiendo el análisis avanzado de amenazas, priorización en base al contexto de negocio y haciendo más eficiente el trabajo del analista. Es una plataforma que, gracias a su capacidad de análisis, muestra el alcance completo de un ataque a los analistas. Además, gracias a su estrategia Run Anywhere, la plataforma se puede desplegar en cualquier entorno (virtual, cloud, físico o híbrido), así como hacer frente a arquitecturas altamente distribuidas. RSA Netwitness incluye en todos sus clientes +50 feeds de inteligencia, agente para endpoints ilimitados, así como el despliegue ilimitado de dispositivos para cubrir cualquier forma de despliegue. <https://www.netwitness.com/en-us/solutions/evolved-siem/>

Observaciones

CCN-STIC-1210 Procedimiento de Empleo Seguro RSA Netwitness Platform

INFORMACIÓN IMPORTANTE

FortiAnalyzer FAZ-1000F, FAZ-150G, FAZ-2000E, FAZ-200F, FAZ-3000F, FAZ-3000G, FAZ-300F, FAZ-300G, FAZ-3500G, FAZ-3700F, FAZ-3700G, FAZ-400E, FAZ-800F, FAZ-810G, FAZ-VM64

Versión 7.0

Fabricante Fortinet

Familia Sistemas de gestión de eventos de seguridad (SIEM)

FORTINET®

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/11/2024

Revisión de Validez 22/10/2025



Descripción

Consola web que ofrece visibilidad en tiempo real, informes bajo demanda o programados para ser exportados en diferentes formatos (PDF, Mail, etc) para dispositivos Fortinet (FortiGate, FortiDDoS, FortiClient, FortiCarrier, Forticlient EMS, FortiMail, FortiWeb, FortiCache, FortiSandbox, etc.). También, mediante Syslog, productos de otros fabricantes. Facilita la realización de análisis forense, cumplimiento legal, descubrimiento e investigación de eventos de una manera centralizada y correlada. Exploración multi-capa. Uso de plantillas predefinidas (Revisión Seguridad 360º, Aplicaciones, Amenazas, uso de Web, cumplimiento normativo, actividad Wifi, VPN, consumo ancho de banda, etc). Capacidad de creación de diferentes perfiles de administración para entornos concretos o capacidades de escritura o lectura configuradas por entorno. Amplia gama de dispositivos físicos o virtuales que proporcionan solución escalable.

Observaciones

CCN-STIC-1444 Procedimiento de empleo seguro FortiAnalyzer

INFORMACIÓN IMPORTANTE

LogICA5 Next Generation SIEM

Versión	v7.1
Fabricante	Grupo ICA Sistemas y Seguridad
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2020
Revisión de Validez	31/12/2024

**Descripción**

La plataforma española Next Generation SIEM LogICA permite a los analistas de ciberseguridad recopilar logs e información ilimitada de seguridad, detectar ataques basados en anomalías y comportamientos desconocidos así como automatizar la respuesta ante incidentes en entornos IT, OT e IoT. LogICA NG SIEM recopila información de cualquier fuente interna y externa a la empresa (comercial, propietaria, aplicaciones, cloud), correlando y analizando en tiempo real esa información, permitiendo contextualizar y priorizar los incidentes de seguridad tanto internos como externos. Combina los casos de uso de detección más sofisticados con la información más precisa de amenazas y vulnerabilidades zero day gracias a la información de fuentes externas de inteligencia, threat hunting y anomalías de red/usuario. Incorpora, además, un cuadro de mando de gestión del servicio, centralizando la información y facilitando su consumo por parte de la organización. LogICA permite adaptarse a las necesidades de despliegue de las organizaciones, en modo on-premise, virtual o entorno cloud.

Observaciones

CCN-STIC-1206 PES NGSiem LogICA

INFORMACIÓN IMPORTANTE

7.3.6 DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS

Google KMS with EKM solution	
Versión	N/A
Fabricante	Google Cloud
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/05/2023
Revisión de Validez	30/04/2025
Descripción	  Google Cloud External Key Manager (EKM) es un servicio de Google Cloud que permite a los clientes generar y gestionar claves criptográficas de cifrado nativo de información en la nube a través de un tercero, protegidas a través de un Hardware criptográfico que está fuera de las infraestructuras de nube de Google. La protección de la información con claves generadas, protegidas y gestionadas fuera del proveedor de nube, habilita escenarios de soberanía del dato desde el momento en que la información almacenada en la nube de Google Cloud solo podrá ser descifrada por el gestor externo de la clave, que podrá ser: • El propio usuario final mediante un módulo EKM instalado en sus propias infraestructuras. • Un socio de confianza del usuario final que hospede y gestione dicho módulo EKM en sus infraestructuras. • Uno de los socios locales de Google Cloud (sometidos exclusivamente a legislación Española) con la infraestructura ya preconfigurada y preparada para ofrecer este servicio desde la plataforma de Google Cloud, como "Control de Soberanía" (por ejemplo, SIA/Minsait/Indra para España, Thales para Francia o T-Systems para Alemania). El servicio EKM se presta desde múltiples regiones de Google Cloud, incluida la de España. Más información aquí: https://cloud.google.com/kms/docs/ekm?hl=es-419
Observaciones	Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

AWS Key Management Service (KMS)

Versión**Fabricante** AWS**Familia** Dispositivos para gestión de claves criptográficas**Tipo** Servicio**Categoría ENS** ALTA**Fecha Inclusión** 01/02/2022**Revisión de Validez** 31/12/2024**Descripción**

AWS Key Management Service (KMS) facilita la creación y la administración de claves criptográficas y el control de su uso en una amplia gama de servicios de AWS y en sus aplicaciones. Utiliza módulos de seguridad de hardware que se han validado según FIPS 140-2 para proteger sus claves.

AWS KMS le proporciona un control centralizado sobre las claves criptográficas que se utilizan para proteger sus datos. El servicio está integrado con otros servicios de AWS, lo que facilita el cifrado de los datos que almacena en estos servicios y el control del acceso a las claves que los descifran. Los servicios integrados con KMS se pueden encontrar en <https://aws.amazon.com/kms/>

Observaciones

CCN-STIC-887A Guía de configuración segura AWS

**INFORMACIÓN IMPORTANTE**

7.4 MONITORIZACIÓN DE LA SEGURIDAD

7.4.1 IDS, IPS Y ANTIDDOs

ASA 5500 Series (5508-X y 5516-X)

Versión	FTD 7.0 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	30/04/2026



Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

SonicWall TZ Serie (300P, 350, 350W, 600P)

Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	28/02/2025



Descripción

La serie TZ de SonicWall ofrece seguridad y rendimiento de entorno Enterprise orientado a pequeñas compañías. Enfocado a entornos departamentales o PYMES de entre 5 y 100 usuarios (aprox), incorpora funciones de prevención de intrusiones, antimalware, filtrado de contenidos/URL y control de aplicaciones a través de redes y entornos inalámbricos. Proporciona inspección profunda de paquetes (DPI), SD-WAN y despliegue zero-touch. Opciones de puertos PoE y wifi 802.11ac. Más info en: <https://www.sonicwall.com/es-mx/products/firewalls/entry-level>

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

Firepower 8000 Series Appliances: Firepower 8350, 8360, 8370, 8390

Versión	6.4
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025

**Descripción**

Sistema de Detección y Prevención de Intrusiones, que consiste en una FMC y sensores.

La FMC proporciona una consola de gestión centralizada y un sistema de base de datos de eventos, agrega y correlaciona datos de intrusión, descubrimiento y conexión, recogidos de los sensores gestionados.

Los sensores monitorizan todo el tráfico de la red en busca de eventos de seguridad y violaciones y pueden alertar o incluso bloquear tráfico malicioso de acuerdo con las reglas definidas para el control de acceso.

Observaciones

CCN-STIC-651B Seguridad en Cortafuegos Cisco Firepower

FMCv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E180D

Versión	6.4
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025

**Descripción**

Sistema de Detección y Prevención de Intrusiones, que consiste en una FMC y sensores.

La FMC proporciona una consola de gestión centralizada y un sistema de base de datos de eventos, agrega y correlaciona datos de intrusión, descubrimiento y conexión, recogidos de los sensores gestionados.

Los sensores monitorizan todo el tráfico de la red en busca de eventos de seguridad y violaciones y pueden alertar o incluso bloquear tráfico malicioso de acuerdo con las reglas definidas para el control de acceso.

Observaciones

CCN-STIC-651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

Firepower AMP Appliances: AMP 8350, 8360, 8370, 8390

Versión	6.4
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025

**Descripción**

Sistema de Detección y Prevención de Intrusiones, que consiste en una FMC y sensores.

La FMC proporciona una consola de gestión centralizada y un sistema de base de datos de eventos, agrega y correlaciona datos de intrusión, descubrimiento y conexión, recogidos de los sensores gestionados. Los sensores monitorizan todo el tráfico de la red en busca de eventos de seguridad y violaciones y pueden alertar o incluso bloquear tráfico malicioso de acuerdo con las reglas definidas para el control de acceso.

Observaciones

CCN-STIC-651B Seguridad en Cortafuegos Cisco Firepower

AWS Shield

Versión	
Fabricante	AWS
Familia	IDS, IPS y AntiDDoS
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	18/11/2024
Revisión de Validez	30/04/2025

**Descripción**

AWS ofrece dos niveles de protección contra los ataques DDoS: AWS Shield Standard y AWS Shield Advanced. AWS Shield Standard se incluye automáticamente sin costo adicional al monto que paga por AWS WAF y sus demás servicios de AWS. Para una protección aún mayor contra los ataques DDoS, AWS ofrece AWS Shield Advanced. AWS Shield Advanced proporciona una mayor protección contra ataques DDoS para sus instancias de Amazon EC2, balanceadores de carga Elastic Load Balancing, distribuciones de Amazon CloudFront y zonas hospedadas de Amazon Route 53.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

ISA 3000 (ISA 3000-4C y ISA 3000-2C2F)

Versión	FTD 7.0 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	30/04/2026

**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

Fortigate/FortiOS

Versión	7.0
Fabricante	Fortinet
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/09/2024
Revisión de Validez	28/02/2025

**Descripción**

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Deep Discovery Inspector

Versión	6.5.1129
Fabricante	Trend Micro
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	N/A
Revisión de Validez	16/05/2026

**Descripción**

Deep Discovery Inspector es una sonda de red anti-APT diseñada para detectar de manera temprana ciberataques en el vector de red (ej.: malware de día 0, movimientos laterales, comunicaciones C&C, exfiltración de datos, explotación de vulnerabilidades etc.). Combinando técnicas de Reputación, Machine Learning y Sandboxing.

Disponible en formato appliance físico o virtual, con distintos niveles de escalado de ancho de banda y configuración de puertos, facilita su implementación en redes con distintos niveles de complejidad.

Integrada con la plataforma XDR Trend Vision One, donde aporta telemetría y detecciones, conforma la plataforma NDR perfecta para hacer frente a los complejos ataques recibidos por el cibercrimen moderno.

Observaciones

CCN-STIC 1227 Procedimiento de Empleo Seguro Deep Discovery Inspector

INFORMACIÓN IMPORTANTE

TippingPoint Threat Protection System

Versión	5.5.5
Fabricante	Trend Micro
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

**Descripción**

Trend Micro™ TippingPoint™ Threat Protection System (TPS) consiste en un appliance IPS dedicado que ofrece protección frente a un amplio catálogo de amenazas: vulnerabilidades y malware tanto conocidos como desconocidos, conexiones sospechosas, geolocalización y filtros de protección frente a DDOS, soportando tráfico asimétrico e inspección SSL.

La combinación de la inteligencia de la Smart Protection Network, Zero Day Initiative y un hardware optimizado proporciona niveles óptimos de rendimiento, baja latencia, gran efectividad, escalabilidad y bajo ratio de falsos positivos.

Dicha tecnología implementa interfaces de red con bypass con el objetivo de evitar interrupciones de tráfico en el caso de fallo hardware del dispositivo.

Adicionalmente, cuenta con la tecnología eVR (Enterprise Vulnerability Remediation), realizando integración con terceros para importar vulnerabilidades y nuevos filtros.

Tipping Point se integra dentro de la arquitectura Vision One XDR y la plataforma Deep Discovery de Trend Micro.

Observaciones

CCN-STIC-1220 PES TIPPING POINT TRENDMICRO

INFORMACIÓN IMPORTANTE

Fortigate/FortiOS

Versión	6.4
Fabricante	Fortinet
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/03/2026

FORTINET**Descripción**

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

FTD Virtual (FTDv) sobre ESXi 6.7 or 7.0 en Cisco Unified Computing System (UCS) - UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 y UCS-E180D-M3 instalado en ISR

Versión	FTD 7.0 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	30/04/2026

CISCO**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

Firepower 2100 Series (2110, 2120, 2130, 2140)

Versión	FTD 7.0 y FMC 7.0
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2026

**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

FMC (Firepower Management Center) Appliances: FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9

Versión	6.4.0.17
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025

**Descripción**

Sistema de Detección y Prevención de Intrusiones, que consiste en una FMC y sensores.

La FMC proporciona una consola de gestión centralizada y un sistema de base de datos de eventos, agrega y correlaciona datos de intrusión, descubrimiento y conexión, recogidos de los sensores gestionados.

Los sensores monitorizan todo el tráfico de la red en busca de eventos de seguridad y violaciones y pueden alertar o incluso bloquear tráfico malicioso de acuerdo con las reglas definidas para el control de acceso.

La versión 6.4.0.17 corrige una vulnerabilidad crítica [CVE-2023-20048] detectada en la versión 6.4 inicialmente cualificada.

Observaciones

CCN-STIC-651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

NGIPSv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E18

Versión	6.4
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025



Descripción

Sistema de Detección y Prevención de Intrusiones, que consiste en una FMC y sensores. La FMC proporciona una consola de gestión centralizada y un sistema de base de datos de eventos, agrega y correlaciona datos de intrusión, descubrimiento y conexión, recogidos de los sensores gestionados. Los sensores monitorizan todo el tráfico de la red en busca de eventos de seguridad y violaciones y pueden alertar o incluso bloquear tráfico malicioso de acuerdo con las reglas definidas para el control de acceso.

Observaciones

CCN-STIC-651B Seguridad en Cortafuegos Cisco Firepower

Cisco FTD (NGFW) 6.4 en Firepower Series 4100 y 9300 con FMC/FMCv

Versión	6.4
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025



Descripción

Los equipos de seguridad Cisco Firepower 4100 y 9300 son plataformas escalables y hechas a propósito con capacidades de Firewall proporcionadas por el software Firepower Threat Defense (FTD) que corre en el sistema operativo FXOS.

Observaciones

CCN-STIC-651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

Firepower 4100 Series (4110, 4112, 4115, 4120, 4125, 4140, 4145 and 4150)

Versión FTD 7.0, FXOS 2.10 y FMC/FMCv 7.0**Fabricante** Cisco Systems**Familia** IDS, IPS y AntiDDoS**Tipo** Producto**Categoría ENS** ALTA**Fecha Inclusión** 19/10/2023**Revisión de Validez** 31/03/2026**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower



FTD Virtual (FTDv) sobre NFVIS 4.4 en ENCS 5406, 5408, y 5412

Versión FTDv 7.0 y FMC/FMCv 7.0**Fabricante** Cisco Systems**Familia** IDS, IPS y AntiDDoS**Tipo** Producto**Categoría ENS** ALTA**Fecha Inclusión** 19/10/2023**Revisión de Validez** 30/04/2026**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

**INFORMACIÓN IMPORTANTE**

Firepower 9300 (including chassis, supervisor blade, and security module)

Versión	FTD 7.0, FXOS 2.10 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2026

**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

Firepower 1000 Series (1010, 1120, 1140, 1150)

Versión	FTD 7.0 y FMC 7.0
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2026

**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

SonicWall SOHO Serie (250, 250W)

Versión 6.5.4.4-44n-federal-12n**Fabricante** SonicWall**Familia** IDS, IPS y AntiDDoS**Tipo** Producto**Categoría ENS** ALTA**Fecha Inclusión** 01/08/2021**Revisión de Validez** 28/02/2025

SONICWALL®

**Descripción**

Los cortafuegos de la serie TZ SOHO de Sonicwall son una solución adecuada para oficinas pequeñas y domésticas, así como para entornos distribuidos en ubicaciones remotas. Despliegan funcionalidades para construir Secure SD-WAN y conectividad WIFI (opcional). El SOHO 250 proporciona un 50% más de rendimiento sobre su antecesor SOHO, así como acceso a los sandboxes avanzados Capture ATP, con lo que se mejora la seguridad en prevención y detección de malware desconocido en un entorno remoto.

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

7.4.2 CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO

AWS CloudWatch

Versión
Fabricante AWS

Familia Captura, Monitorización y Análisis de Tráfico

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/07/2022

Revisión de Validez 31/12/2024

Descripción

Amazon CloudWatch es un servicio de monitorización y administración creado para desarrolladores, operadores de sistemas, ingenieros de fiabilidad (SRE), y administradores de IT. CloudWatch proporciona datos y conocimientos prácticos para monitorizar sus aplicaciones, comprender y responder a los cambios de desempeño de todo el sistema, optimizar la utilización de los recursos y obtener una visión unificada del estado operativo.

Amazon CloudWatch recopila datos operativos y de monitorización en forma de registros, métricas y eventos, proporcionándole una visión unificada de los recursos de AWS, las aplicaciones y los servicios que se ejecutan en AWS y los servidores on-premise.

Puede utilizar CloudWatch para establecer alarmas de alta resolución, visualizar los registros y las métricas de forma paralela, realizar acciones automatizadas, solucionar problemas y descubrir información para optimizar sus aplicaciones y asegurarse de que funcionan correctamente.

Para más información acerca de Amazon CloudWatch, por favor visite <https://aws.amazon.com/es/cloudwatch/>
<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/management-governance.html#amazon-cloudwatch>

Observaciones

CCN-STIC-887A Guía de configuración segura AWS



INFORMACIÓN IMPORTANTE

GigaVUE (GVS-HC301, GVS-HC302, GVS-HC2A1, GVS-HC2A2, GVS-HC101 y GVS-HC102)

Versión	6.1
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	28/06/2023
Revisión de Validez	30/11/2025

**Descripción**

Network Packet Brokers HC Series. Network Packet Brokers de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1g/10g en cobre y funcionalidades de filtrado de tráfico L2-3-4-7 con motor de DPI, generación de Netflow/IPFix/Metadatos, Cifrado/Descifrado de SSL/TLS (incluyendo protocolos RSA, DHE, ECC, y PFS), Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Truncado de paquetes, Eliminación de cabeceras, Enmascarado, De-Duplicación, Clustering, Balanceo, Captura de tráfico para entornos virtuales (VMWare ESX/NSX, Openstack, Kubernetes, AWS, GCP, Azure, Nutanix), simetrización de tráfico para arquitectura HA, Inline Bypass con Heartbeat positivo y negativo, Cambio de medio y velocidad, Bypass HW, TAPs integrados.

Observaciones

CCN-STIC-1301 Procedimiento de Empleo Seguro GigaVUE-OS

GigaVUE (GVS-TAX21-HW, GVS-TAX22-HW, GVS-TAX21A-HW, GVS-TAX22A-HW, GVS-TAC21, GVS-TAC22, GTP-ATX21, GTP-ASF21)

Versión	6.1
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	28/06/2023
Revisión de Validez	30/11/2025

**Descripción**

Network Packet Brokers HC Series. Network Packet Brokers de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1g/10g en cobre y funcionalidades de filtrado de tráfico L2-3-4-7 con motor de DPI, generación de Netflow/IPFix/Metadatos, Cifrado/Descifrado de SSL/TLS (incluyendo protocolos RSA, DHE, ECC, y PFS), Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Truncado de paquetes, Eliminación de cabeceras, Enmascarado, De-Duplicación, Clustering, Balanceo, Captura de tráfico para entornos virtuales (VMWare ESX/NSX, Openstack, Kubernetes, AWS, GCP, Azure, Nutanix), simetrización de tráfico para arquitectura HA, Inline Bypass con Heartbeat positivo y negativo, Cambio de medio y velocidad, Bypass HW, TAPs integrados.

Observaciones

CCN-STIC-1301 Procedimiento de Empleo Seguro GigaVUE-OS

INFORMACIÓN IMPORTANTE

CARMEN

Versión	Versión 7.24.3
Fabricante	S2 GRUPO / CCN
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/07/2026

**Descripción**

CARMEN (Centro de Análisis de Registros y Minería de Eventos) es una solución software de adquisición, procesamiento y análisis de información para soportar el proceso de identificación de Amenazas Persistentes Avanzadas (APT) a partir del tráfico de red interno y saliente de una forma eficiente, apoyando la toma de decisiones a partir de la información generada y procesada. Se compone de agentes que recopilan los flujos de tráfico, un motor de almacenamiento en el que se inserta la información, un sistema de detección de anomalías que se encarga de procesar la información almacenada y una aplicación web que permite la representación y consulta tanto de la información obtenida como de la procesada. Para más información, se puede consultar la web del CCN-CERT (<https://ccn-cert.cni.es/soluciones-seguridad/carmen.html>)

Observaciones

CCN-STIC-1304 Procedimiento de empleo seguro CARMEN

INFORMACIÓN IMPORTANTE

7.4.3 HERRAMIENTAS DE SANDBOX

Deep Discovery Inspector

Versión 6.5.1129

Fabricante Trend Micro

Familia Herramientas de Sandbox

Tipo Producto

Categoría ENS MEDIA

Fecha Inclusión N/A

Revisión de Validez 16/05/2026



Descripción

Deep Discovery Inspector es una sonda de red anti-APT diseñada para detectar de manera temprana ciberataques en el vector de red (ej.: malware de día 0, movimientos laterales, comunicaciones C&C, exfiltración de datos, explotación de vulnerabilidades etc.). Combinando técnicas de Reputación, Machine Learning y Sandboxing.

Disponible en formato appliance físico o virtual, con distintos niveles de escalado de ancho de banda y configuración de puertos, facilita su implementación en redes con distintos niveles de complejidad.

Integrada con la plataforma XDR Trend Vision One, donde aporta telemetría y detecciones, conforma la plataforma NDR perfecta para hacer frente a los complejos ataques recibidos por el cibercrimen moderno.

Observaciones

CCN-STIC 1227 Procedimiento de Empleo Seguro Deep Discovery Inspector

INFORMACIÓN IMPORTANTE

7.5 PROTECCIÓN DE LAS COMUNICACIONES

7.5.1 ENRUTADORES

Dell EMC Networking SmartFabric OS10.5.4 en Switches de las series N, S y Z (N3248TE, S41xx, S52xx, S54xx, Z91xx, Z92xx, Z93xx, Z94xx, Z96xx)

Versión	OS10.5.4
Fabricante	DELL COMPUTER, S.A.
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/03/2026



Descripción

Dell EMC Smart Fabric OS10 es el sistema operativo de red (NOS) que se utiliza en las familias de enrutadores y conmutadores de las serie N (algunos modelos), serie S, serie Z y serie MX de Dell EMC Networking (las plataformas HW que actualmente soportan OS10 son N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n y MX9116n). Dell EMC SmartFabric OS10 es un sistema operativo de red (NOS) que admite múltiples arquitecturas y entornos. La solución SmartFabric OS10 permite la desagregación en varias capas de la funcionalidad de red. SmartFabric OS10 comprende la administración, monitorización y funcionalidad completa y estándar de la industria de redes de nivel 2 y nivel 3 a través de interfaces CLI, SNMP y REST. Los usuarios pueden elegir sus propias aplicaciones de organización, gestión, supervisión y redes de terceros. Para desarrollar redes escalables L2 y L3, SmartFabric OS10 ofrece una solución modular y desagregada en una única imagen binaria.

Observaciones

CCN-STIC-1429 PES DELL EMC Networking

INFORMACIÓN IMPORTANTE

7705 (SAR-18, SAR-8, SAR-F, SAR-M, SAR-W, SAR-Wx, SAR-H, SAR-Hc)

Versión	SAR OS v6.1
Fabricante	NOKIA
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	30/06/2025

NOKIA**Descripción**

La familia de enrutadores de agregación de servicios 7705 SAR de Nokia, ofrece capacidades IP/MPLS e interfaces legacy (serie y TDM) líderes en la industria. Además proporciona plataformas compactas con la capacidad de preparar y agregar de forma fiable y eficiente múltiples contenidos a través de diferentes protocolos de transporte. La gama 7705 SAR de Nokia está optimizada para la adaptación, agregación y enrutamiento multiservicio, especialmente en modernas infraestructuras Ethernet e IP/MPLS.

Gracias al “Service Router Operating System (SR OS)”, y a la capacidad de gestión de red que aporta la solución de “Network Service Platform (NSP)”, ambos productos de Nokia, los enrutadores ofrecen servicios de alta disponibilidad a través de topologías de red flexibles y resistentes, estando disponible en plataformas compactas y de bajo consumo de energía. La familia 7705 SAR resulta adecuada tanto para la agregación del tráfico de red como para la implementación del “backhaul” del acceso radio 3G, LTE y 5G y la conexión de estos servicios a redes IP/MPLS.

EL 7705 SAR de Nokia proporciona una fácil integración de los dispositivos TDM a las redes IP/MPLS. La familia de 7705 SAR ofrece un amplio conjunto de interfaces incluyendo OC-12/STM-4, OC-3/ STM-1, T1/E1, servicios de Teleprotección C37.94 de sistemas eléctricos así como interfaces de voz para telefonía analógica, junto con características de software para retardo asimétrico y compensación por fluctuación. Estas interfaces y sus características garantizan que las aplicaciones incorporadas desde estos dispositivos funcionen exactamente como lo hacen en las redes TDM.

Para garantizar el rendimiento de las aplicaciones de misión crítica, el tráfico se acelera cuando se utiliza cualquiera de las diferentes velocidades Ethernet o enlaces TDM de bajo ancho de banda. Las características de migración de este enrutador permiten a los operadores de red migren de forma eficiente aplicaciones al entorno IP/MPLS.

Observaciones

CCN-STIC-1457 Procedimiento de Empleo Seguro Routers NOKIA SR y SAR

INFORMACIÓN IMPORTANTE

Cisco Embedded Services Router (ESR) 6300

Versión	IOS-XE 17.12
Fabricante	CISCO SYSTEMS, Inc
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/09/2024
Revisión de Validez	28/02/2025

**Descripción**

El TOE incluye componentes de software y hardware. El hardware está representado por dos modelos, el ESR-6300-NCP-K9 y el ESR-6300-CON-K9, mientras que el software es Cisco IOS-XE versión 17.12.

Características clave del ESR6300:

- Tiene un tamaño pequeño, mide 3 pulgadas por 3.75 pulgadas, diseñado para aplicaciones personalizadas.
- Incluye 4 GB de DDR4 DRAM y 4 GB de memoria flash eMMC.
- Hay una carcasa opcional para el enrutador.
- Tiene un conector de interfaz BTB multipin incorporado para conexiones de alimentación, Ethernet y consola. Durante las pruebas, se utilizaron los siguientes puertos:
 - Un puerto de consola UART RS232 RJ45 único.
 - Dos puertos WAN Ethernet Gigabit capaces de operaciones de capa 3.
 - Cuatro puertos LAN Ethernet Gigabit para operaciones de capa 2.

El ESR6300 es una placa de enrutador pequeña y versátil destinada a los socios de Cisco para crear diversos sistemas integrados personalizados. Se adapta a una carcasa especial que coincide con su tamaño y no necesita energía de procesamiento externa. Puede elegir un ESR6300 con una placa de enfriamiento o sin ella. Ambas versiones tienen un conector de interfaz BTB multipin para conectar interfaces de alimentación, Ethernet y consola. Las funciones de seguridad del TOE están contenidas dentro del chasis ESR6300, que alberga la placa y todos sus componentes; no se necesita procesamiento externo para la seguridad.

Cisco Embedded Services Router Series 6300: ESR-6300-NCP-K9, ESR-6300-CON-K9

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9600 Series Switches (C9606R, C9600-SUP-1 y C9600-LC-24C|48YL|48TX|24S)

Versión IOS-XE 17.9 (con fix 17.9.4a)**Fabricante** Cisco Systems**Familia** Enrutadores**Tipo** Producto**Categoría ENS** ALTA**Fecha Inclusión** 13/11/2023**Revisión de Validez** 30/04/2026**Descripción**

Los Cisco Catalyst 9400 9500 y 9600 son equipos de red de alto rendimiento. Ofrecen alta densidad de puertos Ethernet por módulo, con opciones de 10 Gbps, 25 Gbps y 40 Gbps. Están equipados con un procesador que proporciona una alta capacidad de procesamiento y seguridad avanzada.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.



Cisco Catalyst 9200L Series Switches (C9200L-24P-4G|4X, C9200L-24T-4G|4X, C9200L-48P-4G|4X, C9200L-48T-4G|4X, C9200L-48PL-4G|4X, C9200L-24|48PXG-2Y y C9200L-24|48PXG-4X)

Versión IOS-XE 17.9 (con fix 17.9.a)**Fabricante** Cisco Systems**Familia** Enrutadores**Tipo** Producto**Categoría ENS** ALTA**Fecha Inclusión** 14/11/2023**Revisión de Validez** 30/04/2026**Descripción**

Los equipos Cisco Catalyst 9200 y 9200L son switches de alto rendimiento y seguridad reforzada, ideales para empresas que requieren soluciones de red seguras y escalables. Con modelos que varían desde 24 hasta 48 puertos, proporciona una gran flexibilidad para adaptarse a cualquier tamaño de red. Ofrecen gestión avanzada y detección de amenazas mejorada.

Los Cisco Catalyst 9200L son la variante de la serie 9200, manteniendo las mismas características de seguridad y rendimiento. Son ideales para pequeñas y medianas empresas que buscan una red segura y escalable.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.

**INFORMACIÓN IMPORTANTE**

RUCKUS FastIron series ICX7150, ICX7450, ICX7550, ICX7650 e ICX7850 Switch/Router

Versión	9.0.10j
Fabricante	CommScope Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2024
Revisión de Validez	30/11/2026

**Descripción**

La familia RUCKUS ICX de conmutadores de nivel 2 y 3 dispone de una gama de modelos tanto para campus y redes empresariales de 2 y 3 niveles como para Data Center, cubriendo todo el rango de velocidades de puerto desde 1G hasta 100G.

Incluye tecnologías como Stacking a corta y larga distancia, fuentes de alimentación redundantes, nivel 3 avanzado, protocolos de alta disponibilidad, microsegmentación y automatización, entre otras.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

RUCKUS FastIron series ICX8200, ICX7550 e ICX7850 Switch/Router

Versión	10.0.10c
Fabricante	CommScope Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2024
Revisión de Validez	31/10/2026

**Descripción**

La familia RUCKUS ICX de conmutadores de nivel 2 y 3 dispone de una gama de modelos tanto para campus y redes empresariales de 2 y 3 niveles como para Data Center, cubriendo todo el rango de velocidades de puerto desde 1G hasta 100G.

Incluye tecnologías como Stacking a corta y larga distancia, fuentes de alimentación redundantes, nivel 3 avanzado, protocolos de alta disponibilidad, microsegmentación y automatización, entre otras.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Junos OS 22.4R2 MX304

Versión	22.4R2
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	06/05/2024
Revisión de Validez	31/01/2025

JUNIPER
NETWORKS

**Descripción**

Las plataformas de enrutamiento universal MX304 brindan un rendimiento de gran escalabilidad en un factor de forma optimizado para la nube y las economías de coste por puerto o bit más exigentes. Se pueden utilizar tanto en redes de tipo operador, como nodo de borde en redes MPLS, en entornos de movilidad convergente, IoT, empresarial y también en arquitecturas de Core convergente y de borde multiservicio. También soporta el uso como enrutador de conmutación de etiquetas (LSR), provider Edge, equipo de intercambio de Internet y red troncal para implementaciones en redes de carácter metropolitanas, regionales o nacionales, o terminador de túneles IPSEC o Firewall de capa 4. La serie MX admite un amplio conjunto de funcionalidades IPoDWDM, L2, L3, IP/MPLS, SR, SRv6, o terminador de túneles IPSEC para permitir redes de transporte a gran escala con operaciones y aprovisionamiento de servicios simplificados, manteniendo simplicidad en la red. Gracias al tipo de chipsets implementados, tienen una capacidad de programación en el plano de datos casi infinita, lo que le brinda la libertad de implementar nuevas innovaciones de red. Con tecnología de silicio TRIO, la familia MX304 es altamente escalable desde los 1.6Tbps, pasando por 3.2 Tbps hasta los 4.8 Tbps en 2U dependiendo del número de slots utilizados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Ruckus FastIron Series ICX 7550 e ICX 7850. Switch/Router

Versión	09.0.10
Fabricante	CommScope Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025

**Descripción**

La familia RUCKUS ICX de conmutadores de nivel 2 y 3 dispone de una gama de modelos tanto para campus y redes empresariales de 2 y 3 niveles como para Data Center, cubriendo todo el rango de velocidades de puerto desde 1G hasta 100G.

Incluye tecnologías como Stacking a corta y larga distancia, fuentes de alimentación redundantes, nivel 3 avanzado, protocolos de alta disponibilidad, microsegmentación y automatización, entre otras.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

QFX5120-48YM

Versión	Junos OS 22.3R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/05/2024
Revisión de Validez	31/01/2025

JUNIPER
NETWORKS

**Descripción**

Las familias QFX5k, en sus diferentes variantes, son dispositivos de red seguros con alta densidad de puertos 1GbE, 10GbE, 25GbE y 100GbE. Estas plataformas de conmutación para el centro de datos funcionan con el software Junos OS, que es un sistema operativo especialmente diseñado para este tipo de dispositivos. Junos OS proporciona funciones de gestión, control y monitorización, así como toda la provisión de cambios en los dispositivos.

Estos switches para centros de datos son dispositivos de red que soportan la definición, y cumplimiento, de políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión segura.

Como switch de nivel 2 en la capa OSI, realiza el análisis de paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario.

Como switch de nivel 3 en la capa OSI, admite el enrutamiento del tráfico, basado en tablas, identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar el camino más adecuado para cada paquete.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500) (C8200-1N-4T, C8200L-1N-4T, C8500L-8S4X)

Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/03/2024
Revisión de Validez	31/08/2026

**Descripción**

Los routers Cisco Catalyst 8200 y 8500 Series son parte de la cartera de soluciones de Cisco para redes de bordes de la empresa, diseñados para ofrecer una conectividad segura y de alto rendimiento para sucursales y servicios de red en la nube. Estos routers están especialmente diseñados para soportar la creciente demanda de aplicaciones en la nube, movilidad y aumento en el tráfico de datos. Ambas series se integran sin problemas con la arquitectura de red de Cisco, ofreciendo una gestión simplificada y una operatividad mejorada a través de herramientas como Cisco SD-WAN y Cisco DNA Center, permitiendo a las organizaciones modernizar su infraestructura de red y optimizar la experiencia de usuario final.

La serie 8200 es ideal para sucursales medianas a grandes, ofreciendo una plataforma optimizada para la integración de servicios de red, seguridad avanzada y capacidades de enrutamiento flexibles. Con opciones de rendimiento modular, estos routers permiten a las empresas escalar según sus necesidades específicas.

Por su parte, la serie 8500 está orientada a entornos empresariales de alta densidad y centros de datos, proporcionando una solución robusta para el enrutamiento de bordes con capacidades de agregación. Estos routers de alto rendimiento son adecuados para aplicaciones intensivas en ancho de banda y para manejar grandes volúmenes de tráfico de datos con una seguridad integrada de grado empresarial.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

NE40E 8000 Series Routers running VRP software

Versión	V800R012C00SPC300
Fabricante	Huawei Technologies España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	31/12/2024

**Descripción**

Los routers NE40E y NetEngine 8000 equipados con los chipsets NP y la plataforma VRP cumplen con los requisitos de baja latencia y alta fiabilidad tanto de los servicios críticos para el negocio como de las soluciones SDN-WAN avanzadas. Funcionan como nodos core WAN, nodos de acceso en redes de gran escala, nodos de agregación e interconexión en redes de campus y nodos edge en redes IDC de gran escala, ofreciendo un elevado rendimiento (hasta 14.4 tbit/s por stolt), alta fiabilidad, bajo consumo energético y una densidad de puertos por encima de la media. Con un diseño compacto, disipación del calor optimizada y un consumo energético muy bajo, permite construir redes ultra-broadband simplificadas y convergentes.

Observaciones

CCN-STIC-1419 Procedimiento de empleo seguro Routers Huawei NE40E Series

INFORMACIÓN IMPORTANTE

RouterTeldat-M1 Series

Versión	11.01.09
Fabricante	TEL DAT, S.A.
Familia	Enrutadores
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2023
Revisión de Validez	31/10/2025

**Descripción**

Se trata de una familia de routers compactos orientados a oficinas pequeñas y medianas, pero que requieren conexión de alta velocidad. Su diseño compacto y sin ventiladores, para no generar ruido, permiten instalarlo en áreas de trabajo, algo muy útil en pequeñas oficinas, tiendas o despachos profesionales. Además, en estos entornos esta familia de routers favorece el uso de conexiones 3G/4G por la mayor disponibilidad de cobertura que en instalaciones realizadas en salas o armarios técnicos. A pesar de ser routers compactos, algunos modelos pueden alcanzar velocidades de hasta 600 Mbps simétricos, y son muy escalables gracias a un slot y una amplia variedad de tarjetas. Integran conectividad Ethernet WAN y conmutador Ethernet de 4 puertos LAN, además de un punto de acceso Wi-Fi y conectividad 3G/4G. Además de un sofisticado hardware, incluyen un avanzado software adaptado a redes profesionales que incluye todas las funcionalidades demandadas a un router profesional como routing (RIP, OSPF, BGP, VRF, PolicyRouting,...), seguridad (ACLs, Firewall, IPSec, 802.1X, ...), calidad de servicio (CBWFQ, PQ, perfilado, ...), o gestión (CLI, SNMPv3, RADIUS, TACACS+, Syslog, Netflow, Mirroring,...).

Observaciones

CCN-STIC-1455 Procedimiento de empleo seguro Teldat M1 Series

INFORMACIÓN IMPORTANTE

MX204

Versión	Junos 22.3R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/05/2024
Revisión de Validez	31/01/2025


**Descripción**

Las plataformas de enrutamiento universal MX204 brindan un rendimiento de gran escalabilidad en un factor de forma optimizado para la nube y las economías de coste por puerto o bit más exigentes. Se pueden utilizar tanto en redes de tipo operador, como nodo de borde en redes MPLS, en entornos de movilidad convergente, IoT, empresarial y también en arquitecturas de Core convergente y de borde multiservicio. También soporta el uso como enrutador de conmutación de etiquetas (LSR), provider Edge, equipo de intercambio de Internet y red troncal para implementaciones en redes de carácter metropolitanas, regionales o nacionales, o terminador de túneles IPSEC o Firewall de capa 4. La serie MX admite un amplio conjunto de funcionalidades IPoDWDM, L2, L3, IP/MPLS, SR o SRv6, para permitir redes de transporte a gran escala con operaciones y aprovisionamiento de servicios simplificados, manteniendo simplicidad en la red. Gracias al tipo de chipsets implementados, tienen una capacidad de programación en el plano de datos casi infinita, lo que le brinda la libertad de implementar nuevas innovaciones de red. Con tecnología de silicio TRIO, la familia MX204 es altamente escalable hasta 400Gbps en 1U.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Cisco ASR9000 Series y NCS4200 Series (ASR902, ASR903, ASR907, ASR920 y NCS4201, NCS4202, NCS4206, NCS4216)

Versión	IOS-XE 16.9
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025


**Descripción**

Las familias ASR900 y NCS4200 son equipos hechos a propósito como plataformas de routing, soportando adicionalmente cifrado MACsec.

Observaciones

CCN-STIC 1454 Procedimiento de Empleo Seguro Routers CISCO ASR9000 y NCS4200 Series

INFORMACIÓN IMPORTANTE

Aruba HPE 2930F, 2930M, 3810M, and 5400R Switch Series

Versión	ArubaOS 16.11
Fabricante	HPE Aruba Networking
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	27/12/2023
Revisión de Validez	31/12/2024

**Descripción**

Equipos diseñados para utilizarse en labores de acceso y agregación, o núcleo de red de acceso. Son equipos que proporcionan conexiones de todas las velocidades y tipos de medios. Equipos con capacidad de conmutación sin bloqueo (non-blocking). Según la familia, ofrecen soluciones escalables mediante constitución de stacks via puerto de red, puerto dedicado así como existen modelos de chasis. Todas las funciones del sistema operativo se ofrecen con el equipo. Ofrecen diversos tipos de interfaces y velocidades. Ofrecen PoE en algunos modelos, a diferentes potencias.

Pueden ser gestionables, tanto localmente (gestión on-premise) como pueden llegar a administrarse en modalidad Software-as-a-Service

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7950 (XRS-40, XRS-20, XRS-16C), 7750 (SR-12e, SR-12, SR-7, SR-c12, SR-c4), 7450 (ESS-1, ESS-6, ESS-6v, ESS-7, ESS-12)

Versión	SR OSv12.0
Fabricante	NOKIA
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	30/06/2025

NOKIA



Descripción

La plataforma de enrutamiento Core 7950 XRS de Nokia proporciona la escalabilidad, la eficiencia y la versatilidad necesarias a las demandas de servicio impulsadas por la nube, el 5G y el Internet de las cosas. El 7950 XRS se ha implementado por operadores de telecomunicaciones, cable, móviles, servicios públicos y redes privadas de cualquier tamaño, así como por los principales operadores de escala web y proveedores de intercambio de Internet.

El diseño de hardware modular y extensible impulsado por el microprocesador de silicio de enrutamiento FP4 de Nokia garantiza un escalado granular y económico de la capacidad de conmutación y la densidad de puertos con un rendimiento de reenvío determinista. Un solo chasis 7950 XRS-20e equipado con hardware FP4 ofrece una capacidad de conmutación dúplex completa de hasta 48 Tb/s y admite densidades de puertos de hasta 160 puertos de interfaz 400GE, 800 100GE o 4800 10GE.

La familia 7750 Service Router (SR) de Nokia ofrece enrutadores de borde multiservicio de alto rendimiento diseñados para el soporte simultáneo de servicios avanzados de usuario final, empresariales y móviles en una plataforma de borde IP común.

La familia de enrutadores 7750 SR permite la creación de una amplia gama de servicios IP disponibles para las grandes empresas y operadores con requisitos excepcionales de rendimiento, escalabilidad e inteligencia de servicio. La familia 7750 SR utiliza el Sistema Operativo del enrutador de servicios de Nokia (SR OS) y soporta la gestión de los servicios para mejorar la eficiencia operativa.

La familia 7750 SR dispone de la capacidad de servicio para admitir múltiples aplicaciones y funciones en una plataforma común. El innovador diseño de refrigeración térmica "front-to-back" compatible con NEBS de los 7750 SR base para un crecimiento futuro. La familia 7750 SR-e ofrece densidad Gigabit Ethernet (GE) de alta densidad y 10GE, 100GE y 400GE para la distribución de 10GE y 100GE en redes de acceso y agregación.

Observaciones

CCN-STIC-1457 Procedimiento de Empleo Seguro Routers NOKIA SR y SAR

INFORMACIÓN IMPORTANTE

HPE Aruba Networking CX 4100i, 6000, 6100, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, y 10000

Versión	10.13
Fabricante	HPE Aruba Networking
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	20/03/2024
Revisión de Validez	31/12/2024

**Descripción**

La familia Aruba CX implementan soluciones de switching y routing para redes de sucursales, campus y datacenter. Los equipos 10000, 8320, 8325, 8360, y 8400 son idóneos para Datacenter y equipos nucleo (core) de la red de campus. Los equipos 6400 se posicionan como equipos nucleo (core) de la red de campus, mientras los 6300 y 6200 están orientados para redes de acceso. Implementan funcionalidades multicapa, implementan múltiples mecanismos de seguridad en el acceso y administración. Orientado a la segmentación dinámica y a implementar entornos Zero Trust. Permite el despliegue automático desasistido (ZTP) Aruba CX dispone de una arquitectura interna de Sistema Operativo que proporciona una forma de trabajar con el completamente programable. Su motor de analíticas (NAE) permite la inserción de scripts de para la ejecución de tareas avanzadas de monitorización y respuestas a eventos. Los equipos 4100i son equipos con protección medioambientales y de formato industrial.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Cisco Nexus 9200 Series Switches (92348GC-X, 92160YC-X, 92300YC, 9272Q)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	10/04/2025

**Descripción**

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9

INFORMACIÓN IMPORTANTE

MX240, MX480 y MX960 con tarjetas MPC10E y MX-SPC3

Versión	22.2R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2024
Revisión de Validez	31/01/2025

JUNIPER
NETWORKS

**Descripción**

Las plataformas de enrutamiento y switching universal MX240/MX480/MX960 brindan un rendimiento de gran escalabilidad en un factor de forma optimizado para la nube y las economías de coste por puerto o bit más

exigentes. Se pueden utilizar tanto en redes de tipo operador, como nodo de borde en redes MPLS, en entornos de movilidad convergente, IoT, empresarial y también en arquitecturas de Core convergente y de borde multiservicio. También soporta el uso como enrutador de conmutación de etiquetas (LSR), provider Edge, equipo de intercambio de Internet y red troncal para implementaciones en redes de carácter metropolitanas, regionales o nacionales, o terminador de túneles IPSEC o Firewall de capa 4. La serie MX admite un amplio conjunto de funcionalidades IPoDWDM, L2, L3, IP/MPLS, SR, SRv6, terminador de túneles IPSEC o CGNAT para permitir redes de transporte a gran escala con operaciones y provisión de servicios simplificados, manteniendo simplicidad en la red. Gracias al tipo de chipsets implementados, tienen una capacidad de programación en el plano de datos casi infinita, lo que le brinda la libertad de implementar nuevas innovaciones de red. Con tecnología de silicio TRIO, la familia MX es altamente escalable desde los 3Tbps en 5U, hasta un rendimiento de 12 Tbps en 16 slots.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

EX9200(9204|9208|9214) con tarjetas EX9200-15C

Versión	Junos OS 22.3R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/05/2024
Revisión de Validez	31/01/2025

JUNIPER
NETWORKS

**Descripción**

Las plataformas de switching y enrutamiento EX9204, EX9208 y EX9214 brindan un rendimiento de gran escalabilidad en un factor de forma optimizado para la nube y las economías de coste por puerto o bit más exigentes. Estas plataformas permiten a las empresas desplegar redes de campus, centro de datos y Core que admiten aplicaciones de Capa 2 o 3 mediante la combinación de tecnologías tales como Ethernet VPN (EVPN) o LAN virtual extensible (VXLAN). Se pueden utilizar tanto en redes de tipo operador, como redes empresariales en arquitecturas de Core convergente. La serie EX9200 admite un amplio conjunto de funcionalidades L2, L3, VXLAN, IP/MPLS para permitir redes de transporte a gran escala, manteniendo simplicidad en la red. Gracias al tipo de chipsets implementados, tienen una capacidad de programación en el plano de datos casi infinita, lo que le brinda la libertad de implementar nuevas innovaciones de red. Con tecnología de silicio Juniper One, la familia EX9200 es altamente escalable permitiendo hasta un rendimiento máximo de 12 Tbps en 16 slots.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

MXs (MX240|480|960) con tarjetas MPC10E y MX-SPC3

Versión	Junos 22.3R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/05/2024
Revisión de Validez	31/01/2025


**Descripción**

Las plataformas de enrutamiento y switching universal MX240/MX480/MX960 brindan un rendimiento de gran escalabilidad en un factor de forma optimizado para la nube y las economías de coste por puerto o bit más

exigentes. Se pueden utilizar tanto en redes de tipo operador, como nodo de borde en redes MPLS, en entornos de movilidad convergente, IoT, empresarial y también en arquitecturas de Core convergente y de borde multiservicio. También soporta el uso como enrutador de conmutación de etiquetas (LSR), provider Edge, equipo de intercambio de Internet y red troncal para implementaciones en redes de carácter metropolitanas, regionales o nacionales, o terminador de túneles IPSEC o Firewall de capa 4. La serie MX admite un amplio conjunto de funcionalidades IPoDWDM, L2, L3, IP/MPLS, SR, SRv6, terminador de túneles IPSEC o CGNAT para permitir redes de transporte a gran escala con operaciones y provisión de servicios simplificados, manteniendo simplicidad en la red. Gracias al tipo de chipsets implementados, tienen una capacidad de programación en el plano de datos casi infinita, lo que le brinda la libertad de implementar nuevas innovaciones de red. Con tecnología de silicio TRIO, la familia MX es altamente escalable desde los 3Tbps en 5U, hasta un rendimiento de 12 Tbps en 16 slots.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

Cisco Catalyst 9300L Series Switches (C9300L-24T|P-4G, C9300L-48T|P|PF-4G, C9300L-24T|P|UXG-4X, C9300L-48T|P|PF|UXG-4X, C9300L-24UXG-2Q, C9300L-48UXG-2Q)

Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	14/11/2023
Revisión de Validez	30/04/2026


**Descripción**

Los Cisco Catalyst 9300y 9300L son switches de red que ofrecen una alta densidad puertos Ethernet por módulo, incluyendo opciones de PoE+. Están diseñados con un potente procesador y ofrecen servicios de red avanzados para empresas que necesitan una red segura y escalable. Los Cisco Catalyst 9300L, la variante compacta de la serie 9300, ideales para pequeñas y medianas empresas.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.

INFORMACIÓN IMPORTANTE

MX10003

Versión	Junos OS 22.2R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026


**Descripción**

Las plataformas de enrutamiento universal MX10000 brindan un rendimiento de gran escalabilidad y un factor de forma optimizado para la nube y las economías de coste por puerto o bit más exigentes. Se pueden utilizar tanto en redes de tipo operador como nodo de borde PE en una red MPLS, como en entornos de movilidad convergente, IoT, empresarial y también en arquitecturas de Core convergente y de borde multiservicio. También soporta el uso como enrutador de conmutación de etiquetas (LSR), provider Edge, equipo de intercambio de Internet y red troncal para implementaciones en redes de carácter metropolitanas, regionales o nacionales. La serie MX admite un amplio conjunto de funcionalidades IPoDWDM, L2, L3, IP/MPLS, SR, SRv6 para permitir redes de transporte a gran escala con operaciones y aprovisionamiento de servicios simplificados, manteniendo simplicidad en la red. Gracias al tipo de chipsets implementados, tienen una capacidad de programación de plano de datos casi infinita, lo que le brinda la libertad de implementar nuevas innovaciones de red.

Con tecnología de silicio TRIO, la familia MX10000 es altamente escalable desde los 2.4Tbps en 3U, pasando por 38,4 Tbps en 7 slots y hasta un rendimiento de 76,8 Tbps en 13 slots.

Observaciones

CCN-STIC 1456 Procedimiento de Empleo Seguro Juniper MX10003 JunOS 22.2R1

Cisco Catalyst 9500 Series Switches (C9500-12Q|24Q|40X|16X|32C|32QC|24Y4C|48Y4C) con los siguientes módulos de red (C9500-NM-8X y C9500-NM-2Q)

Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	13/11/2023
Revisión de Validez	30/04/2026


**Descripción**

Los Cisco Catalyst 9400 9500 y 9600 son equipos de red de alto rendimiento. Ofrecen alta densidad de puertos Ethernet por módulo, con opciones de 10 Gbps, 25 Gbps y 40 Gbps. Están equipados con un procesador que proporciona una alta capacidad de procesamiento y seguridad avanzada.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9200 Series Switches (C9200-24T, C9200-48T, C9200-24P, C9200-48P, C9200-24PB, C9200-48PB, C9200-48PL, C9200-24PXG, C9200-48PXG) con los módulos de red (C9200-NM-4G|4X|2Y|2Q)

Versión IOS-XE 17.9 (con fix 17.9.a)

Fabricante Cisco Systems

Familia Enrutadores

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 14/11/2023

Revisión de Validez 30/04/2026

Descripción

Los equipos Cisco Catalyst 9200 y 9200L son switches de alto rendimiento y seguridad reforzada, ideales para empresas que requieren soluciones de red seguras y escalables. Con modelos que varían desde 24 hasta 48 puertos, proporciona una gran flexibilidad para adaptarse a cualquier tamaño de red. Ofrecen gestión avanzada y detección de amenazas mejorada.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.



Cisco Catalyst 9400 Series Switches (C9404R, C9407R, C9410R, C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y, C9400-LC-24S|48S|24XS|48P|48T|48U|48UX|48H)

Versión IOS-XE 17.9 (con fix 17.9.4a)

Fabricante Cisco Systems

Familia Enrutadores

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 13/11/2023

Revisión de Validez 30/04/2026

Descripción

Los Cisco Catalyst 9400 9500 y 9600 son equipos de red de alto rendimiento. Ofrecen alta densidad de puertos Ethernet por módulo, con opciones de 10 Gbps, 25 Gbps y 40 Gbps. Están equipados con un procesador que proporciona una alta capacidad de procesamiento y seguridad avanzada.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.



INFORMACIÓN IMPORTANTE

Routers ATN (ATN 980C, ATN 950D, ATN 910C-G & ATN 910D-A) running VRP software

Versión	V300R006C10SPC300
Fabricante	Huawei Technologies España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2022
Revisión de Validez	31/03/2025

**Descripción**

La serie ATN 980C, 950D, 910C-G y 910D-A de Huawei son routers de acceso multiservicio que se han introducido en la transición a LTE y a la cobertura FMC de los operadores.

El objetivo de la serie ATN de Huawei es ofrecer soluciones de red de portadoras de IP de gama alta. Ofrece características ricas de segunda y tercera capa y cuenta con comodidades como el mantenimiento y la administración remotos, la ausencia de puesta en marcha in situ y la funcionalidad plug-and-play.

La serie ATN es compatible con el acceso virtual SDN y está pensada para satisfacer las necesidades de la capa de acceso, los dispositivos de despliegue a gran escala y el acceso a servicios integrados. Al ser un router de acceso multiservicio compacto de 2U de altura y 10GE, puede compartir un armario con la estación base, con una capacidad de conmutación de hasta 56G y soportar un acceso máximo de 8*10GE.

Observaciones

CCN-STIC-1439 Procedimiento de empleo seguro Enrutadores ATN de Huawei

INFORMACIÓN IMPORTANTE

EX4650-48Y, QFX5120-32C, QFX5210-64C, QFX5120- 48T, QFX5120-48Y, QFX5200-32C y QFX5200-48Y

Versión	Junos OS 22.3R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2024
Revisión de Validez	31/01/2025


**Descripción**

Las familias QFX5k, en sus diferentes variantes, son dispositivos de red seguros con alta densidad de puertos 1GbE, 10GbE, 25GbE y 100GbE. Estas plataformas de conmutación para el centro de datos funcionan con el software Junos OS, que es un sistema operativo especialmente diseñado para este tipo de dispositivos. Junos OS proporciona funciones de gestión, control y monitorización, así como toda la provisión de cambios en los dispositivos.

Estos switches para centros de datos son dispositivos de red que soportan la definición, y cumplimiento, de políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión segura.

Como switch de nivel 2 en la capa OSI, realiza el análisis de paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario.

Como switch de nivel 3 en la capa OSI, admite el enrutamiento del tráfico, basado en tablas, identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar el camino más adecuado para cada paquete.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Huawei S Series Ethernet Switches S6735 (S6735-S24X6C y S6735-S48X6C) y S12700 (S12700E-4, S12700E-8 y S12700E-12)

Versión	V200R022C00SPC500
Fabricante	Huawei Technologies España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026

**Descripción**

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet

INFORMACIÓN IMPORTANTE

Huawei S Series Ethernet Switches S5735S (H24S4XC-A, L12P4S-A, L12T4S-A, L24FT4S-A, L24P4S-A, L24P4S-A1, L24P4S-MA, L24P4X-A, L24P4X-A1, L24T4S-A, L24T4S-A1, L24T4S-MA, L24T4X-A, L24T4X-A1, L32ST4X-A, L32ST4X-A1, L48FT4S-A, L48P4S-A, L48P4S-A1, L48P4X-A, L48P4X-A1, L48T4S-A, L48T4S-A1, L48T4S-MA, L48T4X-A, L48T4X-A1, L8P4S-A1, L8T4S-A1, S24P4X-A, S24T4S-A, S24T4X-A, S32ST4X-A, S48P4X-A, S48T4S-A, S48T4X-A)

Versión V200R022C00SPC500

Fabricante Huawei Technologies España

Familia Enrutadores

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/08/2023

Revisión de Validez 31/01/2026

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet



Huawei S Series Ethernet Switches S5731 (H24P4XC, H24T4XC, H48P4XC, H48T4XC, S24P4X, S24T4X, S48P4X, S48T4X, H24HB4XZ, H24P4XC-K, H24T4XC-K, H48HB4XZ, H48P4XC-K, H48T4XC-B, S24N4X2Q-A, S24T4X-A, S24T4X-D, S24UN4X2Q, S32ST4X, S32ST4X-A, S32ST4X-D, S48S4X, S48S4X-A, S48T4X-A) y S5731S (S8UM16UN2Q, H24HB4XZ-A, H24T4S-A, H24T4X-A, H24T4XC-A, H48HB4XZ-A, H48T4S-A, H48T4X-A, H48T4XC-A)

Versión V200R022C00SPC500

Fabricante Huawei Technologies España

Familia Enrutadores

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/08/2023

Revisión de Validez 31/12/2026

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet



INFORMACIÓN IMPORTANTE

Huawei CloudEngine 16800 (CE16804, CE16808 y CE16816), Huawei CloudEngine 12800 (CE12804, CE12808 y CE12816), Huawei CloudEngine 8800 (CE8861-4C-EI y CE8850-64CQ-EI), Huawei CloudEngine 6800 (CE6863-48S6CQ, CE6881-48S6CQ, CE6881-48T6CQ, CE6820-48S6CQ, CE6863E-48S6CQ, CE6870-48S6CQ-EI, CE6870-48S6CQ-EI-A), CE5882-48T4S, CE9860-4C-EI Y CE9860-4C-EI-A

Versión V200R022C00SPC500
Fabricante Huawei Technologies España
Familia Enrutadores

Tipo Producto

Categoría ENS ALTA
Fecha Inclusión 01/08/2023
Revisión de Validez 31/01/2026

Descripción

Los switches CloudEngine son switches que proporcionan servicios estables, fiables y de alto rendimiento en capa 2 y capa 3. Estos switches están diseñados para centros de datos y redes de campus de alta gama. Proporcionan alto rendimiento, interfaces de alta densidad y baja latencia. Los switches CloudEngine Series tienen un diseño hardware avanzado que suministra puertos de alta densidad mientras usa la misma plataforma software Huawei VRP.

Observaciones

CCN-STIC 1424 Procedimiento de Empleo Seguro Huawei CE Series Switches



Cisco Nexus 3200 Series Switches (3232C, 3264C-E)

Versión NX-OS 9.3
Fabricante Cisco Systems
Familia Enrutadores

Tipo Producto

Categoría ENS ALTA
Fecha Inclusión 01/02/2022
Revisión de Validez 10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



INFORMACIÓN IMPORTANTE

Cisco Nexus 3500 Series Switches (3524-X/XL, 3548-X/XL)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 3600 Series Switches (36180YC-R, 3636C-R)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9

**INFORMACIÓN IMPORTANTE**

Cisco Nexus 3400 Series Switches (34180-YC, 3464C, 3432D-S, 3408-S)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Catalyst 9400X/9600X (C9404R, C9407R, C9410R, C9400X-SUP-2, C9400X-SUP-2XL, C9400-LC-48HX, C9400-LC-48XS, C9606R, C9600X-SUP2, C9600-LC-40YL4CD, C9600X-LC-32CD)

Versión	IOS-XE 17.9
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2024
Revisión de Validez	31/07/2026

Descripción

Los Cisco Catalyst 9400X/9600X son switches de red que ofrecen una alta densidad puertos Ethernet por módulo, incluyendo opciones de PoE+. Están diseñados con un potente procesador y ofrecen servicios de red avanzados para empresas que necesitan una red segura y escalable. Son equipos de red de alto rendimiento. Ofrecen alta densidad de puertos Ethernet por módulo, con opciones de 10 Gbps, 25 Gbps y 40 Gbps. Están equipados con un procesador que proporciona una alta capacidad de procesamiento y seguridad avanzada.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.

**INFORMACIÓN IMPORTANTE**

Cisco Catalyst 9300 Series Switches (C9300-24T|P|U|AUX|S|H, C9300-48T|P|U|UXM|UN|S|H, C9300D-24UB|UXB, C9300D-48UB) con los siguientes módulos de red (C9300-NM-4G|8X|2Q|4M|2Y)

Versión IOS-XE 17.9 (con fix 17.9.4a)

Fabricante Cisco Systems

Familia Enrutadores

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 10/11/2023

Revisión de Validez 30/04/2026

Descripción

Los Cisco Catalyst 9300y 9300L son switches de red que ofrecen una alta densidad puertos Ethernet por módulo, incluyendo opciones de PoE+. Están diseñados con un potente procesador y ofrecen servicios de red avanzados para empresas que necesitan una red segura y escalable. Los Cisco Catalyst 9300L, la variante compacta de la serie 9300, ideales para pequeñas y medianas empresas.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.



Ekinops One 2501

Versión OneOS6.12.x5patch01

Fabricante Ekinops

Familia Enrutadores

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 11/07/2024

Revisión de Validez 31/12/2024

Descripción

OneOS6 es una solución de software modular que permite activar una gama de servicios integrados de forma remota y bajo demanda.

Observaciones

N/A



INFORMACIÓN IMPORTANTE

HUAWEI CX600&PTN6900 series Routers

Versión	V800R021C00SPC100
Fabricante	Huawei Technologies Co.,Ltd.
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	11/07/2024
Revisión de Validez	31/12/2024

**Descripción**

Los routers Huawei serie CX600&PTN 6900 que usan el software VRP, se utilizan para satisfacer los requisitos de diferentes tipos de redes. Se pueden desplegar en el borde de las redes troncales IP, redes de área metropolitana IP (MANs) y otras redes IP a gran escala, también se pueden utilizar para acceder, agregar y transmitir servicios Ethernet en redes de área metropolitana (MANs) de convergencia fijo-móvil (FMC).

Observaciones

N/A

Cisco Nexus 9300 Series Switches (93108TC-EX, 93108TC-FX, 9348GC-FXP, 93216TC-FX2, 93180LC-EX, 93180YC-EX, 93180YC-FX, 93240YC-FX2, 93360YC-FX2, 9364C, 9332C, 9336C-FX2, 9364C-GX, 9316D-GX, 93600CD-GX)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	04/10/2025

**Descripción**

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9

INFORMACIÓN IMPORTANTE

Cisco Nexus 9500 Series Switches (9504, 9508, 9516, Supervisor 9500-Sup-A , Supervisor 9500-Sup-A +, Supervisor 9500-Sup-B , Supervisor 9500-Sup-B +, System Controller N9k-SC-A)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	04/10/2025



Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9

Atlas-840, M10-Smart Series, M2 Series, 4GePlus Series, Teldat-5Ge Series, 5Ge-Rail Series, Connect-4GePlus Series, Connect-5Ge Series, Connect-FW Series

Versión	11.02.02.85.03
Fabricante	TEL DAT, S.A.
Familia	Enrutadores
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	20/08/2024
Revisión de Validez	31/01/2025



Descripción

Familia de routers corporativos para los servicios de comunicaciones en redes físicas o en la nube. Disponen, según modelos, de múltiples tecnologías de conexión(WAN, WWAN, LAN, WLAN) y ofrecen una solución eficiente en todo tipo de escenarios, garantizando los SLAs que los usuarios requieren. Estos equipos se integran dentro de los servicios digitales de las empresas facilitando su despliegue, elevando la seguridad e integridad tanto de los datos como del hardware, y optimizando las aplicaciones de los usuarios.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800) y Cisco Catalyst 8300 Rugged Series Routers (IR8300)

Versión IOS-XE 17.9 (con fix 17.9.4a)

Fabricante Cisco Systems

Familia Enrutadores

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/09/2023

Revisión de Validez 28/02/2026

Descripción



Cisco Catalyst 8000V Edge (C8000V): C8000V virtual router deployed on one of the following compatible platforms:

- Cisco UCS C-Series M5 Servers with Intel Xeon Scalable 2nd Generation (Cascade Lake)
- General-purpose computing platforms with Intel Broadwell processors: Xeon D-1559
- General-purpose computing platforms with Intel Goldmont processors: Atom E3950
- General-purpose computing platforms with Intel Coffee Lake processors: Xeon E-2254ML

Cisco 1000 Series Integrated Services Routers (ISR1000):

- IR1821-K9
- IR1831-K9
- IR1833-K9
- IR1835-K9

Cisco Catalyst 1800 Rugged Series Routers (IR1800):

- C1131

Cisco Catalyst 8300 Rugged Series Routers (IR8300):

- IR8340-K9

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.

INFORMACIÓN IMPORTANTE

Huawei S Series Ethernet Switches S5732 (H24S6Q, H24UM2CC, H48S6Q, H48UM2CC, H48XUM2CC, H24S6Q-K, H24UM2C-K, H48S6Q-K, H48UM2C-K)

Versión V200R022C00SPC500

Fabricante Huawei Technologies España

Familia Enrutadores

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/08/2023

Revisión de Validez 31/12/2026

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet



Huawei S Series Ethernet Switches S6730 (H24X6C, H48X6C, S24X6Q, H24X4Y4C, H24X6C-K, H28Y4C, H28Y4C-K, H48X6C-K) y S6730S (H24X6C-A, S24X6C-A)

Versión V200R022C00SPC500

Fabricante Huawei Technologies España

Familia Enrutadores

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/08/2023

Revisión de Validez 31/01/2026

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet



INFORMACIÓN IMPORTANTE

Huawei S Series Ethernet Switches S5735 (L12P4S-A, L12T4S-A, L24P4S-A, L24P4S-A1, L24P4X-A, L24P4X-A1, L24T4S-A, L24T4S-A1, L24T4S-QA1, L24T4X-A, L24T4X-A1, L24T4X-QA1, L32ST4X-A, L32ST4X-A1, L48P4S-A1, L48P4X-A, L48P4X-A1, L48T4S-A, L48T4S-A1, L48T4X-A, L48T4X-A1, L8P4S-A1, L8P4S-QA1, L8P4X-A1, L8T4S-A1, L8T4S-QA1, L8T4X-A1, S24P4X, S24T4X, S24T4X-I, S32ST4X, S48P4X, S48S4X, S48T4X, L24T4X-D, L24T4X-D1, L24T4X-IA1, L32ST4X-D, L32ST4X-D1, L8P4X-IA1, L8T4X-IA1)

Versión V200R022C00SPC500

Fabricante Huawei Technologies España

Familia Enrutadores

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/08/2023

Revisión de Validez 31/01/2026

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet



Huawei S Series Ethernet Switches S5736 (S24UM4XC, S48S4X-A, S24S4XC, S24T4XC, S24U4XC, S48S4XC, S48S4X-D, S48T4XC, S48U4XC)

Versión V200R022C00SPC500

Fabricante Huawei Technologies España

Familia Enrutadores

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/08/2023

Revisión de Validez 31/01/2026

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet



INFORMACIÓN IMPORTANTE

Huawei NetEngine AR6700&AR8000 (AR8140-12G10XG, AR8140-T-12G10XG, AR6710-L26T2X4, AR6710-L26T2X4-T, AR6710-L50T2X4, AR6710-L50T2X4-T) Series Routers

Versión	V600R021C10SPC100
Fabricante	Huawei Technologies Co., Ltd.
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2024
Revisión de Validez	31/07/2026

**Descripción**

Las plataformas de enrutamiento Huawei AR son los primeros diseñados para la era de la cloud, presenta enlaces ascendente de banda ultra ancha 4G/5G y cuenta con un rendimiento de reenvío que es tres veces el promedio de la industria. Ofreciendo además diversas características. Compatible con la red definida por software (SD-WAN), la gestión de la nube, la red privada virtual (VPN), la conmutación de etiquetas (MPLS), la seguridad y la voz.

Observaciones

CCN-STIC 1452 Huawei NetEngine AR6700&AR8000

EX4400-24T|24P|24MP, EX4400-48T|48P|48F|48MP

Versión	Junos OS 22.3R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/05/2024
Revisión de Validez	31/01/2025

**Descripción**

La familia de switches EX4400, en sus diferentes variantes, son dispositivos de red seguros con alta densidad de puertos 10/100/1000Base-T, 100/1000/2500/5000/10000Base-T, así como uplinks 1/10/25GbE o 40/100GbE o variantes con todos sus puertos en fibra. Todas las plataformas EX4400 funcionan con el software Junos OS, que es un sistema operativo especialmente diseñado para este tipo de dispositivos. Junos OS proporciona funciones de gestión, control y monitorización, así como toda la provisión de cambios en los dispositivos. Los switches EX4400 son dispositivos de red que soportan la definición, y cumplimiento, de políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión segura. Como switch de nivel 2 en la capa OSI, realiza el análisis de paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario. Como switch de nivel 3 en la capa OSI, admite el enrutamiento del tráfico, basado en tablas, identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar el camino más adecuado para cada paquete.

Observaciones

Procedimientos de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

EX4100-24P|24T|24MP, EX4100-48P|48T|48MP

Versión	Junos OS 22.4R2
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/04/2024
Revisión de Validez	31/01/2025

JUNIPER
NETWORKS

**Descripción**

La familia de switches EX4100, en sus diferentes variantes, son dispositivos de red seguros con alta densidad de puertos 10/100/1000Base-T o multigigabit 100/1000/2500/5000/10000Base-T así como puertos de uplinks 1/10/25GbE. Todas las plataformas EX4100 funcionan con el software Junos OS, que es un sistema operativo especialmente diseñado para este tipo de dispositivos de red. Junos OS proporciona funciones de gestión, control y monitorización, así como toda la provisión de cambios en los dispositivos. Los switches EX4100 son dispositivos de red que soportan la definición, y cumplimiento, de políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad en el tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión segura. Como switch de nivel 2 en la capa OSI, realiza el análisis de paquetes entrantes, reenvía dichos paquetes en función de la información que contienen en su cabecera Ethernet, haciéndolos llegar así a su destinatario. Como switch de nivel 3 en la capa OSI, permite el enrutamiento del tráfico, basado en tablas, identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar el camino más adecuado para cada paquete. La familia EX4100 soporta también el uso de tecnologías de overlay como es el caso de EVPN-VXLAN que permiten la microsegmentación usando group-based policies (GBP), además de soportar MACsec AES-256 y Power over Ethernet.

Observaciones

Procedimiento de Empleo Seguro Pendiente de Publicación

INFORMACIÓN IMPORTANTE

ACX5448, ACX5448-M y ACX5448-D

Versión	Junos OS 22.3R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/05/2024
Revisión de Validez	31/01/2025

JUNIPER
NETWORKS

**Descripción**

La línea Juniper Networks ACX5448 surge como respuesta a un cambio en las arquitecturas de redes metropolitanas donde las capas de acceso y agregación están extendiendo la inteligencia operativa desde el extremo del proveedor de servicios hasta la red de acceso. Está basada en la simplificación de la arquitectura y en la reducción de costos, la línea ACX5448 brinda a los proveedores de servicios y empresas la capacidad de adoptar una solución metro universal.

Asimismo, proporciona alta capacidad, escalabilidad y una capa de transporte óptico de paquetes, al tiempo que ofrece un rendimiento líder en la industria con una amplia gama de densidades de puertos y tipos de interfaz. La serie ACX presenta el liderazgo IP/MPLS de Juniper desde el core y el perímetro de la red hasta las capas de acceso. La serie ACX admite un amplio conjunto de funcionalidades L2, L3 e IP/MPLS para permitir redes MPLS transparentes a gran escala con operaciones y aprovisionamiento de servicios simplificados manteniendo simplicidad en la red.

ACX5448: El ACX5448 tiene 48 puertos 1GbE/10GbE y 4 puertos 40GbE/100GbE, así como soporte de tecnología PON.

ACX5448-M: El ACX5448-M tiene 44 puertos 1GbE/10GbE y 6 puertos 40GbE/100GbE, así como capacidades de seguridad avanzadas tales como MACsec en todos los puertos 1GbE/10GbE y soporte de tecnología PON.

ACX5448-D: El ACX5448-M tiene 36 puertos 1GbE/10GbE, 2 puertos 40GbE/100GbE y 2 puertos 100G/200G DWDM para ópticas CFP2-DCO y soporte de tecnología PON.

Observaciones

CCN-STIC-1445 PES Router_Juniper_ACX5448-M_JunOS 20.3R1 en proceso de actualización.

INFORMACIÓN IMPORTANTE

Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches IE-9310-26S2C-E | A, IE-9320-26S2C-E | A, IE-9320-22S2C4X-E | A, IE-9320-24P4S-E | A, IE-9320-24T | P4X-E | A, IE-9320-16P8U4X-E | A

Versión	IOS-XE 17.9
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2024
Revisión de Validez	30/06/2026



Descripción

Los Catalyst Industrial Ethernet 9300 Rugged Series Switches son equipos diseñados para entornos industriales exigentes. Este switch es resistente y duradero, capaz de soportar condiciones extremas. Ofrece una conectividad confiable y segura para dispositivos industriales, como cámaras de vigilancia, sensores y controladores. Tiene múltiples puertos Ethernet que permiten la conexión de varios dispositivos y garantizan una comunicación fluida en la red.

Además, son equipos fáciles de configurar y administrar, lo que lo hace adecuado para entornos industriales donde se requiere una infraestructura de red robusta y confiable.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.5.2 SWITCHES

Dell EMC Networking SmartFabric OS10.5.4en Switches de las series N, S y Z (N3248TE, S41xx, S52xx, S54xx, Z91xx, Z92xx, Z93xx, Z94xx, Z96xx)

Versión OS10.5.4

Fabricante DELL COMPUTER, S.A.

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/10/2023

Revisión de Validez 31/03/2026

Descripción

Dell EMC Smart Fabric OS10 es el sistema operativo de red (NOS) que se utiliza en las familias de enrutadores y conmutadores de las serie N (algunos modelos), serie S, serie Z y serie MX de Dell EMC Networking (las plataformas HW que actualmente soportan OS10 son N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n y MX9116n). Dell EMC SmartFabric OS10 es un sistema operativo de red (NOS) que admite múltiples arquitecturas y entornos. La solución SmartFabric OS10 permite la desagregación en varias capas de la funcionalidad de red. SmartFabric OS10 comprende la administración, monitorización y funcionalidad completa y estándar de la industria de redes de nivel 2 y nivel 3 a través de interfaces CLI, SNMP y REST. Los usuarios pueden elegir sus propias aplicaciones de organización, gestión, supervisión y redes de terceros. Para desarrollar redes escalables L2 y L3, SmartFabric OS10 ofrece una solución modular y desagregada en una única imagen binaria.

Observaciones

CCN-STIC-1429 PES DELL EMC Networking



Cisco Catalyst 9600 Series Switches (C9606R, C9600-SUP-1 y C9600-LC-24C|48YL|48TX|24S)

Versión IOS-XE 17.9 (con fix 17.9.4a)

Fabricante Cisco Systems

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 13/11/2023

Revisión de Validez 30/04/2026

Descripción

Los Cisco Catalyst 9400 9500 y 9600 son equipos de red de alto rendimiento. Ofrecen alta densidad de puertos Ethernet por módulo, con opciones de 10 Gbps, 25 Gbps y 40 Gbps. Están equipados con un procesador que proporciona una alta capacidad de procesamiento y seguridad avanzada.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.



INFORMACIÓN IMPORTANTE

Cisco Catalyst 9400X/9600X Series Switches 17.12

Versión	IOS-XE 17.12.02
Fabricante	Cisco Systems, Inc.
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/11/2024
Revisión de Validez	30/04/2025

**Descripción**

Los Cisco Catalyst 9400X/9600X Series Switches 17.12 son soluciones avanzadas para redes empresariales y campus.

Estos switches modulares ofrecen conectividad de alta velocidad con puertos de 10, 25, 40, 100 y hasta 400 Gbps, proporcionando una Plataforma robusta para la agregación y el núcleo de la red.

El Catalyst 9400X es ideal para acceso y distribución, con características como ventiladores de servicio dual y flujo de aire lateral, optimizado para entornos de armarios de cableado.

Por otro lado, el Catalyst 9600X está diseñado para resiliencia a gran escala, con seguridad integral y capacidad de crecimiento.

Ambos modelos soportan tecnologías avanzadas como Cisco StackWise Virtual, que permite la virtualización de la pila de switches para una mayor flexibilidad y redundancia.

Además, incluyen soporte para inspección ARP y protección contra servidores DHCP no autorizados en entornos VXLAN.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

EX4100-F-12P|24P|48P, EX4100-F-12T|24T|48T Junos OS 22.4R2

Versión	22.4R2
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	22/04/2024
Revisión de Validez	31/01/2025

JUNIPER
NETWORKS

**Descripción**

La familia de switches EX4100, en sus diferentes variantes, son dispositivos de red seguros con alta densidad de puertos 10/100/1000Base-T o multigigabit 100/1000/2500/5000/10000Base-T así como puertos de uplinks 1/10/25GbE. Todas las plataformas EX4100 funcionan con el software Junos OS, que es un sistema operativo especialmente diseñado para este tipo de dispositivos de red. Junos OS proporciona funciones de gestión, control y monitorización, así como toda la provisión de cambios en los dispositivos. Los switches EX4100 son dispositivos de red que soportan la definición, y cumplimiento, de políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad en el tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión segura. Como switch de nivel 2 en la capa OSI, realiza el análisis de paquetes entrantes, reenvía dichos paquetes en función de la información que contienen en su cabecera Ethernet, haciéndolos llegar así a su destinatario. Como switch de nivel 3 en la capa OSI, permite el enrutamiento del tráfico, basado en tablas, identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar el camino más adecuado para cada paquete. La familia EX4100 soporta también el uso de tecnologías de overlay como es el caso de EVPN-VXLAN que permiten la microsegmentación usando group-based policies (GBP), además de soportar MACsec AES-256 y Power over Ethernet.

Observaciones

Procedimiento de Empleo Seguro Pendiente de Publicación

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9200L Series Switches (C9200L-24P-4G|4X, C9200L-24T-4G|4X, C9200L-48P-4G|4X, C9200L-48T-4G|4X, C9200L-48PL-4G|4X, C9200L-24|48PXG-2Y y C9200L-24|48PXG-4X)

Versión IOS-XE 17.9 (con fix 17.9.a)

Fabricante Cisco Systems

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 14/11/2023

Revisión de Validez 30/04/2026

Descripción

Los equipos Cisco Catalyst 9200 y 9200L son switches de alto rendimiento y seguridad reforzada, ideales para empresas que requieren soluciones de red seguras y escalables. Con modelos que varían desde 24 hasta 48 puertos, proporciona una gran flexibilidad para adaptarse a cualquier tamaño de red. Ofrecen gestión avanzada y detección de amenazas mejorada.

Los Cisco Catalyst 9200L son la variante de la serie 9200, manteniendo las mismas características de seguridad y rendimiento. Son ideales para pequeñas y medianas empresas que buscan una red segura y escalable.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.



RUCKUS FastIron series ICX7150, ICX7450, ICX7550, ICX7650 e ICX7850 Switch/Router

Versión 9.0.10j

Fabricante CommScope Technologies

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/06/2024

Revisión de Validez 30/11/2026

Descripción

La familia RUCKUS ICX de conmutadores de nivel 2 y 3 dispone de una gama de modelos tanto para campus y redes empresariales de 2 y 3 niveles como para Data Center, cubriendo todo el rango de velocidades de puerto desde 1G hasta 100G.

Incluye tecnologías como Stacking a corta y larga distancia, fuentes de alimentación redundantes, nivel 3 avanzado, protocolos de alta disponibilidad, microsegmentación y automatización, entre otras.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.



INFORMACIÓN IMPORTANTE

RUCKUS FastIron series ICX8200, ICX7550 e ICX7850 Switch/Router

Versión	10.0.10c
Fabricante	CommScope Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2024
Revisión de Validez	31/10/2026

**Descripción**

La familia RUCKUS ICX de conmutadores de nivel 2 y 3 dispone de una gama de modelos tanto para campus y redes empresariales de 2 y 3 niveles como para Data Center, cubriendo todo el rango de velocidades de puerto desde 1G hasta 100G.

Incluye tecnologías como Stacking a corta y larga distancia, fuentes de alimentación redundantes, nivel 3 avanzado, protocolos de alta disponibilidad, microsegmentación y automatización, entre otras.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Junos OS 22.4R2 MX304

Versión	22.4R2
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	06/05/2024
Revisión de Validez	31/01/2025

**Descripción**

Las plataformas de enrutamiento universal MX304 brindan un rendimiento de gran escalabilidad en un factor de forma optimizado para la nube y las economías de coste por puerto o bit más exigentes. Se pueden utilizar tanto en redes de tipo operador, como nodo de borde en redes MPLS, en entornos de movilidad convergente, IoT, empresarial y también en arquitecturas de Core convergente y de borde multiservicio. También soporta el uso como enrutador de conmutación de etiquetas (LSR), provider Edge, equipo de intercambio de Internet y red troncal para implementaciones en redes de carácter metropolitanas, regionales o nacionales, o terminador de túneles IPSEC o Firewall de capa 4. La serie MX admite un amplio conjunto de funcionalidades IPoDWDM, L2, L3, IP/MPLS, SR, SRv6, o terminador de túneles IPSEC para permitir redes de transporte a gran escala con operaciones y aprovisionamiento de servicios simplificados, manteniendo simplicidad en la red. Gracias al tipo de chipsets implementados, tienen una capacidad de programación en el plano de datos casi infinita, lo que le brinda la libertad de implementar nuevas innovaciones de red. Con tecnología de silicio TRIO, la familia MX304 es altamente escalable desde los 1.6Tbps, pasando por 3.2 Tbps hasta los 4.8 Tbps en 2U dependiendo del número de slots utilizados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9500 Series Switches (C9500-12Q, C9500-24Q, C9500-40X, C9500-16X, C9500-32C, C9500-32QC, C9500-24Y4C, C9500-48Y4C) con los siguientes módulos de red (C9500-NM-8X y C9500-NM-2Q)

Versión	IOS-XE 17.6.6a
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

Descripción

Cisco Catalyst 9500 Series Switches

Observaciones

CCN-STIC-1458 Procedimiento de Empleo Seguro CISCO Routers y Switches IOS-XE 17.X La versión inicial cualificada fue la 17.6 pero tras la publicación de la vulnerabilidad pública [CVE-2023-20198], CISCO ha publicado una nueva versión con el fix (17.6.6a).



Cisco Embedded Services 9300 & 3300 Series Switches (ESS-3300-NCP | CON, ESS-3300-24T-NCP | CON, ESS-9300-10X-E)

Versión	IOS-XE 17.9
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/03/2024
Revisión de Validez	31/08/2026

Descripción

Los Cisco Embedded Services 9300 y 3300 Series Switches son plataformas de conmutación integradas y altamente versátiles, diseñadas para aplicaciones empresariales y de Internet de las Cosas (IoT) que requieren una integración y resistencia excepcionales en entornos desafiantes.

La serie 9300 es un conjunto de switches de alto rendimiento con capacidades de Layer 2 y Layer 3, ofreciendo funcionalidades avanzadas de enrutamiento y seguridad. Estos switches están equipados con la tecnología de Cisco IOS XE, lo que les permite manejar aplicaciones intensivas en datos y proporcionar una conectividad confiable y segura para dispositivos de borde.

La serie 3300 está diseñada para entornos industriales y de transporte, con un factor de forma compacto y resistente, cumpliendo con los estándares de durabilidad industrial. Estos switches soportan una amplia gama de voltajes de entrada y tienen clasificaciones extendidas de temperatura, lo que los hace ideales para su uso en condiciones adversas donde otros equipos podrían fallar.

Ambas series ofrecen características como Power over Ethernet (PoE) y PoE+, optimizando la instalación de dispositivos de IoT al permitir la transmisión de datos y energía eléctrica a través del mismo cable de red. Con la gestión inteligente de energía y una arquitectura de hardware confiable, los Cisco Embedded Services 9300 y 3300 Series Switches son soluciones robustas para redes que demandan resistencia y rendimiento en cualquier entorno.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación



INFORMACIÓN IMPORTANTE

Ruckus FastIron Series ICX 7550 e ICX 7850. Switch/Router

Versión	09.0.10
Fabricante	CommScope Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025

**Descripción**

La familia RUCKUS ICX de conmutadores de nivel 2 y 3 dispone de una gama de modelos tanto para campus y redes empresariales de 2 y 3 niveles como para Data Center, cubriendo todo el rango de velocidades de puerto desde 1G hasta 100G.

Incluye tecnologías como Stacking a corta y larga distancia, fuentes de alimentación redundantes, nivel 3 avanzado, protocolos de alta disponibilidad, microsegmentación y automatización, entre otras.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

QFX5120-48T, QFX5120-48Y, QFX5120-32C, QFX5210-64C, EX4650-48Y y QFX5200-48Y

Versión	OS 20.2R1-S1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2022
Revisión de Validez	30/12/2024

**Descripción**

Las familias QFX5k y EX4650, en sus diferentes variantes, son dispositivos de red seguros con alta densidad de puertos 1GbE, 10GbE, 25GbE y 100GbE. Estas plataformas de conmutación para el centro de datos funcionan con el software Junos OS, que es un sistema operativo especialmente diseñado para este tipo de dispositivos. Junos OS proporciona funciones de gestión, control y monitorización, así como toda la provisión de cambios en los dispositivos.

Estos switches para centros de datos son dispositivos de red que soportan la definición, y cumplimiento, de políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión segura.

Como switch de nivel 2 en la capa OSI, realiza el análisis de paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario.

Como switch de nivel 3 en la capa OSI, admite el enrutamiento del tráfico, basado en tablas, identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar el camino más adecuado para cada paquete.

Observaciones

CCN-STIC-1440 Juniper QFX-EX JunOS 20.2

INFORMACIÓN IMPORTANTE

QFX5120-48YM

Versión	Junos OS 22.3R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/05/2024
Revisión de Validez	31/01/2025


**Descripción**

Las familias QFX5k, en sus diferentes variantes, son dispositivos de red seguros con alta densidad de puertos 1GbE, 10GbE, 25GbE y 100GbE. Estas plataformas de conmutación para el centro de datos funcionan con el software Junos OS, que es un sistema operativo especialmente diseñado para este tipo de dispositivos. Junos OS proporciona funciones de gestión, control y monitorización, así como toda la provisión de cambios en los dispositivos.

Estos switches para centros de datos son dispositivos de red que soportan la definición, y cumplimiento, de políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión segura.

Como switch de nivel 2 en la capa OSI, realiza el análisis de paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario.

Como switch de nivel 3 en la capa OSI, admite el enrutamiento del tráfico, basado en tablas, identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar el camino más adecuado para cada paquete.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Cisco Catalyst 9200CX Series Switches

Versión	IOS-XE 17.9
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	20/03/2024
Revisión de Validez	31/12/2024


**Descripción**

Los Cisco Catalyst 9200CX son switches compactos de la serie Catalyst, diseñado para espacios pequeños, ofrece capacidades de conmutación de nivel empresarial, seguridad, PoE y soporte para IoT, ideal para micro sucursales y entornos con limitaciones de espacio.

Catalyst 9200CX incluyen:

C9200CX-12T-2X2G

C9200CX-12P-2X2G

C9200CX-8P-2X2G

Observaciones

Procedimiento de Empleo Seguro Pendiente de Publicación

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9300X Series Switches

Versión	IOS-XE 17.9
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	20/03/2024
Revisión de Validez	31/12/2024

**Descripción**

Los Cisco Catalyst 9300X son una línea de switches de red de la serie Catalyst, que representan la siguiente generación de dispositivos de conmutación de acceso empresarial. Estos switches ofrecen un alto rendimiento, son apilables y están diseñados para soportar una amplia gama de funcionalidades como seguridad avanzada, automatización y conectividad de alta densidad con soporte para tecnologías como Wi-Fi 6, mGig y UPOE+ (Universal Power Over Ethernet Plus). Son adecuados para organizaciones que requieren una infraestructura de red ágil y preparada para el futuro en entornos de campus y sucursales. Catalyst 9300X incluyen:

C9300X-48HX con los siguientes módulos de red: C9300X-NM-4C, C9300X-NM-8M, C9300X-NM-2C, C9300X-NM-8Y

C9300X-48TX con los siguientes módulos de red: C9300X-NM-4C, C9300X-NM-8M, C9300X-NM-2C, C9300X-NM-8Y

C9300X-12Y con los siguientes módulos de red: C9300X-NM-8M, C9300X-NM-2C, C9300X-NM-8Y

C9300X-24Y con los siguientes módulos de red: C9300X-NM-4C, C9300X-NM-8M, C9300X-NM-2C, C9300X-NM-8Y

C9300X-48HXN con los siguientes módulos de red: C9300X-NM-8M, C9300X-NM-2C, C9300X-NM-8Y

C9300X-24HX con los siguientes módulos de red: C9300X-NM-8M, C9300X-NM-2C, C9300X-NM-8Y

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9500X Series Switches

Versión	IOS-XE 17.9
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	20/03/2024
Revisión de Validez	31/12/2024

**Descripción**

Los Cisco Catalyst 9500X forman parte del portafolio de switches de núcleo y distribución de alto rendimiento. Estos dispositivos están diseñados para satisfacer las necesidades de redes de campus, ofreciendo una gran capacidad de conmutación, altas velocidades de puerto, y soporte para tecnologías de red de próxima generación. Con características avanzadas de seguridad, automatización y analítica, los Catalyst 9500X son ideales para entornos que requieren una infraestructura de red robusta, segura y de alta eficiencia.

Catalyst 9500X incluyen:

C9500X-28C8D

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

RouterTeldat-M1 Series

Versión	11.01.09
Fabricante	TEL DAT, S.A.
Familia	Switches
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2023
Revisión de Validez	31/10/2025

**Descripción**

Se trata de una familia de routers compactos orientados a oficinas pequeñas y medianas, pero que requieren conexión de alta velocidad. Su diseño compacto y sin ventiladores, para no generar ruido, permiten instalarlo en áreas de trabajo, algo muy útil en pequeñas oficinas, tiendas o despachos profesionales. Además, en estos entornos esta familia de routers favorece el uso de conexiones 3G/4G por la mayor disponibilidad de cobertura que en instalaciones realizadas en salas o armarios técnicos. A pesar de ser routers compactos, algunos modelos pueden alcanzar velocidades de hasta 600 Mbps simétricos, y son muy escalables gracias a un slot y una amplia variedad de tarjetas. Integran conectividad Ethernet WAN y conmutador Ethernet de 4 puertos LAN, además de un punto de acceso Wi-Fi y conectividad 3G/4G. Además de un sofisticado hardware, incluyen un avanzado software adaptado a redes profesionales que incluye todas las funcionalidades demandadas a un router profesional como routing (RIP, OSPF, BGP, VRF, PolicyRouting,...), seguridad (ACLs, Firewall, IPSec, 802.1X, ...), calidad de servicio (CBWFQ, PQ, perfilado, ...), o gestión (CLI, SNMPv3, RADIUS, TACACS+, Syslog, Netflow, Mirroring,...).

Observaciones

CCN-STIC-1455 Procedimiento de empleo seguro Teldat M1 Series

INFORMACIÓN IMPORTANTE

MX204

Versión	Junos 22.3R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/05/2024
Revisión de Validez	31/01/2025

JUNIPER
NETWORKS

**Descripción**

Las plataformas de enrutamiento universal MX204 brindan un rendimiento de gran escalabilidad en un factor de forma optimizado para la nube y las economías de coste por puerto o bit más exigentes. Se pueden utilizar tanto en redes de tipo operador, como nodo de borde en redes MPLS, en entornos de movilidad convergente, IoT, empresarial y también en arquitecturas de Core convergente y de borde multiservicio. También soporta el uso como enrutador de conmutación de etiquetas (LSR), provider Edge, equipo de intercambio de Internet y red troncal para implementaciones en redes de carácter metropolitanas, regionales o nacionales, o terminador de túneles IPSEC o Firewall de capa 4. La serie MX admite un amplio conjunto de funcionalidades IPoDWDM, L2, L3, IP/MPLS, SR o SRv6, para permitir redes de transporte a gran escala con operaciones y aprovisionamiento de servicios simplificados, manteniendo simplicidad en la red. Gracias al tipo de chipsets implementados, tienen una capacidad de programación en el plano de datos casi infinita, lo que le brinda la libertad de implementar nuevas innovaciones de red. Con tecnología de silicio TRIO, la familia MX204 es altamente escalable hasta 400Gbps en 1U.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9300LM Series Switches

Versión	IOS-XE 17.9
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	20/03/2024
Revisión de Validez	31/12/2024

**Descripción**

Los Cisco Catalyst 9300LM son parte de la serie Catalyst, son switches de acceso empresarial diseñados para redes de campus y sucursales. La variante "LM" se enfoca en ofrecer capacidades de multigigabit Ethernet (mGig) que permiten velocidades de red superiores a 1 Gbps en cableado de cobre existente. Estos switches son apilables y soportan funcionalidades avanzadas como seguridad integrada, automatización y una plataforma preparada para soportar aplicaciones de IoT. Son ideales para escenarios que demandan alta densidad de conectividad y velocidades de red elevadas para manejar el creciente tráfico de datos y dispositivos conectados.

Catalyst 9300LM incluyen:

C9300LM-24U
C9300LM-48UX
C9300LM-48T
C9300LM-48U

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

EX4300-48MP

Versión	Junos OS 19.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2022
Revisión de Validez	31/12/2024

JUNIPER
NETWORKS

**Descripción**

La familia de switches EX4300, en sus diferentes variantes, son dispositivos de red seguros con alta densidad de puertos 10/100/1000Base-T o 100/1000/2500/5000/10000Base-T así como uplinks 1/10/25GbE o 40/100GbE. Todas las plataformas EX4300 funcionan con el software Junos OS, que es un sistema operativo especialmente diseñado para este tipo de dispositivos. Junos OS proporciona funciones de gestión, control y monitorización, así como toda la provisión de cambios en los dispositivos.

Los switches EX4300 son dispositivos de red que soportan la definición, y cumplimiento, de políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión segura.

Como switch de nivel 2 en la capa OSI, realiza el análisis de paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario.

Como switch de nivel 3 en la capa OSI, admite el enrutamiento del tráfico, basado en tablas, identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar el camino más adecuado para cada paquete.

Observaciones

CCN-STIC-1441 JUNIPER EX4300-48MP 19.4R1

INFORMACIÓN IMPORTANTE

Aruba HPE 2930F, 2930M, 3810M, and 5400R Switch Series

Versión	ArubaOS 16.11
Fabricante	HPE Aruba Networking
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	27/12/2023
Revisión de Validez	31/12/2024

**Descripción**

Equipos diseñados para utilizarse en labores de acceso y agregación, o núcleo de red de acceso. Son equipos que proporcionan conexiones de todas las velocidades y tipos de medios. Equipos con capacidad de conmutación sin bloqueo (non-blocking). Según la familia, ofrecen soluciones escalables mediante constitución de stacks via puerto de red, puerto dedicado así como existen modelos de chasis. Todas las funciones del sistema operativo se ofrecen con el equipo. Ofrecen diversos tipos de interfaces y velocidades. Ofrecen PoE en algunos modelos, a diferentes potencias.

Pueden ser gestionables, tanto localmente (gestión on-premise) como pueden llegar a administrarse en modalidad Software-as-a-Service

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

HPE Aruba Networking CX 4100i, 6000, 6100, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, y 10000

Versión	10.13
Fabricante	HPE Aruba Networking
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	20/03/2024
Revisión de Validez	31/12/2024

**Descripción**

La familia Aruba CX implementan soluciones de switching y routing para redes de sucursales, campus y datacenter. Los equipos 10000, 8320, 8325, 8360, y 8400 son idóneos para Datacenter y equipos núcleo (core) de la red de campus. Los equipos 6400 se posicionan como equipos núcleo (core) de la red de campus, mientras los 6300 y 6200 están orientados para redes de acceso. Implementan funcionalidades multicapa, implementan múltiples mecanismos de seguridad en el acceso y administración. Orientado a la segmentación dinámica y a implementar entornos Zero Trust. Permite el despliegue automático desasistido (ZTP) Aruba CX dispone de una arquitectura interna de Sistema Operativo que proporciona una forma de trabajar con el completamente programable. Su motor de analíticas (NAE) permite la inserción de scripts de para la ejecución de tareas avanzadas de monitorización y respuestas a eventos. Los equipos 4100i son equipos con protección medioambientales y de formato industrial.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco Nexus 9200 Series Switches (92348GC-X, 92160YC-X, 92300YC, 9272Q)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



MX240, MX480 y MX960 con tarjetas MPC10E y MX-SPC3

Versión	22.2R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2024
Revisión de Validez	31/01/2025

Descripción

Las plataformas de enrutamiento y switching universal MX240/MX480/MX960 brindan un rendimiento de gran escalabilidad en un factor de forma optimizado para la nube y las economías de coste por puerto o bit más

exigentes. Se pueden utilizar tanto en redes de tipo operador, como nodo de borde en redes MPLS, en entornos de movilidad convergente, IoT, empresarial y también en arquitecturas de Core convergente y de borde multiservicio. También soporta el uso como enrutador de conmutación de etiquetas (LSR), provider Edge, equipo de intercambio de Internet y red troncal para implementaciones en redes de carácter metropolitanas, regionales o nacionales, o terminador de túneles IPSEC o Firewall de capa 4. La serie MX admite un amplio conjunto de funcionalidades IPoDWDM, L2, L3, IP/MPLS, SR, SRv6, terminador de túneles IPSEC o CGNAT para permitir redes de transporte a gran escala con operaciones y provisión de servicios simplificados, manteniendo simplicidad en la red. Gracias al tipo de chipsets implementados, tienen una capacidad de programación en el plano de datos casi infinita, lo que le brinda la libertad de implementar nuevas innovaciones de red. Con tecnología de silicio TRIO, la familia MX es altamente escalable desde los 3Tbps en 5U, hasta un rendimiento de 12 Tbps en 16 slots.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

**INFORMACIÓN IMPORTANTE**

Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12

Versión	IOS-XE 17.12
Fabricante	Cisco Systems, Inc.
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	03/12/2024
Revisión de Validez	31/05/2025

**Descripción**

Los switches Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 son switches de capa de acceso de tipo empresarial para despliegues de sucursales.

Los conmutadores se utilizan para conectar varios dispositivos, como ordenadores, puntos de acceso inalámbricos, impresoras y servidores en la misma red dentro de un edificio o campus.

Un switch o conmutador permite que los dispositivos conectados compartan información y se comuniquen entre sí, y es un componente clave de cualquier red.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

EX9200(9204|9208|9214) con tarjetas EX9200-15C

Versión	Junos OS 22.3R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/05/2024
Revisión de Validez	31/01/2025

**Descripción**

Las plataformas de switching y enrutamiento EX9204, EX9208 y EX9214 brindan un rendimiento de gran escalabilidad en un factor de forma optimizado para la nube y las economías de coste por puerto o bit más exigentes. Estas plataformas permiten a las empresas desplegar redes de campus, centro de datos y Core que admiten aplicaciones de Capa 2 o 3 mediante la combinación de tecnologías tales como Ethernet VPN (EVPN) o LAN virtual extensible (VXLAN). Se pueden utilizar tanto en redes de tipo operador, como redes empresariales en arquitecturas de Core convergente. La serie EX9200 admite un amplio conjunto de funcionalidades L2, L3, VXLAN, IP/MPLS para permitir redes de transporte a gran escala, manteniendo simplicidad en la red. Gracias al tipo de chipsets implementados, tienen una capacidad de programación en el plano de datos casi infinita, lo que le brinda la libertad de implementar nuevas innovaciones de red. Con tecnología de silicio Juniper One, la familia EX9200 es altamente escalable permitiendo hasta un rendimiento máximo de 12 Tbps en 16 slots.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

MXs (MX240|480|960) con tarjetas MPC10E y MX-SPC3

Versión	Junos 22.3R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/05/2024
Revisión de Validez	31/01/2025


**Descripción**

Las plataformas de enrutamiento y switching universal MX240/MX480/MX960 brindan un rendimiento de gran escalabilidad en un factor de forma optimizado para la nube y las economías de coste por puerto o bit más

exigentes. Se pueden utilizar tanto en redes de tipo operador, como nodo de borde en redes MPLS, en entornos de movilidad convergente, IoT, empresarial y también en arquitecturas de Core convergente y de borde multiservicio. También soporta el uso como enrutador de conmutación de etiquetas (LSR), provider Edge, equipo de intercambio de Internet y red troncal para implementaciones en redes de carácter metropolitanas, regionales o nacionales, o terminador de túneles IPSEC o Firewall de capa 4. La serie MX admite un amplio conjunto de funcionalidades IPoDWDM, L2, L3, IP/MPLS, SR, SRv6, terminador de túneles IPSEC o CGNAT para permitir redes de transporte a gran escala con operaciones y provisión de servicios simplificados, manteniendo simplicidad en la red. Gracias al tipo de chipsets implementados, tienen una capacidad de programación en el plano de datos casi infinita, lo que le brinda la libertad de implementar nuevas innovaciones de red. Con tecnología de silicio TRIO, la familia MX es altamente escalable desde los 3Tbps en 5U, hasta un rendimiento de 12 Tbps en 16 slots.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

Cisco Catalyst 9300L Series Switches (C9300L-24T|P-4G, C9300L-48T|P|PF-4G, C9300L-24T|P|UXG-4X, C9300L-48T|P|PF|UXG-4X, C9300L-24UXG-2Q, C9300L-48UXG-2Q)

Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	14/11/2023
Revisión de Validez	30/04/2026


**Descripción**

Los Cisco Catalyst 9300y 9300L son switches de red que ofrecen una alta densidad puertos Ethernet por módulo, incluyendo opciones de PoE+. Están diseñados con un potente procesador y ofrecen servicios de red avanzados para empresas que necesitan una red segura y escalable. Los Cisco Catalyst 9300L, la variante compacta de la serie 9300, ideales para pequeñas y medianas empresas.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.

INFORMACIÓN IMPORTANTE

Virtual Services Platform (VSP) Series Switches (VSP4900, VSP7400, VSP8400 y XA-1400)

Versión	8.3
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/09/2025

**Descripción**

Familia de switches y routers WAN que soportan tecnología Fabric. Mediante esta tecnología, basada en los estándares IEEE 802.1aq e IETF RFC 6329, se permite la creación de redes virtualizadas que automatizan el provisionamiento extremo a extremo de servicios de red, eliminando el riesgo de bucles y utilizando un único protocolo. Se soportan virtualizaciones de Nivel 2, Nivel 3 y routing de IP Multicast. Los equipos ofrecen una variedad de interfaces, desde 1 Gbps hasta 100 Gbps.

Observaciones

CCN-STIC-1451 Procedimiento de empleo seguro Extreme Networks Virtual Services Platform (VSP) Series Switches

Cisco Catalyst 9500 Series Switches (C9500-12Q|24Q|40X|16X|32C|32QC|24Y4C|48Y4C) con los siguientes módulos de red (C9500-NM-8X y C9500-NM-2Q)

Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	13/11/2023
Revisión de Validez	30/04/2026

**Descripción**

Los Cisco Catalyst 9400 9500 y 9600 son equipos de red de alto rendimiento. Ofrecen alta densidad de puertos Ethernet por módulo, con opciones de 10 Gbps, 25 Gbps y 40 Gbps. Están equipados con un procesador que proporciona una alta capacidad de procesamiento y seguridad avanzada.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9200 Series Switches (C9200-24T, C9200-48T, C9200-24P, C9200-48P, C9200-24PB, C9200-48PB, C9200-48PL, C9200-24PXG, C9200-48PXG) con los módulos de red (C9200-NM-4G|4X|2Y|2Q)

Versión IOS-XE 17.9 (con fix 17.9.a)

Fabricante Cisco Systems

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 14/11/2023

Revisión de Validez 30/04/2026

Descripción

Los equipos Cisco Catalyst 9200 y 9200L son switches de alto rendimiento y seguridad reforzada, ideales para empresas que requieren soluciones de red seguras y escalables. Con modelos que varían desde 24 hasta 48 puertos, proporciona una gran flexibilidad para adaptarse a cualquier tamaño de red. Ofrecen gestión avanzada y detección de amenazas mejorada.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.



Cisco Catalyst 9400 Series Switches (C9404R, C9407R, C9410R, C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y, C9400-LC-24S|48S|24XS|48P|48T|48U|48UX|48H)

Versión IOS-XE 17.9 (con fix 17.9.4a)

Fabricante Cisco Systems

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 13/11/2023

Revisión de Validez 30/04/2026

Descripción

Los Cisco Catalyst 9400 9500 y 9600 son equipos de red de alto rendimiento. Ofrecen alta densidad de puertos Ethernet por módulo, con opciones de 10 Gbps, 25 Gbps y 40 Gbps. Están equipados con un procesador que proporciona una alta capacidad de procesamiento y seguridad avanzada.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.



INFORMACIÓN IMPORTANTE

Switches EXOS: x440-G2, x460-G2, x465, x435, x695, 5520, 5420

Versión	EXOS 31.3.100
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	31/05/2025

**Descripción**

Familia de conmutadores apilables de alto rendimiento, que proporcionan conectividad gigabit, multigigabit, 10G, 25G, 40G y 100G. Los equipos pueden posicionarse tanto en el acceso como en la agregación en el núcleo, soportando protocolos de routing avanzado (BGP, MPLS, VXLAN, etc). También proporciona soluciones de implementación de Fabric

Observaciones

CCN-STIC-1446 PES Switches EXoS

EX4650-48Y, QFX5120-32C, QFX5210-64C, QFX5120- 48T, QFX5120-48Y, QFX5200-32C y QFX5200-48Y

Versión	Junos OS 22.3R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2024
Revisión de Validez	31/01/2025

**Descripción**

Las familias QFX5k, en sus diferentes variantes, son dispositivos de red seguros con alta densidad de puertos 1GbE, 10GbE, 25GbE y 100GbE. Estas plataformas de conmutación para el centro de datos funcionan con el software Junos OS, que es un sistema operativo especialmente diseñado para este tipo de dispositivos. Junos OS proporciona funciones de gestión, control y monitorización, así como toda la provisión de cambios en los dispositivos.

Estos switches para centros de datos son dispositivos de red que soportan la definición, y cumplimiento, de políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión segura.

Como switch de nivel 2 en la capa OSI, realiza el análisis de paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario.

Como switch de nivel 3 en la capa OSI, admite el enrutamiento del tráfico, basado en tablas, identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar el camino más adecuado para cada paquete.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Alcatel-Lucent Enterprise OmniSwitch Serie 6360 (OS6360-10, OS6360-P10, OS6360-24, OS6360-P24, OS6360-PH24, OS6360-P24X, OS6360-48, OS6360-P48, OS6360-P48X, OS6360-PH48)

Versión AOS 8.9.R01

Fabricante Alcatel-Lucent Enterprise

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/05/2022

Revisión de Validez 28/02/2026

Descripción

OS6360: Familia de conmutadores L2+ apilables con puertos 1G y enlaces 1G/10G. Diseñados como equipos de acceso en redes convergentes de alta capacidad.

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS



Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches

Versión IOS-XE 17.3 (con fix 17.3.8a)

Fabricante Cisco Systems

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/11/2022

Revisión de Validez 31/03/2025

Descripción

La familia de switches industriales Catalyst de Cisco están basados en una plataforma de switching y routing construida a propósito con capacidades de filtro para capa 2 y 3 de los niveles OSI.

Observaciones

CCN-STIC-1450 Procedimiento de empleo Seguro de Catalyst 9000 y Catalyst IE3000



INFORMACIÓN IMPORTANTE

Cisco Catalyst 9200 Series Switches (C9200-24T, C9200-48T, C9200-24P, C9200-48P, C9200-24PB, C9200-48PB, C9200-48PL, C9200-24PXG, C9200-48PXG) con los módulos de red (C9200-NM-4G, C9200-NM-4X, C9200-NM)

Versión	IOS-XE 17.6.6a
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

Descripción

Cisco Catalyst 9200 Series Switches

Observaciones

CCN-STIC-1458 Procedimiento de Empleo Seguro Routers y Switches IOS-XE 17.X La versión inicial cualificada fue la 17.6 pero tras la publicación de la vulnerabilidad pública [CVE-2023-20198], CISCO ha publicado una nueva versión con el fix (17.6.6a).



Cisco Catalyst 9200L Series Switches (C9200L-24P-4G|4X, C9200L-24T-4G|4X, C9200L-48P-4G|4X, C9200L-48T-4G|4X, C9200L-48PL-4G|4X, C9200L-24|48PXG-2Yy C9200L-24|48PXG-4X)

Versión	IOS-XE 17.6.6a
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/06/2025

Descripción

Series Cisco Catalyst 9200L.

Observaciones

CCN-STIC-1450 Procedimiento de empleo Seguro de Catalyst 9000 y Catalyst IE3000 La versión inicial cualificada fue la 17.6 pero tras la publicación de la vulnerabilidad pública [CVE-2023-20198], CISCO ha publicado una nueva versión con el fix (17.6.6a).



INFORMACIÓN IMPORTANTE

Cisco Catalyst 9300 Series Switches (C9300-24T|P|U|UX|S|UB|UXB|H y C9300-48T|P|U|UXM|UN|S|UB|H) con los siguientes módulos de red (C9300-NM-4G, C9300-NM-8X, C9300-NM-2Q, C9300-NM-4M, C9300-NM-2Y)

Versión IOS-XE 17.6.6a

Fabricante Cisco Systems

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/02/2023

Revisión de Validez 31/07/2025

Descripción

Cisco Catalyst 9300 Series Switches

Observaciones

CCN-STIC-1458 Procedimiento de Empleo Seguro CISCO Routers y Switches IOS-XE 17.X La versión inicial cualificada fue la 17.6 pero tras la publicación de la vulnerabilidad pública [CVE-2023-20198], CISCO ha publicado una nueva versión con el fix (17.6.6a).



Cisco Catalyst 9300L Series Switches (C9300L-24T|P-4G, C9300L-48T|P-4G, C9300L-24T|P-4X, C9300L-48T|P-4X, C9300L-48PF-4G|4X, C9300L-24UXG-4X|2Q, C9300L-48UXG-4X|2Q)

Versión IOS-XE 17.6.6a

Fabricante Cisco Systems

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/02/2023

Revisión de Validez 31/07/2025

Descripción

Cisco Catalyst 9300L Series Switches

Observaciones

CCN-STIC-1458 Procedimiento de Empleo Seguro CISCO Routers y Switches IOS-XE 17.X La versión inicial cualificada fue la 17.6 pero tras la publicación de la vulnerabilidad pública [CVE-2023-20198], CISCO ha publicado una nueva versión con el fix (17.6.6a).



INFORMACIÓN IMPORTANTE

Cisco Catalyst 9400 Series Switches (C9404R, C9407R, C9410R, C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y, C9400-LC-24S|48S|24XS|48P|48T|48U|48UX|48H)

Versión	IOS-XE 17.6.6a
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

Descripción

Cisco Catalyst 9400 Series Switches

Observaciones

CCN-STIC-1458 Procedimiento de Empleo Seguro CISCO Routers y Switches IOS-XE 17.X La versión inicial cualificada fue la 17.6 pero tras la publicación de la vulnerabilidad pública [CVE-2023-20198], CISCO ha publicado una nueva versión con el fix (17.6.6a).



Cisco Catalyst 9600 Series Switches (C9606R, C9600-SUP-1 y C9600-LC-24C|48YL|48TX|24S)

Versión	IOS-XE 17.6.6a
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/06/2025

Descripción

Cisco Catalyst 9600 Series Switches

Observaciones

CCN-STIC-1450 Procedimiento de empleo Seguro de Catalyst 9000 y Catalyst IE3000. La versión inicial cualificada fue la 17.6 pero tras la publicación de la vulnerabilidad pública [CVE-2023-20198], CISCO ha publicado una nueva versión con el fix (17.6.6a).

**INFORMACIÓN IMPORTANTE**

H3C S10500 Series, S7500 Series, S6500 Series, S5100 Series, S5500 Series, S12500 Series, S9800 Series and S6800 Series

Versión H3C Comware Software 7.1.070**Fabricante** New H3C Technologies Co., Ltd**Familia** Switches**Tipo** Producto**Categoría ENS** ALTA**Fecha Inclusión** 01/11/2023**Revisión de Validez** 30/04/2026**Descripción**

Los switches series de H3C son dispositivos de red diseñados para entornos empresariales, gubernamentales, educativos, financieros o industriales que ofrecen una variedad de funciones para garantizar conectividad eficiente y confiable. Los switches series de H3C proporcionan protocolos de seguridad estandarizados para la gestión de la configuración.

Entre otras capacidades, los dispositivos de switch de H3C incluyen una diversidad de puertos, gestión de energía eficiente, calidad de servicio (QoS) para priorizar el tráfico crítico, VLAN para segmentación de red, medidas de seguridad avanzadas como control de acceso y autenticación, opciones de apilamiento para aumentar la capacidad, herramientas de gestión remota y supervisión, compatibilidad con IPv6 y características como el puerto espejo para facilitar la monitorización y el análisis de la red.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C



Huawei Cloud Engine 6800 (6881-48T6CQ)

Versión V200R020C00SPC600 Patch V200R020SPH100T**Fabricante** Huawei Technologies España**Familia** Switches**Tipo** Producto**Categoría ENS** ALTA**Fecha Inclusión** 01/02/2022**Revisión de Validez** 31/08/2024**Descripción**

Es un switch que proporciona servicios estables, fiables y de alto rendimiento en capa 2 y capa 3. Estos switches están diseñados para centros de datos y redes de campus de alta gama. Proporcionan alto rendimiento, interfaces de alta densidad y baja latencia. Tienen un diseño hardware avanzado que suministra puertos de alta densidad mientras usa la misma plataforma software Huawei VRP.

Observaciones

CCN-STIC 1424 Procedimiento de Empleo Seguro Huawei CE Series Switches

**INFORMACIÓN IMPORTANTE**

Cisco Nexus 3200 Series Switches (3232C, 3264C-E)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 3500 Series Switches (3524-X/XL, 3548-X/XL)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9

**INFORMACIÓN IMPORTANTE**

Cisco Nexus 3600 Series Switches (36180YC-R, 3636C-R)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 3400 Series Switches (34180-YC, 3464C, 3432D-S, 3408-S)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9

**INFORMACIÓN IMPORTANTE**

Cisco Catalyst 9400X/9600X (C9404R, C9407R, C9410R, C9400X-SUP-2, C9400X-SUP-2XL, C9400-LC-48HX, C9400-LC-48XS, C9606R, C9600X-SUP2, C9600-LC-40YL4CD, C9600X-LC-32CD)

Versión	IOS-XE 17.9
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2024
Revisión de Validez	31/07/2026



Descripción

Los Cisco Catalyst 9400X/9600X son switches de red que ofrecen una alta densidad puertos Ethernet por módulo, incluyendo opciones de PoE+. Están diseñados con un potente procesador y ofrecen servicios de red avanzados para empresas que necesitan una red segura y escalable. Son equipos de red de alto rendimiento. Ofrecen alta densidad de puertos Ethernet por módulo, con opciones de 10 Gbps, 25 Gbps y 40 Gbps. Están equipados con un procesador que proporciona una alta capacidad de procesamiento y seguridad avanzada.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.

Cisco Catalyst 9300 Series Switches (C9300-24T|P|U|AUX|S|H, C9300-48T|P|U|UXM|UN|S|H, C9300D-24UB|UXB, C9300D-48UB) con los siguientes módulos de red (C9300-NM-4G|8X|2Q|4M|2Y)

Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/11/2023
Revisión de Validez	30/04/2026



Descripción

Los Cisco Catalyst 9300y 9300L son switches de red que ofrecen una alta densidad puertos Ethernet por módulo, incluyendo opciones de PoE+. Están diseñados con un potente procesador y ofrecen servicios de red avanzados para empresas que necesitan una red segura y escalable. Los Cisco Catalyst 9300L, la variante compacta de la serie 9300, ideales para pequeñas y medianas empresas.

Observaciones

CCN-STIC-1458 Procedimiento de empleo seguro Routers y Switches IOS-XE 17.X.

INFORMACIÓN IMPORTANTE

Huawei CE Series Switches (CE6820H-48S6CQ , CE6860-HAM, CE6860-SAN, CE6863H-48S6CQ, CE6866-48S8CQ-P, CE6881H-48S6CQ, CE6881H-48T6CQ, CE8850-HAM, CE8850-SAN, CE8851-32CQ8DQ-P, CE16804, CE16808 y CE16816)

Versión	V300R022C00SPC200
Fabricante	Huawei Technologies Co., Ltd.
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/03/2026



Descripción

Es un switch que proporciona servicios estables, fiables y de alto rendimiento en capa 2 y capa 3. Estos switches están diseñados para centros de datos y redes de campus de alta gama. Proporcionan alto rendimiento, interfaces de alta densidad y baja latencia. Tienen un diseño hardware avanzado que suministra puertos de alta densidad mientras usa la misma plataforma software Huawei VRP.

Observaciones

CCN-STIC 1424 Procedimiento de Empleo Seguro Huawei CE Series Switches

Cisco Nexus 9300 Series Switches (93108TC-EX, 93108TC-FX, 9348GC-FXP, 93216TC-FX2, 93180LC-EX, 93180YC-EX, 93180YC-FX, 93240YC-FX2, 93360YC-FX2, 9364C, 9332C, 9336C-FX2, 9364C-GX, 9316D-GX, 93600CD-GX)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	04/10/2025



Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9

INFORMACIÓN IMPORTANTE

Cisco Nexus 9500 Series Switches (9504, 9508, 9516, Supervisor 9500-Sup-A , Supervisor 9500-Sup-A +, Supervisor 9500-Sup-B , Supervisor 9500-Sup-B +, System Controller N9k-SC-A)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	04/10/2025



Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9

Atlas-840, M10-Smart Series, M2 Series, 4GePlus Series, Teldat-5Ge Series, 5Ge-Rail Series, Connect-4GePlus Series, Connect-5Ge Series, Connect-FW Series

Versión	11.02.02.85.03
Fabricante	TEL DAT, S.A.
Familia	Switches
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	20/08/2024
Revisión de Validez	31/01/2025



Descripción

Familia de routers corporativos para los servicios de comunicaciones en redes físicas o en la nube. Disponen, según modelos, de múltiples tecnologías de conexión(WAN, WWAN, LAN, WLAN) y ofrecen una solución eficiente en todo tipo de escenarios, garantizando los SLAs que los usuarios requieren. Estos equipos se integran dentro de los servicios digitales de las empresas facilitando su despliegue, elevando la seguridad e integridad tanto de los datos como del hardware, y optimizando las aplicaciones de los usuarios.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Alcatel-Lucent Enterprise OmniSwitch Serie 6560 (OS6560-P24Z8, OS6560-P24Z24, OS6560-P48Z16, OS6560-24Z8, OS6560-24Z24, OS6560-24X4, OS6560-P24X4, OS6560-48X4, OS6560-P48X4 y OS6560-X10)

Versión AOS 8.9.R01

Fabricante Alcatel-Lucent Enterprise

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/04/2021

Revisión de Validez 28/02/2026

Descripción

Familia de conmutadores L3 compactos apilables con alta densidad de puertos 1GE, Multigigabit ethernet 1/2.5 GigE y enlaces 10GE, diseñados como equipos de acceso en redes convergentes de alta capacidad. <https://www.al-enterprise.com/es-es/productos/conmutadores>

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS



Huawei S Series Ethernet Switches S5731 (S5731-H24T4XC, S5731-H48T4XC, S5731-H24P4XC, S5731-H48P4XC, S5731-S24T4X, S5731-S24P4X, S5731-S48T4X y S5731-S48P4X)

Versión V200R020C00SPC300 y V200R021C00SPC100

Fabricante Huawei Technologies España

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/03/2021

Revisión de Validez 31/08/2024

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet



INFORMACIÓN IMPORTANTE

EX4400-24T|24P|24MP, EX4400-48T|48P|48F|48MP

Versión	Junos OS 22.3R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/05/2024
Revisión de Validez	31/01/2025

JUNIPER
NETWORKS

**Descripción**

La familia de switches EX4400, en sus diferentes variantes, son dispositivos de red seguros con alta densidad de puertos 10/100/1000Base-T, 100/1000/2500/5000/10000Base-T, así como uplinks 1/10/25GbE o 40/100GbE o variantes con todos sus puertos en fibra. Todas las plataformas EX4400 funcionan con el software Junos OS, que es un sistema operativo especialmente diseñado para este tipo de dispositivos. Junos OS proporciona funciones de gestión, control y monitorización, así como toda la provisión de cambios en los dispositivos. Los switches EX4400 son dispositivos de red que soportan la definición, y cumplimiento, de políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión segura. Como switch de nivel 2 en la capa OSI, realiza el análisis de paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario. Como switch de nivel 3 en la capa OSI, admite el enrutamiento del tráfico, basado en tablas, identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar el camino más adecuado para cada paquete.

Observaciones

Procedimientos de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

EX4100-24P|24T|24MP, EX4100-48P|48T|48MP

Versión	Junos OS 22.4R2
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/04/2024
Revisión de Validez	31/01/2025

JUNIPER
NETWORKS

**Descripción**

La familia de switches EX4100, en sus diferentes variantes, son dispositivos de red seguros con alta densidad de puertos 10/100/1000Base-T o multigigabit 100/1000/2500/5000/10000Base-T así como puertos de uplinks 1/10/25GbE. Todas las plataformas EX4100 funcionan con el software Junos OS, que es un sistema operativo especialmente diseñado para este tipo de dispositivos de red. Junos OS proporciona funciones de gestión, control y monitorización, así como toda la provisión de cambios en los dispositivos. Los switches EX4100 son dispositivos de red que soportan la definición, y cumplimiento, de políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad en el tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión segura. Como switch de nivel 2 en la capa OSI, realiza el análisis de paquetes entrantes, reenvía dichos paquetes en función de la información que contienen en su cabecera Ethernet, haciéndolos llegar así a su destinatario. Como switch de nivel 3 en la capa OSI, permite el enrutamiento del tráfico, basado en tablas, identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar el camino más adecuado para cada paquete. La familia EX4100 soporta también el uso de tecnologías de overlay como es el caso de EVPN-VXLAN que permiten la microsegmentación usando group-based policies (GBP), además de soportar MACsec AES-256 y Power over Ethernet.

Observaciones

Procedimiento de Empleo Seguro Pendiente de Publicación

INFORMACIÓN IMPORTANTE

Huawei S Series Switches (S3710, S5732, S5735I, S5735, S5755, S6730, S6750, S16700-4, S16700-8, S8700-10, S8700-4 y S8700-6)	
Versión	V600R023C10SPC500
Fabricante	Huawei Technologies Co., Ltd.
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2024
Revisión de Validez	31/12/2024
Descripción	Los modelos cualificados son: S3710-H24T4S-A, S3710-H24P4S-A, S3710-H48T4S-A, S3710-H48LP4S-A, S5732-H24S4X6QZ-TV2, S5732-H24S4X6QZ-V2, S5732-H24UM4Y2CZ-TV2, S5732-H24UM4Y2CZ-V2, S5732-H44S4X6QZ-TV2, S5732-H44S4X6QZ-V2, S5732-H48UM4Y2CZ-TV2, S5732-H48UM4Y2CZ-V2, S5735-S24T4XE-V2, S5735-S24P4XE-V2, S5735-S48T4XE-V2, S5735-S48P4XE-V2, S5735-S24U4XE-V2, S5735-S48U4XE-V2, S5735I-S24T4XE-V2, S5735I-S24U4XE-V2, S5735I-S8T4SN-V2, S5735I-S8T4XN-V2, S5735I-S8U4XN-V2, S5735-L8T4X-QA-V2, S5735-L8T4S-A-V2, S5735-L10T4X-A-V2, S5735-L8P4X-QA-V2, S5735-L8P4S-A-V2, S5735-L8P2T4X-A-V2, S5735-L16T4X-QA-V2, S5735-L16T4S-A-V2, S5735-L24T4X-QA-V2, S5735-L24T4S-A-V2, S5735-L24T4XE-A-V2, S5735-L24T4XE-D-V2, S5735-L24P4S-A-V2, S5735-L24P4XE-A-V2, S5735-L48T4S-A-V2, S5735-L48T4XE-A-V2, S5735-L48T4XE-D-V2, S5735-L48LP4S-A-V2, S5735-L48LP4XE-A-V2, S5735-L48P4XE-A-V2, S5735I-L8P4X-A-V2, S5735I-L10T4X-A-V2, S5755-H48T4Y2CZ, S5755-H48P4Y2CZ, S5755-H48U4Y2CZ, S5755-H24T4Y2CZ, S5755-H24P4Y2CZ, S5755-H24U4Y2CZ, S5755-H24UTM4X4Y2C, S5755-H24UTM4X4Y2C-T, S5755-H48UTM4X4Y2C, S5755-H48UTM4X4Y2C-T, S5755-H24N4Y-A, S5755-H48N4Y-A, S5755-H24UN4Y2CZ, S5755-H48UN4Y2CZ, S5735-L14P2S-QA-V2, S5735-L14P2S-TQA-V2, S5735-L16LP2X-QA-V2, S5735-L16P2UM2X-QA-V2, S5735-L16LP2UM2X-QA-V2, S5735-L24ST4XE-A-V2, S5735-S24HS4XE-V2, S5735-S24ST4XE-V2, S5735-L48S4XE-A-V2, S5735-L48S4X-A-V2, S5735-S48HS4XE-V2, S5735-S48S4XE-V2, S5732-H48XUM2CC, S5735I-H24U8S4XE-QA-V2, S5735I-S24T8S4XE-QA-V2, S5735I-S16T8S4XE-QD-V2, S5735-S48PN4XE-V2, S5735-S24PN4XE-V2, S5735-L48LPN4XE-A-V2, S5735-L24PN4XE-A-V2, S5735-L24LU8S4XE-QA-V2, S5735-S48T4XE-C-V2, S5735-S24T4XE-C-V2, S6730-H24X6C-TV2, S6730-H24X6C-V2, S6730-H28X6CZ-TV2, S6730-H28X6CZ-V2, S6730-H48X6C-TV2, S6730-H48X6C-V2, S6730-H48X6CZ-TV2, S6730-H48X6CZ-V2, S6730-H48Y6C-TV2, S6730-H48Y6C-V2, S6750-H36C, S6750-H48Y8C, S6730-S48X6Q. Observaciones CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet



ACX5448, ACX5448-M y ACX5448-D

Versión	Junos OS 22.3R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/05/2024
Revisión de Validez	31/01/2025

JUNIPER
NETWORKS

**Descripción**

La línea Juniper Networks ACX5448 surge como respuesta a un cambio en las arquitecturas de redes metropolitanas donde las capas de acceso y agregación están extendiendo la inteligencia operativa desde el extremo del proveedor de servicios hasta la red de acceso. Está basada en la simplificación de la arquitectura y en la reducción de costos, la línea ACX5448 brinda a los proveedores de servicios y empresas la capacidad de adoptar una solución metro universal.

Asimismo, proporciona alta capacidad, escalabilidad y una capa de transporte óptico de paquetes, al tiempo que ofrece un rendimiento líder en la industria con una amplia gama de densidades de puertos y tipos de interfaz. La serie ACX presenta el liderazgo IP/MPLS de Juniper desde el core y el perímetro de la red hasta las capas de acceso. La serie ACX admite un amplio conjunto de funcionalidades L2, L3 e IP/MPLS para permitir redes MPLS transparentes a gran escala con operaciones y aprovisionamiento de servicios simplificados manteniendo simplicidad en la red.

ACX5448: El ACX5448 tiene 48 puertos 1GbE/10GbE y 4 puertos 40GbE/100GbE, así como soporte de tecnología PON.

ACX5448-M: El ACX5448-M tiene 44 puertos 1GbE/10GbE y 6 puertos 40GbE/100GbE, así como capacidades de seguridad avanzadas tales como MACsec en todos los puertos 1GbE/10GbE y soporte de tecnología PON.

ACX5448-D: El ACX5448-M tiene 36 puertos 1GbE/10GbE, 2 puertos 40GbE/100GbE y 2 puertos 100G/200G DWDM para ópticas CFP2-DCO y soporte de tecnología PON.

Observaciones

CCN-STIC-1445 PES Router_Juniper_ACX5448-M_JunOS 20.3R1 en proceso de actualización.

INFORMACIÓN IMPORTANTE

Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches IE-9310-26S2C-E | A, IE-9320-26S2C-E | A, IE-9320-22S2C4X-E | A, IE-9320-24P4S-E | A, IE-9320-24T | P4X-E | A, IE-9320-16P8U4X-E | A

Versión	IOS-XE 17.9
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2024
Revisión de Validez	30/06/2026



Descripción

Los Catalyst Industrial Ethernet 9300 Rugged Series Switches son equipos diseñados para entornos industriales exigentes. Este switch es resistente y duradero, capaz de soportar condiciones extremas. Ofrece una conectividad confiable y segura para dispositivos industriales, como cámaras de vigilancia, sensores y controladores. Tiene múltiples puertos Ethernet que permiten la conexión de varios dispositivos y garantizan una comunicación fluida en la red.

Además, son equipos fáciles de configurar y administrar, lo que lo hace adecuado para entornos industriales donde se requiere una infraestructura de red robusta y confiable.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Alcatel-Lucent Enterprise OmniSwitch Serie 6900 (OS6900-X20, OS6900-X40, OS6900-T20, OS6900-T40, OS6900-X72, OS6900-Q32, OS6900-V72, OS6900-C32, OS6900-C32E, OS6900-X48C6, OS6900-T48C6, OS6900-X48C4E, OS6900-V48C8, OS6900-X24C2, OS6900-T24C2)

Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026



Descripción

OS6900: Familia de conmutadores L3+ compactos apilables de alta densidad 10GE, 25GE, 40GE y 100GE. Diseñadas para que sean flexibles. Pueden instalarse como conmutadores convergentes situados en la parte superior del bastidor (TOR) o tipo spine para entornos de Data Centers y también como dispositivos de agregación y de núcleo en una red de campus. <https://www.al-enterprise.com/es-es/productos/conmutadores>

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

INFORMACIÓN IMPORTANTE

Alcatel-Lucent Enterprise OmniSwitch Serie 6865 (OS6865-P16X, OS6865-U12X y OS6865-U28X)

Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026

**Descripción**

OS6865: Familia de conmutadores L3+ con puertos 1G y 10G, preparados para entorno industrial o redes de misión crítica como transportes y utilities, con amplio rango de temperaturas de funcionamiento (-40°C a +75°C). <https://www.al-enterprise.com/es-es/productos/conmutadores>

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6860 (OS6860E-24, OS6860E-P24, OS6860E-48, OS6860E-P48, OS6860E-U28, OS6860E-P24Z8, TA6860E-P48, OS6860N-U28, OS6860N-P48Z, OS6860N-P48M, OS6860N-P24M, OS6860N-P24Z)

Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026

**Descripción**

OS6860: Familia de conmutadores L3+ compactos apilables con alta densidad de puertos 1GE, Multigigabit ethernet 1/2.5/5/10 GigE y enlaces 10GE, 25GE y 100GE, diseñadas para redes convergentes. Con funciones de Acceso unificado avanzadas que permiten la creación de redes orientadas a las aplicaciones. Puede supervisar y controlar las aplicaciones de la red mediante capacidades de Deep Packet Inspection (DPI). <https://www.al-enterprise.com/es-es/productos/conmutadores>

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

INFORMACIÓN IMPORTANTE

Alcatel-Lucent Enterprise OmniSwitch Serie 9900 (OS9907-CFM, OS99-CMM, OS99-XNI-48, OS99-XNI-U48, OS99-GNI-48, OS99-GNI-P48, OS99-CNI-U8, OS99-XNI-P24Z8, OS99-XNI-P48Z16, OS99-XNI-U12Q, OS99-XNI-U24, OS99-XNI-U48, OS99-GNI-U48, y OS99-XNI-UP24Q2)

Versión AOS 8.9.R01

Fabricante Alcatel-Lucent Enterprise

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/04/2021

Revisión de Validez 28/02/2026

Descripción

OS9900: Conmutador LAN L3+ con chasis modular de alta capacidad de interfaces 1GE, 10GE y 100GE para conmutación segura y con alta disponibilidad en el núcleo de las redes empresariales, campus y redes Metro Ethernet. <https://www.al-enterprise.com/es-es/productos/conmutadores>

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS



Alcatel-Lucent Enterprise OmniSwitch Serie 6465 (OS6465-P6, TA6465-P6, OS6465-P12, TA6465-P12, OS6465-P28, TA6465-P28, OS6465T-P12 y OS6465T-12)

Versión AOS 8.9.R01

Fabricante Alcatel-Lucent Enterprise

Familia Switches

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/04/2021

Revisión de Validez 28/02/2026

Descripción

OS6465: Familia de conmutadores L2+ con puertos 1G y 10G, preparados para entorno industrial, con amplio rango de temperaturas de funcionamiento (-40°C a +75°C). Diseñados como equipos de acceso en redes de tipo industrial, transportes o utilities. <https://www.al-enterprise.com/es-es/productos/conmutadores>

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS



INFORMACIÓN IMPORTANTE

7.5.3 CORTAFUEGOS

ASA 5500 Series (5508-X y 5516-X)

Versión	FTD 7.0 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	30/04/2026



Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

SRX1600, SRX2300, SRX4300

Versión	Juno OS 19.2R1
Fabricante	Juniper Networks
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	24/05/2024
Revisión de Validez	31/01/2025

JUNIPER
NETWORKS

**Descripción**

La familia de firewall mid-range de Juniper Networks®, que incluye los modelos SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300 y SRX4600, protege las redes de centros de datos y campus de misión crítica para empresas, proveedores de servicios móviles y proveedores de servicios en la nube. Está diseñado para arquitecturas de servicios de seguridad de alto rendimiento y protege los activos de TI corporativos críticos como un firewall de próxima generación (NGFW). Además, actúa como un punto de cumplimiento para las soluciones de seguridad basadas en la nube y proporciona visibilidad y control de aplicaciones para mejorar la experiencia del usuario y la aplicación.

Al integrar networking y seguridad en una sola plataforma, esta familia ofrece múltiples interfaces de alta velocidad, prevención de ataques, protección avanzada contra amenazas y autenticación, junto con capacidades de IPsec de alto rendimiento. También ofrece alta escalabilidad, alta disponibilidad, protección robusta, visibilidad de aplicaciones, identificación de usuarios e inspección profunda de contenido para proporcionar un control sin igual sobre la infraestructura de seguridad.

La familia SRX mid-range también actúa como un punto de cumplimiento central, aprovechando la automatización para proteger a los usuarios en un entorno de red de múltiples proveedores. Asimismo, ofrece SD-WAN totalmente automatizado tanto para empresas como para proveedores de servicios. Debido a su alto rendimiento y escala, los miembros de esta familia pueden actuar como concentrador de VPN y finalizar las conexiones VPN en varias topologías SD-WAN.

Observaciones

CCN-STIC-1442 PES Cortafuegos Juniper SRX JunOS 19.2R1

INFORMACIÓN IMPORTANTE

CloudGuard Network (VMware ESXi/NSX)

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

**Descripción**

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

SonicWall TZ Serie (300P, 350, 350W, 600P)

Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	28/02/2025

**Descripción**

La serie TZ de SonicWall ofrece seguridad y rendimiento de entorno Enterprise orientado a pequeñas compañías. Enfocado a entornos departamentales o PYMES de entre 5 y 100 usuarios (aprox), incorpora funciones de prevención de intrusiones, antimalware, filtrado de contenidos/URL y control de aplicaciones a través de redes y entornos inalámbricos. Proporciona inspección profunda de paquetes (DPI), SD-WAN y despliegue zero-touch. Opciones de puertos PoE y wifi 802.11ac. Más info en: <https://www.sonicwall.com/es-mx/products/firewalls/entry-level>

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

Sonicwall TZ Serie (300, 300W, 400, 400W, 500, 500W, 600), NSa (2650, 3600, 3650, 4600, 4650, 5600, 5650, 6600, 6650, 9250, 9450 y 9650), SM (9200, 9400, 9600 y 9800)

Versión 6.5.4.4-44n-federal-12n

Fabricante SONICWALL

SONICWALL®

Familia Cortafuegos

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/08/2021

Revisión de Validez 28/02/2025



Descripción

La serie TZ de SonicWall ofrece seguridad y rendimiento de entorno Enterprise orientado a pequeñas compañías. Enfocado a entornos departamentales o PYMES de entre 5 y 100 usuarios (aprox), incorpora funciones de prevención de intrusiones, antimalware, filtrado de contenidos/URL y control de aplicaciones a través de redes y entornos inalámbricos. Proporciona inspección profunda de paquetes (DPI), SD-WAN y despliegue zero-touch.

La serie SOHO son una solución adecuada para oficinas pequeñas y domésticas, así como para entornos distribuidos en ubicaciones remotas. Despliegan funcionalidades para construir Secure SD-WAN y conectividad WIFI (opcional). El SOHO 250 proporciona un 50% más de rendimiento sobre su antecesor SOHO, así como acceso a los sandboxes avanzados Capture ATP, con lo que se mejora la seguridad en prevención y detección de malware desconocido en un entorno remoto.

La serie NSa están indicados para compañías medianas / grandes, empresas deslocalizadas geográficamente y datacenters, consolidando tecnologías automatizadas de prevención y detección de amenazas como la inspección de memoria profunda en tiempo real (RTDMI). Desarrollados sobre una arquitectura de hardware de múltiples núcleos con interfaces 10-GbE y 2.5-GbE, la serie NSa cuenta con capacidades basadas en la nube y en el equipo, como descifrado e inspección TLS/SSL, application intelligence y control, SD-WAN segura, visualización en tiempo real y administración de WLAN.

La serie SM está dedicada para grandes empresas, centros de datos, carriers y proveedores de servicios con necesidades multi-gigabit. Dirigido a compañías de entre 1000 y más de 50.000 usuarios (aprox.), realiza detección y prevención de amenazas mediante la combinación de la protección basada en appliances con la inteligencia de la nube en una plataforma de alto desempeño y consolida tecnologías de seguridad que brindan protección contra amenazas a millones de conexiones sin ralentizar el desempeño.

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

Palo Alto Networks PA-220R, PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.0

Versión PAN-OS 11.0

Fabricante Palo Alto Networks

Familia Cortafuegos

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 10/06/2024

Revisión de Validez 30/11/2024

Descripción



Palo Alto Networks ofrece soluciones robustas para proteger redes empresariales en entornos digitales modernos. Sus Firewalls de Nueva Generación (NGFW) de capa 7 destacan por su adaptabilidad y seguridad avanzada, empleando machine learning y WildFire para detectar y responder rápidamente a amenazas, ya sean conocidas o desconocidas. Aplican políticas basadas en identidades y usuarios para asegurar accesos seguros, gestionadas eficientemente mediante arquitectura de inspección en un único ciclo.

En línea con la estrategia Zero Trust, los firewalls refuerzan políticas de acceso mínimo y previenen amenazas avanzadas. Ofrecen suscripciones como Advanced Threat Prevention para detener ataques de día cero, Advanced URL Filtering para protección de navegación en tiempo real, y Advanced WildFire para prevenir el 99% de amenazas de archivos. Además, complementan con DNS Security, IoT Security adaptada y Next-Generation CASB para proteger aplicaciones SaaS.

Comercializados en múltiples formatos con las mismas capacidades, como PA-Series, VM-Series, CN-Series y Cloud NGFW para AWS y Azure, además de Prisma Access para seguridad global desde la nube, todas gestionadas centralmente por Panorama o Strata Cloud Manager.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Check Point Security Gateway Serie 3000 (CPAP-SG3100, CPAP-SG3200, CPAP-SG3600, CPAP-SG3800)

Versión R.81

Fabricante Check Point Software Technologies

Familia Cortafuegos

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/02/2023

Revisión de Validez 31/07/2025

Descripción



Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Check Point Security Gateway Serie 6000 (CPAP-SG6200, CPAP-SG6400, CPAP-SG6600, CPAP-SG6700, CPAP-SG6900)

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025



Descripción

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

PA-5400 Series (PA-5410, PA-5420, PA-5430, PA-5450)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025



Descripción

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

Check Point Security Gateway serie 15000 (CPAP-SG15400, CPAP-SG15600)

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

**Descripción**

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

Forcepoint NGFW 2200 series (N2201, N2205, N2210)

Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2025

**Descripción**

Firewalls de Nueva Generación orientados a compañías u organismos de tamaño medio, de tipo appliance físico de 1RU, con capacidades IPS, SD-WAN, URL Filtering y Detección Avanzada de Malware. Dependiendo del modelo concreto de dispositivo se puede disponer de un rendimiento de 13,5 Gbps de Throughput NGFW/NGIPS, 35 millones de conexiones concurrentes y 100 contextos virtuales. Más información en: <https://www.forcepoint.com/environments/forcepoint-ngfw-appliances>

Observaciones

CCN-STIC-1409 Procedimiento de empleo seguro cortafuegos Forcepoint NGFW

INFORMACIÓN IMPORTANTE

Check Point Security Threat Emulation/Extraction (CPAP-SBTE100X-4VM, CPAP-SBTE250X-8VM, CPAP-SBTE1000X-A-28VM, CPAP-SBTE2000X)

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025



Descripción

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

Eudemon1000EN USG6510E, USG6530E, USG6525E, USG555E, USG6565E, USG6575E-B, USG6610E, USG6620E, USG6650E, USG6605E-B, USG6712E y USG6716E.

Versión	V600R007C20SPC300 + V600R007C20SPH315T
Fabricante	Huawei Technologies España
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024



Descripción

Los firewalls de nueva generación de la serie Huawei HiSecEngine están diseñados para todo tipo de empresas, instituciones y centros de datos de próxima generación. Los firewalls disponen de capacidades NGFW y se integran con otros dispositivos de seguridad para defenderse de manera proactiva contra amenazas de red, mejorar las capacidades de detección y resolver problemas de deterioro del rendimiento. Proporcionan capacidades de aceleración de procesamiento de servicios de cifrado/descifrado mejorando el rendimiento de los firewalls, la detección de seguridad y los servicios IPSec.

Observaciones

CCN-STIC-1433 PES Huawei USG 6000E Series Firewall

INFORMACIÓN IMPORTANTE

Checkpoint Security Gateway y Maestro Hyperscale Appliances (140, 154**, 156**, 175, 3600, 3800, 6200, 6400, 6600, 6700, 7000, 16000, 16200, 16600HS, 26000, 28000, 6600, 6700, 6900, 7000, 16600, 28600, 28600HS, Smart-1 525, Smart-1 660-S, Smart-1 660-M, Smart-1 6000-L, Smart-1 6000-XL, ESXi (HPE D360 G10))

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2022
Revisión de Validez	30/11/2024



Descripción

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

WatchGuard Fireware on Firebox NGFWs (T35, T40, T80, T55, M270, M370, M470, M570, M670, M4600 y M5600)

Versión	FirewareOS 12.10
Fabricante	WatchGuard Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2023
Revisión de Validez	30/05/2025



Descripción

Los equipos UTM de WatchGuard están enfocados en ofrecer la mejor seguridad para cualquier empresa y entorno corporativo distribuido. Nuestros dispositivos de seguridad de red están diseñados, desde el inicio, para enfocarse en facilitar el despliegue, el uso y la administración continua. Proporcionan protección contra ataques de malware avanzado y phishing, así como las protecciones de seguridad tradicionales: prevención de intrusiones (IPS), filtrado de URL, control de aplicaciones, antispam y antivirus, ... ofreciendo en todo momento visibilidad del entorno (productividad y seguridad) Cuentan con capacidades SD-WAN, y VPN. Están disponibles tanto en equipos físicos como virtuales. <https://www.watchguard.com/es/wgrd-products/network-security>

Observaciones

CCN-STIC-1421 Procedimiento de empleo seguro WatchGuard Fireware

INFORMACIÓN IMPORTANTE

FortiGate NGFW Appliances (FG40F, FG-60F, FWF-60F, FG-80F, FG-80F-PoE, FG-90G, FG-91G, FG-200F, FG-1100E, FG-1800F, FG-1800F-0DC, FG-2200E, FG-2600F, FG-2600F-0DC, FG-3300E, FG-3400E, FG-3400E-0DC, FG-4200F, FG-4200F-0DC, FG-4400F, FG-4400F-0DC)

Versión	FortiOS 6.4
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2024
Revisión de Validez	31/03/2026




Descripción

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

PA-5200 Series (PA-5220, PA-5250, PA-5260, PA-5280)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025




Descripción

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP. Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

Check Point Security Gateway Quantum Force 9000 (CPAP-SG9100, CPAP-SG9200, CPAP-SG9300, CPAP-SG9400, CPAP-SG9700, CPAP-SG9800)

Versión R81.00

Fabricante Check Point Software Technologies



Familia Cortafuegos

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/07/2024

Revisión de Validez 31/12/2024



Descripción

La familia Quantum Force permite una arquitectura modular de máxima seguridad con interfaces de red intercambiables de forma eficiente en appliances de 1U de espacio en rack con rendimientos en FW de hasta 185 Gbps y NGTP hasta 20 Gbps

Los equipos permiten un control granular del acceso “Zero Trust” protegiendo a los usuarios frente amenazas avanzadas con los módulos de seguridad IPS, anti-malware, antibot, Threat Emulations, DNS Security, Zero-Phising y Threat Extraction.

Para más información <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

FortiGate NGFW Appliances (FG-61E, FG-61F, FWF-61E, FWF-61F, FG-81E, FG-81E-PoE, FG-81F, FG-81F-2R, FG-81F-2R-3G4G-PoE, FG-81F-2R-PoE, FG-81F-PoE, FG-90E, FG-91E)

Versión FortiOS 6.4

Fabricante Fortinet



Familia Cortafuegos

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/04/2023

Revisión de Validez 30/09/2025



Descripción

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguad Services y su protección contra amenazas basadas en IA.

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

INFORMACIÓN IMPORTANTE

Check Point Security Gateway Quantum Force 19000 (CPAP-SG19100, CPAP-SG19200)

Versión	R81.00
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2024
Revisión de Validez	31/12/2024

**Descripción**

La familia Quantum Force permite una arquitectura modular de máxima seguridad con interfaces de red intercambiables de forma eficiente en appliances de 2U de espacio en rack con rendimientos en FW de hasta 800 Gbps y NGTP hasta 37 Gbps.

Los equipos permiten un control granular del acceso “Zero Trust” protegiendo a los usuarios frente amenazas avanzadas con los módulos de seguridad IPS, anti-malware, antibot, Threat Emulations, DNS Security, Zero-Phising y Threat Extraction.

Para más información <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Check Point Security Gateway Quantum Force 29000 (CPAP-SG29100, CPAP-SG29200)

Versión	R81.00
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2024
Revisión de Validez	31/12/2024

**Descripción**

La familia Quantum Force permite una arquitectura modular de máxima seguridad con interfaces de red intercambiables de forma eficiente en appliances de 2U de espacio en rack con rendimientos en FW de hasta 1.400Gbps (1.4Tbps) y NGTP hasta 63.5 Gbps

Los equipos permiten un control granular del acceso “Zero Trust” protegiendo a los usuarios frente amenazas avanzadas con los módulos de seguridad IPS, anti-malware, antibot, Threat Emulations, DNS Security, Zero-Phising y Threat Extraction.

Para más información <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

WatchGuard Fireware on Firebox NGFWs (T25, T45, T85, M290, M390, M590, M590, M690, M4800, M5800)

Versión	FirewareOS 12.10
Fabricante	WatchGuard Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2024
Revisión de Validez	30/05/2025



Descripción

Los equipos UTM de WatchGuard están enfocados en ofrecer la mejor seguridad para cualquier empresa y entorno corporativo distribuido. Nuestros dispositivos de seguridad de red están diseñados, desde el inicio, para enfocarse en facilitar el despliegue, el uso y la administración continua. Proporcionan protección contra ataques de malware avanzado y phishing, así como las protecciones de seguridad tradicionales: prevención de intrusiones (IPS), filtrado de URL, control de aplicaciones, antispam y antivirus, ... ofreciendo en todo momento visibilidad del entorno (productividad y seguridad) Cuentan con capacidades SD-WAN, y VPN. Están disponibles tanto en equipos físicos como virtuales. <https://www.watchguard.com/es/wgrd-products/network-security>

Observaciones

CCN-STIC-1421 Procedimiento de empleo seguro WatchGuard Fireware

INFORMACIÓN IMPORTANTE

SRX1500, SRX4100, SRX4200, SRX4600

Versión	Junos OS 19.2R1
Fabricante	Juniper Networks
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	31/12/2024

JUNIPER
NETWORKS

**Descripción**

La familia de firewall mid-range de Juniper Networks®, que incluye los modelos SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300 y SRX4600, protege las redes de centros de datos y campus de misión crítica para empresas, proveedores de servicios móviles y proveedores de servicios en la nube. Está diseñado para arquitecturas de servicios de seguridad de alto rendimiento y protege los activos de TI corporativos críticos como un firewall de próxima generación (NGFW). Además, actúa como un punto de cumplimiento para las soluciones de seguridad basadas en la nube y proporciona visibilidad y control de aplicaciones para mejorar la experiencia del usuario y la aplicación.

Al integrar networking y seguridad en una sola plataforma, esta familia ofrece múltiples interfaces de alta velocidad, prevención de ataques, protección avanzada contra amenazas y autenticación, junto con capacidades de IPsec de alto rendimiento. También ofrece alta escalabilidad, alta disponibilidad, protección robusta, visibilidad de aplicaciones, identificación de usuarios e inspección profunda de contenido para proporcionar un control sin igual sobre la infraestructura de seguridad.

La familia SRX mid-range también actúa como un punto de cumplimiento central, aprovechando la automatización para proteger a los usuarios en un entorno de red de múltiples proveedores. Asimismo, ofrece SD-WAN totalmente automatizado tanto para empresas como para proveedores de servicios. Debido a su alto rendimiento y escala, los miembros de esta familia pueden actuar como concentrador de VPN y finalizar las conexiones VPN en varias topologías SD-WAN.

Observaciones

CCN-STIC-1442 PES Cortafuegos Juniper SRX JunOS 19.2R1

INFORMACIÓN IMPORTANTE

ISA 3000 (ISA 3000-4C y ISA 3000-2C2F)

Versión	FTD 7.0 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	30/04/2026

**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

Huawei USG6000F & USG12000F Series Firewall

Versión	V600R023C10SPC100
Fabricante	Huawei Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	09/12/2024
Revisión de Validez	31/05/2025

**Descripción**

N/A

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

FortiGate NGFW VM64

Versión	FortiOS 6.4
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025

FORTINET**Descripción**

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

Next-Generation Firewall with PAN-OS PA-200 Series (PA-220, PA220R), PA-400, PA-800 Series (PA-820, PA850), PA-3200 Series (PA-3220, PA3250, PA3260), PA-5200 Series (PA-5220, PA5250, PA5260, PA5280), PA-5450, PA-7000 Series (PA-7050, PA7080), VM-Series (VM-50, VM-100, VM-300, VM-500, VM-700, VM-1000HV)

Versión	10.1
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2022
Revisión de Validez	31/03/2025

paloalto
NETWORKS**Descripción**

Firewalls de Nueva Generación orientado a grandes empresas y datacenters, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado.

Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido. Soportan hipervisores: vmware ESXi, Citrix SDX, Microsoft Hyper-V, KVM, vmware vCloud Air, Microsoft Azure y Amazon AWS.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

Cortafuegos SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC y SRX380

Versión	Junos OS 20.4R1
Fabricante	Juniper Networks
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

JUNIPER
NETWORKS

**Descripción**

La línea SRX300 de firewalls proporciona capacidades de seguridad, redes y SD-WAN de próxima generación para satisfacer las necesidades cambiantes de su red empresarial basada en la IA y habilitada para la nube. La gestión del SRX300 a través de la arquitectura en la nube Juniper Mist simplifica las operaciones de sus sucursales. Tanto si está añadiendo nuevas aplicaciones en varias ubicaciones, conectándose a la nube o esforzándose por mejorar la eficiencia operativa, el SRX300 puede ayudarle con una conectividad escalable, segura y fácil de gestionar.

El SRX300 admite funciones de firewall de nueva generación como prevención de intrusiones, visibilidad y control de aplicaciones y funciones de seguridad de contenidos que incluyen antivirus, antispam y filtrado Web mejorado. Advanced Threat Prevention proporciona una defensa integral frente a amenazas con detección dinámica de malware, fuentes de amenazas de SecIntel, Juniper Encrypted Traffic Insights y Juniper Adaptive Threat Profiling.

Observaciones

CCN-STIC-1442 PES Cortafuegos Juniper SRX

Fortigate/FortiOS

Versión	7.0
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/09/2024
Revisión de Validez	28/02/2025

FORTINET

**Descripción**

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Aruba Mobility Controller (9004, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280) y puntos de acceso.

Versión	ArubaOS 8.6
Fabricante	Aruba
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2024



Descripción

Las familias Aruba Mobility Controllers 7000's, 7200's, 9000s y las Virtual Mobility Controller (appliance virtual) junto con los puntos de acceso de las familias 500s, 300s y 200s permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Con esta versión se soporta también WPA3 y Wifi-6/802.11ax (con las familias 500s) así como WiFi-5/802.1ac y Wifi-4/802.11n. Se implementan avanzadas características de seguridad, en el control de acceso a la red, así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro. Los Puntos de Acceso en modo pueden trabajar en modo Campus (CAP) y modo Remoto (RAP), lo que permite conectar de forma segura puntos de acceso que cruzan redes ajenas como internet). Se implementan mejoras en actualizaciones de software sin pérdida de servicio. Aruba Multizona permite a un Punto de Acceso dar servicio a varias Mobility Controllers de diferentes dominios o entornos de seguridad. Los Mobility Controllers puede actuar como servidores de túneles IPSEC/SSL para el cliente Aruba VIA.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS 8.6. Controladoras y Puntos de Acceso

Aruba Mobility Controller (9004, 9012, 9240, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) y Aruba Virtual Mobility Controllers (MC-VA-50, MC-VA-250 y MC-VA-1k)

Versión	ArubaOS 8.10
Fabricante	HPE Aruba Networking
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/03/2026



Descripción

Los Aruba Mobility Controllers permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan avanzadas características de seguridad, en el control de acceso a la red, así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS Controladoras y Puntos de Acceso

INFORMACIÓN IMPORTANTE

Sophos Firewall

Versión	SFOS v20.0
Fabricante	Sophos
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/08/2024
Revisión de Validez	31/01/2025


**Descripción**

Sophos Firewall es una solución integral de seguridad de red que ofrece capacidades avanzadas de firewall, protección contra amenazas, filtrado web, control de aplicaciones y un sistema de prevención de intrusiones. El firewall admite alta disponibilidad y rendimiento mediante la agrupación en clústeres y el equilibrio de carga. También incluye controles de identidad de usuario, así como informes y análisis detallados. En resumen, combina múltiples funciones de seguridad en una solución fácil de gestionar, adecuada para redes de todos los tamaños.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Check Point Security Gateway Serie 7000 (CPAP-SG7000)

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025


**Descripción**

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Servidores de Gestión Smart-1 (CPAP-NGSM-405, CPAP-NGSM-410, CPAP-NGSM-625, CPAP-NGSM-5050, CPAP-NGSM-5150)

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025



Descripción

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

Check Point Security Gateway Serie 5000 (CPAP-SG5100, CPAP-SG5200, CPAP-SG5400, CPAP-SG5600, CPAP-SG5800, CPAP-SG5900)

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025



Descripción

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Check Point Security Gateway Serie 23000 (CPAP-SG23500, CPAP-SG23800, CPAP-SG23900)

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

**Descripción**

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

Check Point Security Gateway Serie 16000 (CPAP-SG16000, CPAP-SG16200, CPAP-SG16600HS)

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

**Descripción**

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Check Point Security Threat Emulation/Extraction (CPAP-SBTE250XN y CPAP-SBTE2000XN)

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

**Descripción**

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

Fortigate/FortiOS

Versión	6.4
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/03/2026

**Descripción**

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Check Point Security Gateway Serie 26000 y 28000 (CPAP-SG26000, CPAP-SG28000, CPAP-SG28600)

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

**Descripción**

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

PA-400 Series (PA-410, PA-440, PA-450, PA-460)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

**Descripción**

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

FTD Virtual (FTDv) sobre ESXi 6.7 or 7.0 en Cisco Unified Computing System (UCS) - UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 y UCS-E180D-M3 instalado en ISR

Versión FTD 7.0 y FMC/FMCv 7.0

Fabricante Cisco Systems

Familia Cortafuegos

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 19/10/2023

Revisión de Validez 30/04/2026

Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower



PA-800 Series (PA-820, A-850)

Versión PAN-OS v10.2

Fabricante Palo Alto

Familia Cortafuegos

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/06/2023

Revisión de Validez 30/11/2025

Descripción

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks



INFORMACIÓN IMPORTANTE

Check Point Maestro Hyperscale Appliances (CPAP-MHO-140, CPAP-MHO-175-xC)

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

**Descripción**

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

PA-3400 Series (PA-3410, PA-3420, PA-3430, PA-3440)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

**Descripción**

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

Forcepoint NGFW 3400 series (N3401, N3405, N3410)

Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2025

Descripción

Firewalls de Nueva Generación orientados a grandes redes Campus y Datacenters, de tipo appliance físico de 2RU, IPS, SD-WAN, URL Filtering y Detección Avanzada de Malware. Dependiendo del modelo concreto de dispositivo se puede disponer de hasta un rendimiento de 35 Gbps de Throughput NGFW/NGIPS, 200 millones de conexiones concurrentes y 250 contextos virtuales. Más información en: <https://www.forcepoint.com/environments/forcepoint-ngfw-appliances>

Observaciones

CCN-STIC-1409 Procedimiento de empleo seguro cortafuegos Forcepoint NGFW



Forcepoint NGFW N120 series (N120, N120W, N120WL) y N60

Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2025

Descripción

Firewalls de Nueva Generación orientados a proteger oficinas remotas o entornos SD-WAN de tipo appliance físico con formato sobremesa, con capacidades IPS, SD-WAN, URL Filtering y Detección Avanzada de Malware. Dependiendo del modelo concreto de dispositivo se puede disponer un rendimiento de hasta 450mbps de Throughput NGFW/NGIPS y 3,2 millones de conexiones concurrentes. Más información en: <https://www.forcepoint.com/environments/forcepoint-ngfw-appliances>

Observaciones

CCN-STIC-1409 Procedimiento de empleo seguro cortafuegos Forcepoint NGFW

**INFORMACIÓN IMPORTANTE**

Forcepoint Virtual Appliance (ESXi)

Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2025

Descripción

Firewalls de Nueva Generación orientados a dar servicios de protección perimetral en entornos virtuales, IPS, SD-WAN, URL Filtering y Detección Avanzada de Malware. Dependiendo del número de vCPU asignados se puede disponer de un rendimiento de más de 10GB Gbps de Throughput NGFW/NGIPS. Más información en: <https://www.forcepoint.com/environments/forcepoint-ngfw-appliances>

Observaciones

CCN-STIC-1409 Procedimiento de empleo seguro cortafuegos Forcepoint NGFW



Firepower 2100 Series (2110, 2120, 2130, 2140)

Versión	FTD 7.0 y FMC 7.0
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2026

Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower



INFORMACIÓN IMPORTANTE

Servidores de Gestión Smart-1 600 and 6000 series (CPAP-NGSM600S-X, CPAP-NGSM600M-X, CPAP-NGSM6000L-X, CPAP-NGSM6000XL-X)

Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025



Descripción

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.

Para más información: <https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf>

Observaciones

CCN-STIC 653 Seguridad en Check Point

PA-3200 Series (PA-3220, PA-3250, PA-3260)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025



Descripción

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

PA-220 Series (PA-220, PA-220R)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

**Descripción**

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

Stormshield Network Security UTM/NG-Firewall (Appliances desde SN210 a SN6100 en 4 compilaciones distintas: S, M, L y XL).

Versión	4.3
Fabricante	Stormshield
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2024
Revisión de Validez	31/03/2025

**STORMSHIELD****Descripción**

Firewalls de nueva generación de capa 7, IPS y concentrador de túneles VPN. Con capacidades de bloqueo de amenazas avanzadas, ataques de día cero, filtrado de navegación web o gestión de vulnerabilidades. El mismo equipamiento realiza inspección profunda de protocolos OT, además de IT.

Observaciones

Procedimiento de Empleo Seguro Pendiente de publicación.

INFORMACIÓN IMPORTANTE

PA-7000 Series (PA-7050, PA-7080)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

**Descripción**

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

VM-Series (VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000-HV)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

**Descripción**

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

Firepower 4100 Series (4110, 4112, 4115, 4120, 4125, 4140, 4145 and 4150)

Versión	FTD 7.0, FXOS 2.10 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2026

**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

FTD Virtual (FTDv) sobre NFVIS 4.4 en ENCS 5406, 5408, y 5412

Versión	FTDv 7.0 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	30/04/2026

**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

Firepower 9300 (including chassis, supervisor blade, and security module)

Versión	FTD 7.0, FXOS 2.10 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2026

**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

Firepower 1000 Series (1010, 1120, 1140, 1150)

Versión	FTD 7.0 y FMC 7.0
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2026

**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

SMB Firewall Quantum Spark series. Family 1500 and models 1600, 1800, 1900 and 2000

Versión	R81.10.00
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2022
Revisión de Validez	28/02/2025

**Descripción**

La gama de cortafuegos de nueva generación Quantum Spark están diseñados específicamente para entornos medianos/pequeños con las mismas capacidades que un firewall de datacenter y con un rendimiento que va desde los 600 Mbps hasta los 5 Gbps. Cuentan con una gran variedad de modelos entre los que se incluye un modelo ruggedizado el cual está certificado para su uso en entornos industriales/transporte/marítimo.

A nivel de conectividad ofrece una gran cantidad de opciones, entre las que se destacan: modem LTE, WIFI, xDSL, fibra óptica y por supuesto cobre.

Observaciones

CCN-STIC-653 Seguridad en Checkpoint

FortiGate NGFW Appliances (FG-100F, FG-101E, FG-101F, FG-201E, FG-201F, FG-301E, FG400F, FG-401E, FG401F, FG-501E, FG-600F, FG-601E, FG-601F)

Versión	FortiOS 6.4
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025

**Descripción**

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

INFORMACIÓN IMPORTANTE

FortiGate NGFW Appliances (FG-1101E, FG-1801F, FG-1801F-DC, FG-2000E, FG-2201E, FG-2500E, FG-2601F, FG-2601F-DC, FG-3301E, FG-3401E, FG-3401E-DC, FG-3601E, FG-4201F, FG-4201F-DC, FG-4401F, FG-4401F-DC, FG-5001E1, FG-6300F, FG-6301F, FG-6500F, FG-6501F)

Versión	FortiOS 6.4
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025

FORTINET



Descripción

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

INFORMACIÓN IMPORTANTE

OpnSense Business Edition

Versión	23.4
Fabricante	Deciso B.V
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2022
Revisión de Validez	31/01/2025


**Descripción**

OPNsense es una plataforma de enrutamiento y cortafuegos basada en un sistema operativo BSD de código abierto fortificado, fácil de usar e implantar.

Se trata de un cortafuegos con estado, es decir, un cortafuegos que hace un seguimiento del estado de las conexiones de red (como flujos TCP, comunicación UDP) que viajan a través de él. El producto ofrece una agrupación de reglas de cortafuegos por categoría, una característica excelente para las configuraciones de red más exigentes.

OPNsense incluye la mayoría de las funciones disponibles en los cortafuegos comerciales y más en muchos casos con los beneficios del software de código abierto y verificable.

Suministra las siguientes funcionalidades de seguridad:

- Protección frente al tráfico de red externo a través de la limitación de los paquetes entrantes siguiendo la política aplicada.
- Limitación del acceso a la red externa desde la red interna, de forma que solo se permita a aquellos dispositivos o usuarios especificados en la política de seguridad aplicada.

Con respecto a la versión standard, esta versión da acceso a un repositorio mejorado de actualizaciones Business Edition y plugins extra.

Observaciones

CCN-STIC-1453 Procedimiento de Empleo Seguro Cortafuegos OPNSense

SonicWall SOHO Serie (250, 250W)

Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	28/02/2025


**Descripción**

Los cortafuegos de la serie TZ SOHO de Sonicwall son una solución adecuada para oficinas pequeñas y domésticas, así como para entornos distribuidos en ubicaciones remotas. Despliegan funcionalidades para construir Secure SD-WAN y conectividad WIFI (opcional). El SOHO 250 proporciona un 50% más de rendimiento sobre su antecesor SOHO, así como acceso a los sandboxes avanzados Capture ATP, con lo que se mejora la seguridad en prevención y detección de malware desconocido en un entorno remoto.

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

7.5.4 PROXIES

Zscaler Work from Anywhere	
Versión	ZIA Agent 4.2.0.178
Fabricante	Zscaler Spain, S.L.
Familia	Proxies
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/01/2023
Revisión de Validez	30/06/2025
Descripción	  Zscaler es una plataforma de seguridad en la nube que proporciona un proxy web seguro para proteger a las empresas de las amenazas en línea. El proxy de Zscaler se ejecuta en la nube y se conecta a través de un túnel cifrado a los dispositivos de los usuarios, lo que permite a las empresas proteger sus dispositivos y datos mientras los usuarios acceden a Internet. El proxy de Zscaler ofrece varias características de seguridad, incluyendo filtrado de contenido, detección de amenazas, prevención de intrusiones y cumplimiento normativo. El filtrado de contenido ayuda a evitar el acceso a sitios web maliciosos o inapropiados, mientras que la detección de amenazas utiliza técnicas avanzadas de aprendizaje automático para identificar y bloquear las amenazas en tiempo real. La prevención de intrusiones ayuda a proteger contra ataques de red y la violación de datos, mientras que el cumplimiento normativo ayuda a las empresas a cumplir con las regulaciones y estándares de seguridad. Además, el proxy de Zscaler también ofrece características adicionales, como la capacidad de controlar el acceso a aplicaciones y servicios en la nube, la protección contra el robo de identidad y el filtrado de correo electrónico. También proporciona una visibilidad detallada y un control granular de las actividades en línea de los usuarios, lo que permite a las empresas detectar y abordar rápidamente cualquier actividad sospechosa. Además, Zscaler ofrece una integración con otras soluciones de seguridad, como firewalls, sistemas de detección de intrusos y sistemas de gestión de amenazas, lo que permite una protección más completa y una respuesta más rápida a las amenazas. Observaciones Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Fortinet FortiProxy

Versión	2.0
Fabricante	Fortinet
Familia	Proxies
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	15/05/2025

FORTINET®**Descripción**

A medida que las ciber amenazas se van haciendo más sofisticadas, las compañías necesitan cada vez más una aproximación integral para proteger a los usuarios del tráfico web malicioso, los websites peligrosos y aquel contenido que pueda suponer una amenaza para ellos y sus organizaciones. El Secure Web Gateway (SWG) de Fortinet (FortiProxy) aborda esta situación con un único producto que incluye filtrado de URL, protección contra amenazas avanzadas y malware, filtrado de DNS, DLP, IPS.... La protección de los usuarios contra amenazas procedentes de Internet facilita el cumplimiento de las políticas corporativas tanto normativas como de seguridad.

Observaciones

CCN-STIC-1425 PES FortiProxy

INFORMACIÓN IMPORTANTE

Symantec WPS

Versión

Fabricante Symantec a division of Broadcom

Familia Proxies

Tipo Servicio

Categoría ENS MEDIA

Fecha Inclusión 01/02/2024

Revisión de Validez 31/01/2026

Descripción

Web Protección Suite de Symantec es una solución integral de seguridad en la nube diseñada para salvaguardar a las empresas contra las amenazas en línea. Esta suite ofrece un proxy web seguro que opera en la nube y se conecta a los dispositivos de los usuarios a través de un túnel cifrado, garantizando la protección de los dispositivos y datos corporativos durante la navegación por Internet. Web Protección Suite de Symantec ofrece una amplia gama de características de seguridad, entre las que se incluyen el filtrado de contenido, la detección de amenazas, la prevención de intrusiones y el cumplimiento normativo. El filtrado de contenido ayuda a bloquear el acceso a sitios web maliciosos o inapropiados, mientras que la detección de amenazas utiliza avanzadas técnicas de análisis para identificar y neutralizar las amenazas en tiempo real. La prevención de intrusiones protege contra ataques de red y la violación de datos, mientras que el cumplimiento normativo ayuda a las empresas a cumplir con las regulaciones y estándares de seguridad. Además, Web Protección Suite ofrece funcionalidades adicionales, como el control de acceso a aplicaciones y servicios en la nube, Web Isolation y Sandboxing Asimismo, proporciona una visibilidad detallada y un control granular de las actividades en línea de los usuarios, lo que permite a las empresas detectar y abordar rápidamente cualquier actividad sospechosa. Además, Web Protección Suite se integra fácilmente con otras soluciones de seguridad, como firewalls, sistemas de detección de intrusos y sistemas de gestión de amenazas, para proporcionar una protección completa y una respuesta rápida ante cualquier amenaza.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.



INFORMACIÓN IMPORTANTE

Forcepoint On-Premise Security

Versión	8.5
Fabricante	Forcepoint
Familia	Proxies
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2021
Revisión de Validez	28/02/2026

**Descripción**

Los dispositivos Forcepoint Web Security realizan la función de proxy de navegación segura integrando múltiples motores de clasificación de contenidos y análisis de seguridad en tiempo real con capacidad de inspección de tráfico seguro y también análisis de datos salientes con capacidad para aplicar políticas frente a fugas de información. Las plataformas funcionan como proxies directos http, https, ftp y SOCKS para la protección y control de usuarios y puestos de conexión. El propósito de estos dispositivos es proporcionar una capa de seguridad entre la red Interna y una o más redes externas (típicamente una red corporativa e Internet), aislando el tráfico de los usuarios a nivel de aplicación y proporcionando además diferentes mecanismos de optimización WAN para el tráfico que procesan.

Observaciones

CCN-STIC-1507 Procedimiento de Empleo Seguro Forcepoint On-premise Security 8.5

INFORMACIÓN IMPORTANTE

7.5.5 DISPOSITIVOS DE RED INALÁMBRICOS

Cisco Aironet 3800 Series Access Points (AIR-AP3802I-x-K9, AIR-AP3802I-x-K9C, AIR-AP3802E-x-K9, AIR-AP3802E-x-K9C, AIR-AP3802P-x-K9 y AIR-AP3802P-x-K9C)

Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026



Descripción

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

CCN-STIC-1438 Procedimiento de Empleo Seguro Controladoras inalámbricas CISCO WLC 9800 y Puntos de Acceso Cisco Catalyst

Huawei AirEngine (5760-22W, 5760-51, 5761-10W, 5761-11, 5761-11W, 5761-12W, 5761-21, 5761R-11, 5761R-11E, 5761S-10W, 5761S-11, 5761S-11W, 5761S-12, 5761S-13, 5761S-21, 6760-51E, 6760R-51, 6760-X1, 6760-X1E, 6761-21, 6761-21E, 6761S-21, 8760R-X1, 8760-X1-PRO, 5761-10WD, 5761-11E, 5761-12, 5761RS-11, 5762-12, 5762-12SW, 5762-13W, 5762-15HW, 5762-16W, 5762S-11, 5762S-11SW, 5762S-12, 5762S-12SW, 5762S-13W, 6760R-51E, 6761-21T, 6761-22T, 6761S-21T, 8760R-X1E) y WLAN AC (AC6508, AC6805, AirEngine 9700-M1)

Versión	V200R022C00SPC100 + V200R022C00SPH301T
Fabricante	Huawei Technologies España
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026



Descripción

Los equipos Huawei Wireless Lan combinan plataformas específicas de Controlador (Access Controller) y Punto de Acceso (Access Points) para crear un sistema de acceso inalámbrico que se adapta a redes de campus, redes de oficinas y redes de área metropolitana (MAN) de cualquier tamaño, y a la cobertura de zonas Wi-Fi, proporcionando acceso seguro a la red a los usuarios inalámbricos.

Observaciones

CCN-STIC-1426 Procedimiento de empleo seguro Huawei AirEngine Series

INFORMACIÓN IMPORTANTE

Huawei AirEngine (5760-22W, 5760-51, 5761-10W, 5761-11, 5761-11W, 5761-21, 5761R-11, 5761R-11E, 5761RS-11, 5761S-10W, 5761S-11, 5761S-11W, 5761S-12, 5761S-13, 5761S-21, 6760-51E, 6760R-51, 6760-X1, 6760-X1E, 3562-10, 3562-10SW, 5562-10, 5562-10SW, 5562-17W, 5760-11DH, 5761-10WD, 5761-11E, 5761-12, 5761-12W)

Versión V200R023C00SPC100 + V200R023C00SPH327T

Fabricante Huawei Technologies Co., Ltd.

Familia Dispositivos de Red Inalámbricos

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 13/09/2024

Revisión de Validez 28/02/2027

Descripción

Los equipos Huawei Wireless Lan combinan plataformas específicas de Controlador (Access Controller) y Punto de Acceso (Access Points) para crear un sistema de acceso inalámbrico que se adapta a redes de campus, redes de oficinas y redes de área metropolitana (MAN) de cualquier tamaño, y a la cobertura de zonas Wi-Fi, proporcionando acceso seguro a la red a los usuarios inalámbricos.

Observaciones

CCN-STIC-1426 Procedimiento de empleo seguro Huawei AirEngine Series



Huawei AirEngine (5762-10, 5762-10SW, 5762-12, 5762-12SW, 5762-13W, 5762-15HW, 5762-16W, 5762-17W, 5762S-11, 5762S-11SW, 5762S-12, 5762S-12SW, 5762S-13W, 6760R-51E, 6761-21, 6761-21E, 6761-21T, 6761-22T, 6761S-21, 6761S-21T, 8760R-X1, 8760R-X1E, 8760-X1-PRO, 8761-X1, 8771-X1T, 9700D-S) y WLAN AC (AC6508, AC6805, AirEngine 9700-M1)

Versión V200R023C00SPC100 + V200R023C00SPH327T

Fabricante Huawei Technologies Co., Ltd.

Familia Dispositivos de Red Inalámbricos

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 13/09/2024

Revisión de Validez 28/02/2027

Descripción

Los equipos Huawei Wireless Lan combinan plataformas específicas de Controlador (Access Controller) y Punto de Acceso (Access Points) para crear un sistema de acceso inalámbrico que se adapta a redes de campus, redes de oficinas y redes de área metropolitana (MAN) de cualquier tamaño, y a la cobertura de zonas Wi-Fi, proporcionando acceso seguro a la red a los usuarios inalámbricos.

Observaciones

CCN-STIC-1426 Procedimiento de empleo seguro Huawei AirEngine Series



INFORMACIÓN IMPORTANTE

Cisco 9105 Series Wi-Fi 6 Access Points (C9105AXI-x, C9105AXW-x, C9105AXIT-x y C9105AXWT-x)

Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026

**Descripción**

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

Aruba Mobility Controller (9004, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280) y puntos de acceso.

Versión	ArubaOS 8.6
Fabricante	Aruba
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2024



a Hewlett Packard
Enterprise company

**Descripción**

Las familias Aruba Mobility Controllers 7000's, 7200's, 9000s y las Virtual Mobility Controller (appliance virtual) junto con los puntos de acceso de las familias 500s, 300s y 200s permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Con esta versión se soporta también WPA3 y Wifi-6/802.11ax (con las familias 500s) así como WiFi-5/802.11ac y Wifi-4/802.11n. Se implementan avanzadas características de seguridad, en el control de acceso a la red, así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro. Los Puntos de Acceso en modo pueden trabajar en modo Campus (CAP) y modo Remoto (RAP), lo que permite conectar de forma segura puntos de acceso que cruzan redes ajenas como internet). Se implementan mejoras en actualizaciones de software sin pérdida de servicio. Aruba Multizona permite a un Punto de Acceso dar servicio a varias Mobility Controllers de diferentes dominios o entornos de seguridad. Los Mobility Controllers puede actuar como servidores de túneles IPSEC/SSL para el cliente Aruba VIA.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS 8.6. Controladoras y Puntos de Acceso

INFORMACIÓN IMPORTANTE

Aruba Mobility Controller (9004, 9012, 9240, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) y Aruba Virtual Mobility Controllers (MC-VA-50, MC-VA-250 y MC-VA-1k)

Versión	ArubaOS 8.10
Fabricante	HPE Aruba Networking
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/03/2026



Descripción

Los Aruba Mobility Controllers permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan avanzadas características de seguridad, en el control de acceso a la red, así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS Controladoras y Puntos de Acceso

Cisco Aironet 2800 Series Access Points (AIR-AP2802I-x-K9, AIR-AP2802I-x-K9C, AIR-AP2802E-x-K9 y AIR-AP2802E-x-K9C)

Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026



Descripción

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

CCN-STIC-1438 Procedimiento de Empleo Seguro Controladoras inalámbricas CISCO WLC 9800 y Puntos de Acceso Cisco Catalyst

INFORMACIÓN IMPORTANTE

Cisco 9115 Series Wi-Fi 6 Access Points (C9115AXI-x y C9115AXE-x)

Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026

Descripción

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

Procedimiento de empleo seguro pendiente de publicación



Cisco 9130 Series Wi-Fi 6 Access Points (C9130AXI-x, C9130AXE-x, C9130AXE-STA-x)

Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026

Descripción

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

**INFORMACIÓN IMPORTANTE**

Cisco 9800-80-K9 Wireless Controller, 9800-40-K9 Wireless Controller, 9800-L Wireless Controller (C9800-L-F-K9 y C9800-L-C-K9), C9800-CL-K9 Wireless Controller for Private Cloud.

Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026



Descripción

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

CCN-STIC-1438 Procedimiento de Empleo Seguro Controladoras inalámbricas CISCO WLC 9800 y Puntos de Acceso Cisco Catalyst

Cisco Aironet 4800 Access Point (AIR-AP4800-x-K9 y AIR-AP4800-x-K9)C

Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026



Descripción

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

CCN-STIC-1438 Procedimiento de Empleo Seguro Controladoras inalámbricas CISCO WLC 9800 y Puntos de Acceso Cisco Catalyst

INFORMACIÓN IMPORTANTE

Cisco 9120 Series Wi-Fi 6 Access Points (C9120AXI-x, C9120AXE-x, C9120AXP-x)

Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026

**Descripción**

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

Cisco Aironet 1560 Series Access Points (AIR-AP1562I-x-K9, AIR-AP1562E-x-K9 y AIR-AP1562D-x-K9)

Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026

**Descripción**

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

CCN-STIC-1438 Procedimiento de Empleo Seguro Controladoras inalámbricas CISCO WLC 9800 y Puntos de Acceso Cisco Catalyst

INFORMACIÓN IMPORTANTE

Cisco EW6300 Series Access Points (ESW-6300-CON-X-K9)

Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026

Descripción

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

Procedimiento de empleo seguro pendiente de publicación



Cisco IW6300 Series Access Points (IW-6300H-AC-X-K9, IW-6300H-DC-X-K9 y W-6300H-DCW-X-K9)

Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2026

Descripción

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

**INFORMACIÓN IMPORTANTE**

7.5.6 PASARELAS SEGURAS DE INTERCAMBIO DE DATOS

PSTfile

Versión	v4.4.2
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2025



Descripción

PSTfile es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de ficheros entre dominios de seguridad. Se establece una correspondencia entre carpetas, en servidores de ficheros de ambas redes y PSTfile, automáticamente, mueve o copia los ficheros del origen al destino. Soporta los protocolos FTP, FTPS, SFTP y SMB. La transferencia de ficheros desde el dominio de alta seguridad al de baja requiere autorización mediante firma digital.

Observaciones

Procedimiento de empleo seguro: CCN-STIC-1401 Configuración segura de pasarelas de AUTEK

PSTmail

Versión	v3.0.5
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2025



Descripción

PSTmail es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de correo electrónico entre dominios de seguridad. Posibilita el empleo de direcciones de correo de redes externas, desde una red interna, más segura. Soporta las versiones seguras de los protocolos de correo. Los mensajes de salida requieren autorización mediante firma digital (S/MIME).

Observaciones

Procedimiento de empleo seguro: CCN-STIC-1401 Configuración segura de pasarelas de AUTEK

INFORMACIÓN IMPORTANTE

7.5.7 DIODOS DE DATOS

PSTdiode

Versión	v1.3.1-A
Fabricante	Autek Ingeniería
Familia	Diodos de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2019
Revisión de Validez	31/12/2024



Descripción

El diodo de datos hardware PSTdiode es un dispositivo de protección de perímetro que permite la transferencia de información en un único sentido entre dos dominios de seguridad con garantía física de transmisión unidireccional. Su aplicación principal es la introducción de información en una red aislada en entornos clasificados. También se puede aplicar para extraer información de una red de control industrial en entornos de infraestructuras críticas. En ambos casos se garantiza que no existe tráfico en el sentido inverso. Existen modelos de transferencia de ficheros y tráfico UDP.

Observaciones

Procedimiento de empleo seguro: CCN-STIC 1408 Procedimiento de empleo seguro Diodo Auttek Ingeniería

INFORMACIÓN IMPORTANTE

7.5.8 REDES PRIVADAS VIRTUALES: IPSEC

ASA 5500 Series (5508-X y 5516-X)

Versión	FTD 7.0 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	30/04/2026



Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

SonicWall TZ Serie (300P, 350, 350W, 600P)

Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	28/02/2025



Descripción

La serie TZ de SonicWall ofrece seguridad y rendimiento de entorno Enterprise orientado a pequeñas compañías. Enfocado a entornos departamentales o PYMES de entre 5 y 100 usuarios (aprox), incorpora funciones de prevención de intrusiones, antimalware, filtrado de contenidos/URL y control de aplicaciones a través de redes y entornos inalámbricos. Proporciona inspección profunda de paquetes (DPI), SD-WAN y despliegue zero-touch. Opciones de puertos PoE y wifi 802.11ac. Más info en: <https://www.sonicwall.com/es-mx/products/firewalls/entry-level>

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

Cisco Secure Client - AnyConnect v5.1

Versión	v5.1 installed on Red Hat Enterprise Linux 8.2.
Fabricante	CISCO SYSTEMS, Inc
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/09/2024
Revisión de Validez	28/02/2025

**Descripción**

El Cisco AnyConnect TOE es una aplicación de cliente que proporciona a los usuarios remotos un túnel VPN seguro para proteger los datos en tránsito en redes IPv4 e IPv6. El TOE proporciona IPsec para autenticar y cifrar el tráfico de red que viaja a través de una red pública no protegida. Al proteger la comunicación contra divulgación o modificación no autorizada, los usuarios remotos pueden conectarse de forma segura a los recursos y aplicaciones de la red de una organización.

Observaciones

Procedimiento de Empleo Seguro Pendiente de Publicación

Palo Alto Networks PA-220R, PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.0

Versión	PAN-OS 11.0
Fabricante	Palo Alto Networks
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/06/2024
Revisión de Validez	30/11/2024

**Descripción**

Palo Alto Networks ofrece soluciones robustas para proteger redes empresariales en entornos digitales modernos. Sus Firewalls de Nueva Generación (NGFW) de capa 7 destacan por su adaptabilidad y seguridad avanzada, empleando machine learning y WildFire para detectar y responder rápidamente a amenazas, ya sean conocidas o desconocidas. Aplican políticas basadas en identidades y usuarios para asegurar accesos seguros, gestionadas eficientemente mediante arquitectura de inspección en un único ciclo.

En línea con la estrategia Zero Trust, los firewalls refuerzan políticas de acceso mínimo y previenen amenazas avanzadas. Ofrecen suscripciones como Advanced Threat Prevention para detener ataques de día cero, Advanced URL Filtering para protección de navegación en tiempo real, y Advanced WildFire para prevenir el 99% de amenazas de archivos. Además, complementan con DNS Security, IoT Security adaptada y Next-Generation CASB para proteger aplicaciones SaaS.

Comercializados en múltiples formatos con las mismas capacidades, como PA-Series, VM-Series, CN-Series y Cloud NGFW para AWS y Azure, además de Prisma Access para seguridad global desde la nube, todas gestionadas centralmente por Panorama o Strata Cloud Manager.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

PA-5400 Series (PA-5410, PA-5420, PA-5430, PA-5450)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

**Descripción**

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

WatchGuard Fireware on Firebox NGFWs (T35, T40, T80, T55, M270, M370, M470, M570, M670, M4600 y M5600)

Versión	FirewareOS 12.10
Fabricante	WatchGuard Technologies
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2023
Revisión de Validez	30/05/2025

**Descripción**

Los equipos UTM de WatchGuard están enfocados en ofrecer la mejor seguridad para cualquier empresa y entorno corporativo distribuido. Nuestros dispositivos de seguridad de red están diseñados, desde el inicio, para enfocarse en facilitar el despliegue, el uso y la administración continua. Proporcionan protección contra ataques de malware avanzado y phishing, así como las protecciones de seguridad tradicionales: prevención de intrusiones (IPS), filtrado de URL, control de aplicaciones, antispam y antivirus, ... ofreciendo en todo momento visibilidad del entorno (productividad y seguridad) Cuentan con capacidades SD-WAN, y VPN. Están disponibles tanto en equipos físicos como virtuales. <https://www.watchguard.com/es/wgrd-products/network-security>

Observaciones

CCN-STIC-1421 Procedimiento de empleo seguro WatchGuard Fireware

INFORMACIÓN IMPORTANTE

FortiGate NGFW Appliances (FG40F, FG-60F, FWF-60F, FG-80F, FG-80F-PoE, FG-90G, FG-91G, FG-200F, FG-1100E, FG-1800F, FG-1800F-0DC, FG-2200E, FG-2600F, FG-2600F-0DC, FG-3300E, FG-3400E, FG-3400E-0DC, FG-4200F, FG-4200F-0DC, FG-4400F, FG-4400F-0DC)

Versión FortiOS 6.4

Fabricante Fortinet

Familia Redes privadas virtuales: IPsec

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/02/2024

Revisión de Validez 31/03/2026

Descripción

FORTINET



Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

PA-5200 Series (PA-5220, PA-5250, PA-5260, PA-5280)

Versión PAN-OS v10.2

Fabricante Palo Alto

Familia Redes privadas virtuales: IPsec

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/06/2023

Revisión de Validez 30/11/2025

Descripción

paloalto
NETWORKS



Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP. Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

FortiGate NGFW Appliances (FG-61E, FG-61F, FWF-61E, FWF-61F, FG-81E, FG-81E-PoE, FG-81F, FG-81F-2R, FG-81F-2R-3G4G-PoE, FG-81F-2R-PoE, FG-81F-PoE, FG-90E, FG-91E)

Versión FortiOS 6.4

Fabricante Fortinet

Familia Redes privadas virtuales: IPsec

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/04/2023

Revisión de Validez 30/09/2025

FORTINET



Descripción

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

Cisco Secure Client - AnyConnect 5.0 for iOS 16

Versión 5.0

Fabricante Cisco Systems

Familia Redes privadas virtuales: IPsec

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 18/03/2024

Revisión de Validez 31/12/2024

CISCO



Descripción

Cisco Secure Client (antes conocido como Cisco Anyconnect) es un cliente VPN, que permite a los usuarios de una organización, con dispositivos Android, trabajar de manera remota de forma completamente segura como si estuvieran conectados directamente a su red privada. Proporciona a los usuarios remotos un túnel VPN seguro que autentica y cifra el tráfico de red que viaja a través de una red pública desprotegida.

Cisco Secure Client es un cliente software. Para la certificación en Common Criteria se evaluó en un equipo iPhone 11 con versión iOS 16.

Observaciones

Procedimiento de Empleo Seguro Pendiente de Publicación

INFORMACIÓN IMPORTANTE

WatchGuard Firewall on Firebox NGFWs (T25, T45, T85, M290, M390, M590, M590, M690, M4800, M5800)

Versión	FirewareOS 12.10
Fabricante	WatchGuard Technologies
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2024
Revisión de Validez	30/05/2025



Descripción

Los equipos UTM de WatchGuard están enfocados en ofrecer la mejor seguridad para cualquier empresa y entorno corporativo distribuido. Nuestros dispositivos de seguridad de red están diseñados, desde el inicio, para enfocarse en facilitar el despliegue, el uso y la administración continua. Proporcionan protección contra ataques de malware avanzado y phishing, así como las protecciones de seguridad tradicionales: prevención de intrusiones (IPS), filtrado de URL, control de aplicaciones, antispam y antivirus, ... ofreciendo en todo momento visibilidad del entorno (productividad y seguridad) Cuentan con capacidades SD-WAN, y VPN. Están disponibles tanto en equipos físicos como virtuales. <https://www.watchguard.com/es/wgrd-products/network-security>

Observaciones

CCN-STIC-1421 Procedimiento de empleo seguro WatchGuard Firewall

ISA 3000 (ISA 3000-4C y ISA 3000-2C2F)

Versión	FTD 7.0 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	30/04/2026



Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

Cisco Secure Client - AnyConnect 5.0 for Android 12

Versión	5.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2023
Revisión de Validez	30/06/2026

**Descripción**

Cisco Secure Client (antes conocido como Cisco Anyconnect) es un cliente VPN, que permite a los usuarios de una organización, con dispositivos Android, trabajar de manera remota de forma completamente segura como si estuvieran conectados directamente a su red privada. Proporciona a los usuarios remotos un túnel VPN seguro que autentica y cifra el tráfico de red que viaja a través de una red pública desprotegida.

Cisco Secure Client es un cliente software. Para la certificación en Common Criteria se evaluó en un equipo Galaxy A71 5G con versión Android 12.

Observaciones

CCN-STIC 1448 Cisco AnyConnect Secure Mobility Android y Windows

FortiGate NGFW VM64

Versión	FortiOS 6.4
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025

**Descripción**

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

INFORMACIÓN IMPORTANTE

Next-Generation Firewall with PAN-OS PA-200 Series (PA-220, PA220R), PA-400, PA-800 Series (PA-820, PA850), PA-3200 Series (PA-3220, PA3250, PA3260), PA-5200 Series (PA-5220, PA5250, PA5260, PA5280), PA-5450, PA-7000 Series (PA-7050, PA7080), VM-Series (VM-50, VM-100, VM-300, VM-500, VM-700, VM-1000HV)

Versión 10.1

Fabricante Palo Alto

Familia Redes privadas virtuales: IPSec

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/10/2022

Revisión de Validez 31/03/2025

Descripción



Firewalls de Nueva Generación orientado a grandes empresas y datacenters, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado.

Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido. Soportan hipervisores: vmware ESXi, Citrix SDX, Microsoft Hyper-V, KVM, vmware vCloud Air, Microsoft Azure y Amazon AWS.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

Cisco Secure Client - AnyConnect para Windows 10

Versión 5.0

Fabricante Cisco Systems

Familia Redes privadas virtuales: IPSec

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/03/2024

Revisión de Validez 31/12/2024

Descripción



Cisco Secure Client (antes conocido como Cisco Anyconnect) es un cliente VPN, que permite a los usuarios de una organización, con dispositivos Android, trabajar de manera remota de forma completamente segura como si estuvieran conectados directamente a su red privada. Proporciona a los usuarios remotos un túnel VPN seguro que autentica y cifra el tráfico de red que viaja a través de una red pública desprotegida.

Además de las funciones de VPN, Cisco AnyConnect puede incluir otras características de seguridad como la protección contra malware, el filtrado de contenido web y la prevención de intrusiones, dependiendo de los módulos adicionales implementados en la solución.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Fortigate/FortiOS

Versión	7.0
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/09/2024
Revisión de Validez	28/02/2025

FORTINET®**Descripción**

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

Aruba Mobility Controller (9004, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280) y puntos de acceso.

Versión	ArubaOS 8.6
Fabricante	Aruba
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2024

aruba
a Hewlett Packard
Enterprise company

**Descripción**

Las familias Aruba Mobility Controllers 7000's, 7200's, 9000s y las Virtual Mobility Controller (appliance virtual) junto con los puntos de acceso de las familias 500s, 300s y 200s permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Con esta versión se soporta también WPA3 y Wifi-6/802.11ax (con las familias 500s) así como Wifi-5/802.11ac y Wifi-4/802.11n. Se implementan avanzadas características de seguridad, en el control de acceso a la red, así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro. Los Puntos de Acceso en modo pueden trabajar en modo Campus (CAP) y modo Remoto (RAP), lo que permite conectar de forma segura puntos de acceso que cruzan redes ajenas como internet). Se implementan mejoras en actualizaciones de software sin pérdida de servicio. Aruba Multizona permite a un Punto de Acceso dar servicio a varias Mobility Controllers de diferentes dominios o entornos de seguridad. Los Mobility Controllers puede actuar como servidores de túneles IPSEC/SSL para el cliente Aruba VIA.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS 8.6. Controladoras y Puntos de Acceso

INFORMACIÓN IMPORTANTE

MX240, MX480 y MX960 con tarjetas MPC10E y MX-SPC3

Versión	22.2R1
Fabricante	Juniper Networks
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2024
Revisión de Validez	31/01/2025

JUNIPER
NETWORKS

**Descripción**

Las plataformas de enrutamiento y switching universal MX240/MX480/MX960 brindan un rendimiento de gran escalabilidad en un factor de forma optimizado para la nube y las economías de coste por puerto o bit más

exigentes. Se pueden utilizar tanto en redes de tipo operador, como nodo de borde en redes MPLS, en entornos de movilidad convergente, IoT, empresarial y también en arquitecturas de Core convergente y de borde multiservicio. También soporta el uso como enrutador de conmutación de etiquetas (LSR), provider Edge, equipo de intercambio de Internet y red troncal para implementaciones en redes de carácter metropolitanas, regionales o nacionales, o terminador de túneles IPSEC o Firewall de capa 4. La serie MX admite un amplio conjunto de funcionalidades IPoDWDM, L2, L3, IP/MPLS, SR, SRv6, terminador de túneles IPSEC o CGNAT para permitir redes de transporte a gran escala con operaciones y provisión de servicios simplificados, manteniendo simplicidad en la red. Gracias al tipo de chipsets implementados, tienen una capacidad de programación en el plano de datos casi infinita, lo que le brinda la libertad de implementar nuevas innovaciones de red. Con tecnología de silicio TRIO, la familia MX es altamente escalable desde los 3Tbps en 5U, hasta un rendimiento de 12 Tbps en 16 slots.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

Aruba Mobility Controller (9004, 9012, 9240, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) y Aruba Virtual Mobility Controllers (MC-VA-50, MC-VA-250 y MC-VA-1k)

Versión	ArubaOS 8.10
Fabricante	HPE Aruba Networking
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/03/2026

aruba
a Hewlett Packard
Enterprise company

**Descripción**

Los Aruba Mobility Controllers permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan avanzadas características de seguridad, en el control de acceso a la red, así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS Controladoras y Puntos de Acceso

INFORMACIÓN IMPORTANTE

Fortigate/FortiOS

Versión	6.4
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/03/2026

FORTINET®**Descripción**

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

PA-400 Series (PA-410, PA-440, PA-450, PA-460)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

paloalto®
NETWORKS**Descripción**

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

FTD Virtual (FTDv) sobre ESXi 6.7 or 7.0 en Cisco Unified Computing System (UCS) - UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 y UCS-E180D-M3 instalado en ISR

Versión	FTD 7.0 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	30/04/2026



Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

PA-800 Series (PA-820, A-850)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025



Descripción

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

PA-3400 Series (PA-3410, PA-3420, PA-3430, PA-3440)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

**Descripción**

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

Firepower 2100 Series (2110, 2120, 2130, 2140)

Versión	FTD 7.0 y FMC 7.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2026

**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

PA-3200 Series (PA-3220, PA-3250, PA-3260)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

**Descripción**

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

PA-220 Series (PA-220, PA-220R)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

**Descripción**

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

PA-7000 Series (PA-7050, PA-7080)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

**Descripción**

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

VM-Series (VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000-HV)

Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

**Descripción**

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.

Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

Firepower 4100 Series (4110, 4112, 4115, 4120, 4125, 4140, 4145 and 4150)

Versión FTD 7.0, FXOS 2.10 y FMC/FMCv 7.0**Fabricante** Cisco Systems**Familia** Redes privadas virtuales: IPsec**Tipo** Producto**Categoría ENS** ALTA**Fecha Inclusión** 19/10/2023**Revisión de Validez** 31/03/2026**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower



FTD Virtual (FTDv) sobre NFVIS 4.4 en ENCS 5406, 5408, y 5412

Versión FTDv 7.0 y FMC/FMCv 7.0**Fabricante** Cisco Systems**Familia** Redes privadas virtuales: IPsec**Tipo** Producto**Categoría ENS** ALTA**Fecha Inclusión** 19/10/2023**Revisión de Validez** 30/04/2026**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

**INFORMACIÓN IMPORTANTE**

Firepower 9300 (including chassis, supervisor blade, and security module)

Versión	FTD 7.0, FXOS 2.10 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2026

**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

Firepower 1000 Series (1010, 1120, 1140, 1150)

Versión	FTD 7.0 y FMC 7.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2026

**Descripción**

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)

-FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

FortiGate NGFW Appliances (FG-100F, FG-101E, FG-101F, FG-201E, FG-201F, FG-301E, FG400F, FG-401E, FG401F, FG-501E, FG-600F, FG-601E, FG-601F)

Versión FortiOS 6.4

Fabricante Fortinet

Familia Redes privadas virtuales: IPSec

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/04/2023

Revisión de Validez 30/09/2025

Descripción

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

FORTINET



FortiGate NGFW Appliances (FG-1101E, FG-1801F, FG-1801F-DC, FG-2000E, FG-2201E, FG-2500E, FG-2601F, FG-2601F-DC, FG-3301E, FG-3401E, FG-3401E-DC, FG-3601E, FG-4201F, FG-4201F-DC, FG-4401F, FG-4401F-DC, FG-5001E1, FG-6300F, FG-6301F, FG-6500F, FG-6501F)

Versión FortiOS 6.4

Fabricante Fortinet

Familia Redes privadas virtuales: IPSec

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/04/2023

Revisión de Validez 30/09/2025

Descripción

Firewalls de Nueva Generación (NGFW) con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Las funcionalidades de seguridad más destacables son: reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, protección DoS, proxy explícito, Inspección SSL, capacidades SDWAN, VPN (IPSEC y SSL), control de Access Points, LTE/5G y Switches, todo ello potenciado gracias su integración con Fortiguard Services y su protección contra amenazas basadas en IA.

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

FORTINET



INFORMACIÓN IMPORTANTE

Aruba Virtual Intranet Access (VIA) Client

Versión	4.3
Fabricante	Aruba
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	30/06/2025

**Descripción**

Aruba Virtual Intranet Access (VIA) es un servicio VPN seguro para usuarios que necesitan conectividad corporativa remota desde el hogar, ubicaciones temporales o mientras están en movimiento. Se encuentra disponible como una descarga de software para Google Android, Apple iOS, MacOS, Linux y Windows, pudiéndose integrar con plataformas de múltiple factor de autenticación (MFA, 2FA).

La función cualificada del VIA es la de cliente VPN IPSEC que evalúa y selecciona automáticamente la mejor conexión segura para efectuar la conexión VPN con la organización. A diferencia de las VPN tradicionales que requieren hardware dedicado (terminadores de túneles), Aruba integra servicios VPN directamente en la infraestructura segura existente de Aruba (Mobility Controllers) para simplificar la arquitectura y la administración.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS 8.6. Controladoras y Puntos de Acceso

IS101

Versión	1.01
Fabricante	ISTRIA SOLUCIONES DE CRIPTOGRAFIA
Familia	Redes privadas virtuales: IPsec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2018
Revisión de Validez	31/12/2025

**Descripción**

El equipo IS101 es un cifrador de altas prestaciones que, sobre una plataforma hardware segura con un FW/SW específico, implementa protocolo IPsec en modo túnel. (con encapsulado ESP y protocolo IKEv2), lo que permite establecer, de forma sencilla y eficiente, redes privadas virtuales (VPN) sobre una red IP no confiable (ya sea pública o privada). Diseñado para sistemas en entornos críticos que manejan información sensible. Velocidad de transferencia de 2Gbps agregados.

Observaciones

CCN-STIC-1405 Procedimiento de empleo seguro IS101

INFORMACIÓN IMPORTANTE

SonicWall SOHO Serie (250, 250W)

Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	28/02/2025

SONICWALL®

**Descripción**

Los cortafuegos de la serie TZ SOHO de Sonicwall son una solución adecuada para oficinas pequeñas y domésticas, así como para entornos distribuidos en ubicaciones remotas. Despliegan funcionalidades para construir Secure SD-WAN y conectividad WIFI (opcional). El SOHO 250 proporciona un 50% más de rendimiento sobre su antecesor SOHO, así como acceso a los sandboxes avanzados Capture ATP, con lo que se mejora la seguridad en prevención y detección de malware desconocido en un entorno remoto.

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

7.5.9 REDES PRIVADAS VIRTUALES: SSL

Cisco AnyConnect Secure Mobility Client for iOS 13

Versión	4.9
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: SSL
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/06/2026

Descripción

El Cisco AnyConnect Secure Mobility Client v4.9 for IOS 13 es un cliente VPN, que permite a los usuarios de una organización, con dispositivos IOS, trabajar de manera remota de forma completamente segura como si estuvieran conectados directamente a su red privada.

Observaciones

CCN-STIC-1449 Cisco AnyConnect Secure Mobility para iOS



Cisco AnyConnect Secure Mobility Client for Android 11

Versión	4.10
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: SSL
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/06/2026

Descripción

El Cisco AnyConnect Secure Mobility Client v4.10 for Android 11 es un cliente VPN, que permite a los usuarios de una organización, con dispositivos Android, trabajar de manera remota de forma completamente segura como si estuvieran conectados directamente a su red privada.

Observaciones

CCN-STIC 1448 Cisco AnyConnect Secure Mobility Android y Windows



INFORMACIÓN IMPORTANTE

Cisco AnyConnect Secure Mobility Client for Windows 10

Versión	4.10
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: SSL
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/06/2026

**Descripción**

El Cisco AnyConnect Secure Mobility Client v4.10 for Windows 10 es un cliente VPN, que permite a los usuarios de una organización, con dispositivos Windows, trabajar de manera remota de forma completamente segura como si estuvieran conectados directamente a su red privada.

Observaciones

CCN-STIC 1448 Cisco AnyConnect Secure Mobility Android y Windows

INFORMACIÓN IMPORTANTE

7.5.10 REDES PRIVADAS VIRTUALES: OTROS

OpenNAC Enterprise		 
Versión	CMI/CMIX 1.6.0-23.7153 Core 1.2.2-0.11643	
Fabricante	Cipherbit – Grupo Oesia	
Familia	Redes privadas virtuales: Otros	
Tipo	Producto	
Categoría ENS	MEDIA	
Fecha Inclusión	01/09/2021	
Revisión de Validez	31/12/2024	
Descripción		
El módulo de concentración de VPNs de la plataforma OpenNAC Enterprise by Cipherbit ofrece una solución avanzada para la gestión de túneles VPN, actuando como frontend mediante un agente nativo, multiplataforma, que combina rendimiento, seguridad y adaptabilidad.		
Observaciones		
CCN-STIC-1105 Procedimiento de empleo seguro EMMA		

INFORMACIÓN IMPORTANTE

7.5.11 HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA (IM)

Sotera Phone H1U	
Versión	0.455
Fabricante	Sotera Digital Security Corporation
Familia	Herramientas de mensajería instantánea (IM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2024
Revisión de Validez	31/01/2027
Descripción	El SecurePhone es un teléfono móvil de propiedad exclusiva de Sotera que funciona con el sistema operativo INTEGRITY. El SecurePhone permite que se realicen comunicaciones de voz y texto seguras en cualquier lugar del mundo y utilizando cualquier red pública, brindando privacidad a sus usuarios. Diseñado con la idea de brindar un nivel único de protección, el SecurePhone fue fabricado desde cero con el propósito de proteger su hardware, software y aplicaciones de mensajería contra ciberataques sofisticados. Para más detalles, visitar www.soteradigital.com/es. Observaciones CCN-STIC-1640 Procedimiento de empleo seguro Sotera Phone H1U



COMSec	
Versión	v4.2
Fabricante	Indra
Familia	Herramientas de mensajería instantánea (IM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2018
Revisión de Validez	31/12/2024
Descripción	COMSec es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con su alto nivel de seguridad, gran calidad de audio y facilidad de uso protege de forma eficaz cualquier información sensible de la organización. Las llamadas y los datos intercambiados por COMSec son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: comsec.indracompany.com Observaciones CCN-STIC-1407 Procedimiento de Empleo Seguro de COMSec



INFORMACIÓN IMPORTANTE

7.5.12 HERRAMIENTAS VOZ IP

Cisco Unified Communications Manager (C220 M5 y C240 M5)

Versión	12.5 y 14 (con Centos 7.7)
Fabricante	Cisco Systems
Familia	Herramientas Voz IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2023
Revisión de Validez	31/08/2025

**Descripción**

Sistema de comunicaciones empresarial que suministra voz y videollamadas sobre una red IP.

Observaciones

CCN-STIC-1460 PES Cisco Unified Communications Manager

Sotera Phone H1U

Versión	0.455
Fabricante	Sotera Digital Security Corporation
Familia	Herramientas Voz IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2024
Revisión de Validez	31/01/2027

**Descripción**

El SecurePhone es un teléfono móvil de propiedad exclusiva de Sotera que funciona con el sistema operativo INTEGRITY. El SecurePhone permite que se realicen comunicaciones de voz y texto seguras en cualquier lugar del mundo y utilizando cualquier red pública, brindando privacidad a sus usuarios. Diseñado con la idea de brindar un nivel único de protección, el SecurePhone fue fabricado desde cero con el propósito de proteger su hardware, software y aplicaciones de mensajería contra ciberataques sofisticados. Para más detalles, visitar www.soteradigital.com/es.

Observaciones

CCN-STIC-1640 Procedimiento de empleo seguro Sotera Phone H1U

INFORMACIÓN IMPORTANTE

COMSec

Versión	v4.2
Fabricante	Indra
Familia	Herramientas Voz IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2018
Revisión de Validez	31/12/2024

**Descripción**

COMSec es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con su alto nivel de seguridad, gran calidad de audio y facilidad de uso protege de forma eficaz cualquier información sensible de la organización. Las llamadas y los datos intercambiados por COMSec son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: comsec.indracompany.com

Observaciones

CCN-STIC-1407 Procedimiento de Empleo Seguro de COMSec

INFORMACIÓN IMPORTANTE

7.5.13 HERRAMIENTAS DE VIDEOCONFERENCIA

PEXIP Infinity		 
Versión	v.25.4 (Build 59565.0.0); Client software v1.6.2	
Fabricante	PEXIP	
Familia	Herramientas de videoconferencia	
Tipo	Producto	
Categoría ENS	MEDIA	
Fecha Inclusión	01/03/2022	
Revisión de Validez	31/08/2025	
Descripción		
Plataforma de infraestructura de videoconferencia virtualizada y distribuida, para gestionar equipos de videoconferencia de sala H.323/SIP y clientes de escritorio PC, Mac, Linux, con cliente WebRTC. Actúa de Call Control, consta de firewall traversal, unidad multiconferencia (MCU), sistema de gestión de terminales y aloja usuarios de escritorio y móviles. Proporciona bridge para interoperar con usuarios de Microsoft Teams CVI, Google Meet, Skype for Business, Webex y WebRTC, y hace streaming y recording. Integra Outlook y Google Calendar para la planificación de sesiones, SSO, certificados y LDAP. Consta de una amplia librería de APIs. La arquitectura se basa en 3 tipos de nodos: - Management Node para gestionar y configurar la plataforma, las políticas de llamadas y la monitorización. - Transcoding Nodes, donde se procesan y alojan las conferencias y multiconferencias. Proporciona redundancia y es resistente a pérdida de paquetes y bajos ratios de transferencia. - Edge Nodes en donde se negocia la señalización con redes externas y donde securiza el tráfico y oculta la topología de red interna. Esta arquitectura es escalable y permite la securización de las comunicaciones mediante cifrado. Permite la privacidad de datos, equipos y usuarios.		
Observaciones		
CCN-STIC-1616 PES Pexip Infinity		

INFORMACIÓN IMPORTANTE

7.5.14 WEB APPLICATION FIREWALL (WAF)

AWS WAF

Versión
Fabricante AWS

Familia Web Application Firewall (WAF)

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 18/11/2024

Revisión de Validez 30/04/2025

Descripción

AWS WAF es un firewall de aplicación web que le permite monitorear y administrar las solicitudes web que se reenvían a recursos protegidos mediante AWS. Con AWS WAF, puede proteger recursos como distribuciones de Amazon CloudFront, API de REST de Amazon API Gateway, Application Load Balancers y API GraphQL de AWS AppSync. Puede usar AWS WAF para inspeccionar las solicitudes web y ver si cumplen las condiciones que especifique, como la dirección IP desde la que se originan las solicitudes, el valor de un componente de solicitud específico o la velocidad a la que se envían las solicitudes. AWS WAF puede administrar las solicitudes coincidentes de varias formas: puede contarlas, bloquearlas o permitir las, o bien enviar desafíos, como verificaciones de CAPTCHA, al navegador o al usuario del cliente.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.



INFORMACIÓN IMPORTANTE

7.5.15 REDES DEFINIDAS POR SOFTWARE (SDN)

iMaster NCE Campus	
Versión	V300R020C10CP1061
Fabricante	Huawei Technologies España
Familia	Redes definidas por software (SDN)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/10/2024
Revisión de Validez	31/03/2025
Descripción	El sistema de gestión y control para redes de campus de conducción autónoma iMaster NCE-Campus de Huawei de próxima generación integra funciones de gestión, control(NAC), análisis e inteligencia artificial (IA), proporciona una automatización de ciclo de vida completo de las redes de campus. El cierre inteligente de fallos también se implementa a través de análisis de big data e IA.
Observaciones	Procedimiento de empleo seguro pendiente de publicación.



INFORMACIÓN IMPORTANTE

7.5.16 CIFRADORES IP

IS101

Versión	1.01
Fabricante	ISTRIA SOLUCIONES DE CRIPTOGRAFIA
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2018
Revisión de Validez	31/12/2025

**Descripción**

El equipo IS101 es un cifrador de altas prestaciones que, sobre una plataforma hardware segura con un FW/SW específico, implementa protocolo IPSec en modo túnel. (con encapsulado ESP y protocolo IKEv2), lo que permite establecer, de forma sencilla y eficiente, redes privadas virtuales (VPN) sobre una red IP no confiable (ya sea pública o privada). Diseñado para sistemas en entornos críticos que manejan información sensible. Velocidad de transferencia de 2Gbps agregados.

Observaciones

CCN-STIC-1405 Procedimiento de empleo seguro IS101

EP960

Versión	1.09.17
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	31/12/2025

**Descripción**

Cifrador personal de tamaño reducido (120x80x25mm) para la protección de las comunicaciones. Cuenta con varios interfaces negros (interfaces no seguros donde la información ya está cifrada) : Ethernet, WiFi y 3G/4G. Ofrece un nivel medio de seguridad y proporciona una solución de WiFi seguro.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

7.6 PROTECCIÓN DE LA INFORMACIÓN Y LOS SOPORTES DE LA INFORMACIÓN

7.6.1 ALMACENAMIENTO CIFRADO DE DATOS

CRYHOD	
Versión	Q.2021.2
Fabricante	PRIMX
Familia	Almacenamiento cifrado de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2023
Revisión de Validez	30/11/2025
Descripción Cryhod es un programa de cifrado moderno que asegura el cifrado completo de los discos duros de las estaciones de trabajo portátiles de la organización. Cryhod implementa mecanismo de autenticación fuerte (doble factor) mediante la tarjeta SmartCard de la FNMT en el Pre-Boot del equipo lo que permite identificar unívocamente a los usuarios del sistema y protegerlo frente a ataques en caso de pérdida o robo.	
Observaciones CCN-STIC-1505 Procedimiento de Empleo Seguro CRYHOD de PRIMX	

CRYHOD
FOR DISKS AND LAPTOPS



ZONE CENTRAL	
Versión	Q.2021.1
Fabricante	PRIMX
Familia	Almacenamiento cifrado de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2023
Revisión de Validez	30/04/2025
Descripción ZONECENTRAL es un software de cifrado de datos cuyo objetivo es asegurar la confidencialidad de todos los archivos de una organización (locales, en la red y compartidos) incluyendo los perfiles de usuario. ZONECENTRAL facilita la gestión de "la necesidad de conocer", protegiendo el acceso a los datos sensibles y segmentando la información entre los diferentes perfiles de usuarios. Solo los usuarios autorizados pueden entender el contenido de un determinado fichero. ZONECENTRAL se instala en los puestos de trabajo como cualquier otro software de seguridad informática, integrándose con otras soluciones del tipo PKI, tarjetas inteligentes, token, etc.. y aplica de forma automática las políticas de seguridad de la empresa.	
Observaciones Procedimiento de Empleo Seguro pendiente de publicación.	

ZONECENTRAL
FOR FILES AND FOLDERS



INFORMACIÓN IMPORTANTE

7.6.2 CIFRADO Y COMPARTICIÓN SEGURA DE INFORMACIÓN

EP852

Versión	3.05
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2025



Descripción

El EP852 es un cifrador de ficheros fuera de línea que permite el cifrado y descifrado de ficheros y el transporte de información cifrada en el dispositivo. Mejora las prestaciones en cuanto a almacenamiento y velocidad de las versiones anteriores de los Token USB así como la puesta en marcha del dispositivo, carga y distribución de claves.

Observaciones

Utilización según el PE-2020-4 -Procedimiento de Empleo Seguro EP852 -(ESP)

INFORMACIÓN IMPORTANTE

SMiD Cloud

Versión	2.1
Fabricante	ENCIFRA
Familia	Cifrado y compartición segura de información
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2024

**Descripción**

SMiD cloud es un dispositivo hardware Plu&Play que se integra en una red local SMB de Microsoft y que se encarga del almacenamiento cifrado de los ficheros que se almacenen en él. El uso de SMiD cloud NO requiere la instalación de ningún tipo de software o agente en los equipos que lo utilizan. Los ficheros cifrados pueden almacenarse en local y/o en uno o varios proveedores de almacenamiento en la nube. Los dispositivos SMiD cloud sólo mantienen copias en claro de los ficheros que están siendo utilizados y retornan cualquier fichero a su estado cifrado cuando se dejan de utilizar.

El arranque de todo dispositivo SMiD cloud requiere la presencia en el arranque de una llave física USB de arranque sin la cual el dispositivo no arranca. Si se configura explícitamente para ello, los dispositivos SMiD cloud pueden ser clonados en el caso de que el original se deteriore, sea sustraído o destruido.

SMiD cloud es compatible con Directorio Activo y con cualquier sistema operativo que opere en la red local SMB. El uso de diferentes dispositivos permite la compartimentalización automática del riesgo y de los sistemas de almacenamiento. La estructura del sistema de ficheros no sale del dispositivo SMiD cloud que los creó y no son deducibles desde el exterior.

SMiD cloud protege confidencialidad e integridad de la información que se le entrega frente a ataques en la nube o en almacenamiento local. Cualquier ataque de ransomware no pone en peligro las copias cifradas en local o en la nube ya que son inaccesibles incluso para los usuarios autorizados o para el administrador del dispositivo.

Cada fichero se cifra con una clave distinta, realmente aleatoria y de 256 bits de longitud, mediante el cifrador AES-256. La integridad de cada fichero está controlada con el valor SHA-256 del mismo.

Observaciones

Sin Procedimiento de Empleo Seguro

INFORMACIÓN IMPORTANTE

GuardedBox

Versión	10.5
Fabricante	DinoSec
Familia	Cifrado y compartición segura de información
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	31/05/2025

**Descripción**

GuardedBox es una solución para almacenamiento, compartición y control seguros de información, con cifrado E2E, disponible para despliegues on-premise y en nube pública o privada, tanto autogestionados como en modalidad SaaS.

La información almacenada (denominada "secretos") y sus metadatos se guardan cifrados en el servidor mediante claves AES-256 bits, y se cifran y descifran en el lado cliente mediante criptografía asimétrica de curva elíptica reconocida para ENS en categoría ALTA y complementada con sofisticados controles de acceso.

Funcionalidades:

- Intercambio en tiempo real: individual o de grupo, disponible tanto para usuarios registrados como externos, con filtros por dominio y mecanismos de control para conocer los estados actuales y pasados de compartición.
- Notificaciones: avisa a los usuarios (por email y en el interfaz) de los eventos que afectan a los elementos de su ámbito.
- Auditoría: implementada como blockchain, registra todos los eventos sin desvelar el contenido de la información.
- Recordatorios: para definir avisos sobre acciones necesarias.
- Diseño APIfido: admite integración con otras soluciones del entorno (SSO, logging, etc.).
- Personalizaciones a medida.
- Panel de administración.

Observaciones

CCN-STIC 1509 Procedimiento de empleo seguro Guardedbox

INFORMACIÓN IMPORTANTE

EP880

Versión	V2.08.36 y V2.09.35
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2026

**Descripción**

El EP880 es una aplicación software que se ejecuta sobre ordenador con sistema operativo Windows y que permite realizar, en origen, el cifrado y firma de ficheros de datos “off-line” almacenados en el disco duro del ordenador o dispositivos de almacenamiento externos conectados al ordenador, para su posterior almacenamiento y/o envío de forma segura desde el correo electrónico u otro medio y, en destino, el descifrado y verificación de la integridad de los datos.

Observaciones

CCN-STIC-1506 Procedimiento de Empleo Seguro EP880

EP852

Versión	3.04
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2025

**Descripción**

El EP852 es un cifrador de ficheros fuera de línea que permite el cifrado y descifrado de ficheros y el transporte de información cifrada en el dispositivo. Mejora las prestaciones en cuanto a almacenamiento y velocidad de las versiones anteriores de los Token USB así como la puesta en marcha del dispositivo, carga y distribución de claves.

Observaciones

Utilización según el PE-2020-4 -Procedimiento de Empleo Seguro EP852 -(ESP)

INFORMACIÓN IMPORTANTE

7.6.3 HERRAMIENTAS DE BORRADO SEGURO

Blancco File Eraser

Versión	v8.5.2
Fabricante	Blancco
Familia	Herramientas de borrado seguro
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/06/2024



Descripción

La solución de borrado de archivos Blancco File Eraser permite administrar y automatizar rutinas de borrado de datos en ordenadores de sobremesa, portátiles y servidores. **BENEFICIOS PRINCIPALES** 1. Borrado seguro de datos en ficheros. 2. Borrado automatizado. 3. Monitoriza e informa de todas las actividades de borrado. 4. Borrado conforme a los criterios de los órganos normativos gracias a su reporte certificado de auditoría y en cumplimiento con RGPD. 5. Sencilla instalación. Más información: espana@deletetecnology.com - 91 761 23 70.

Observaciones

CCN-STIC 1502 Procedimiento de empleo seguro de Blancco File Eraser

Blancco Drive Eraser

Versión	7.6
Fabricante	Blancco
Familia	Herramientas de borrado seguro
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2020
Revisión de Validez	30/06/2024



Descripción

Software de borrado seguro de datos para discos duros HDD y estado sólido SSD en computadoras de escritorio, laptops y almacenamiento masivo con adaptadores IDE, SATA, SAS, SCSI, FIBRA CANAL FC, SSD y Emmc. Ofrece un borrado seguro del 100% del disco duro por particiones físicas al realizar una sobre escritura en la totalidad de los sectores contenidos en el disco duro. Permite un borrado automatizado, monitorización de las actividades de borrado e informa de todas las actividades de borrado facilitando el cumplimiento de las Políticas de Seguridad y Retención de Información. El borrado realizado es conforme a los criterios de los órganos normativos gracias a su reporte certificado de auditoría y en cumplimiento con RGPD. Dispone de una instalación flexible y sencilla.

Observaciones

CCN-STIC 1504 Procedimiento de empleo seguro de Blancco Drive Eraser

INFORMACIÓN IMPORTANTE

OLVIDO Windows

Versión	1.0.6
Fabricante	authUSB
Familia	Herramientas de borrado seguro
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	28/02/2025

**Descripción**

OLVIDO es una herramienta de borrado seguro que realiza tareas de sobreescritura y borrado sobre los sistemas de archivos y discos reconocidos. Ofrece al usuario la posibilidad de borrar de forma segura distintos elementos guardados en los dispositivos de almacenamiento:

- Ficheros y carpetas
- Espacio Libre
- Fragmentos de clúster no utilizados
- Discos y volúmenes

Dispone de un módulo de planificación con el que se permite al usuario programar la ejecución de las tareas de borrado. OLVIDO implementa distintos algoritmos estándar de borrado y permite al usuario seleccionar el algoritmo de borrado a aplicar en cada tarea. Así mismo, ofrece la posibilidad al administrador de definir algoritmos de borrado personalizados, especificando el número de pases y el patrón de sobreescritura. Permite la integración con un servidor Syslog para el envío de registros de actividad y estado de las tareas de borrado realizadas.

La versión aprobada permite, con el algoritmo de borrado CCN-Clasificado, la reclasificación y desclasificación de:

- Discos magnéticos hasta RESERVADO o equivalente.
- Discos SSD hasta DIFUSIÓN LIMITADA o equivalente.

Se ejecuta sobre Windows 10, Windows Server 2016 y Windows Server 2021.

Observaciones

CCN-STIC-1508 Procedimiento de empleo seguro OLVIDO

INFORMACIÓN IMPORTANTE

7.6.4 SISTEMAS PARA PREVENCIÓN DE FUGAS DE DATOS

Microsoft Purview Data Loss Prevention

Versión
Fabricante Microsoft

Familia Sistemas para prevención de fugas de datos

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 30/10/2024

Revisión de Validez 31/03/2025

Descripción

Microsoft Purview Data Loss Prevention (DLP) es una solución de nube integrada y extensible que permite a las organizaciones gestionar sus políticas de prevención de pérdida de datos desde un único portal.

Utiliza análisis de contenido y algoritmos de aprendizaje automático para identificar, monitorizar y proteger automáticamente información sensible en servicios de Microsoft 365, así como en aplicaciones de Office y Endpoints con Windows y macOS.

Esta solución ayuda a prevenir el uso no autorizado, la transferencia o el intercambio de datos sensibles a través de aplicaciones, servicios y dispositivos.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.



Forcepoint On-Premise Security

Versión 8.5

Fabricante Forcepoint

Familia Sistemas para prevención de fugas de datos

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/05/2021

Revisión de Validez 28/02/2026

Descripción

Los dispositivos Forcepoint Web Security realizan la función de proxy de navegación segura integrando múltiples motores de clasificación de contenidos y análisis de seguridad en tiempo real con capacidad de inspección de tráfico seguro y también análisis de datos salientes con capacidad para aplicar políticas frente a fugas de información. Las plataformas funcionan como proxies directos http, https, ftp y SOCKS para la protección y control de usuarios y puestos de conexión. El propósito de estos dispositivos es proporcionar una capa de seguridad entre la red Interna y una o más redes externas (típicamente una red corporativa e Internet), aislando el tráfico de los usuarios a nivel de aplicación y proporcionando además diferentes mecanismos de optimización WAN para el tráfico que procesan.

Observaciones

CCN-STIC-1507 Procedimiento de Empleo Seguro Forcepoint On-premise Security 8.5



INFORMACIÓN IMPORTANTE

7.6.5 HERRAMIENTAS PARA FIRMA ELECTRÓNICA

Cryptomathic Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0

Versión	6.0
Fabricante	Cryptomathic S/A
Familia	Herramientas para firma electrónica
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/11/2024
Revisión de Validez	30/04/2025



Descripción

Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0 constituye la última innovación de Cryptomathic en soluciones rQSCD/rQSealCD. Este rQSCD, certificado Common Criteria EAL4+ AVA_VAN 5, está diseñado para satisfacer los requisitos de los entornos más exigentes en términos de privacidad y seguridad. Con cumplimiento de eIDAS 2.0, Signer SAM v6.0 está también preparado para garantizar la conformidad con el perfil de seguridad de nivel financiero de la API (FAPI 2) y con el estándar CSC v2. El Signer SAM v6.0 es un sistema confiable que proporciona el servicio de firmas y sellos digitales remotos. Asegura que las claves de firma de cada usuario firmante se utilicen exclusivamente bajo su control y únicamente para los fines previstos, es decir, la generación de firmas o sellos remotos cualificados. Las funcionalidades y características de seguridad del Signer SAM v6.0 están diseñadas específicamente para proteger estas operaciones, a los usuarios firmantes y a las claves empleadas en la generación de las firmas o sellos. Respaldo por el HSM CP5 de Utimaco, también certificado CC EAL4+, Signer SAM v6.0 destaca por su cumplimiento más estricto de las normativas del sector.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Ascertia ADSS Server Signature Activation Module (SAM)

Versión	7.0
Fabricante	Ascertia Limited
Familia	Herramientas para firma electrónica
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2022
Revisión de Validez	01/11/2025

**Descripción**

El ADSS SAM v.7.0.2 es el nuevo rQSCD/rQSealCD de Ascertia certificado Common Criteria EAL4+ EN 419 241-2 (SCAL2).

El ADSS SAM v.7.0.2 cumple con los estándares FIPS 140-2 Level 3, EN 419 241-1 & 2 (SCAL1 & SCAL2), EN 419 221-5, TS 119 431-1, TS 119 431-2, TS 119 432 y Cloud Signature Consortium (CSC).

Este nuevo rQSCD/rQSealCD da respuesta a las necesidades más exigentes de seguridad y confianza que necesitan los Proveedores de Servicios de Confianza Cualificados, proporcionando un alto rendimiento y una alta disponibilidad para la emisión de sellos de tiempo cualificados, de firma digital remota cualificada (reconocida) y de sello electrónico corporativo cualificado. El ADSS SAM v.7 también está disponible en modo "software only" para satisfacer los requerimientos de los Proveedores de Servicios de Confianza Avanzados.

El ADSS SAM v.7.0.2 destaca por su gran flexibilidad, resiliencia y escalabilidad; todo ello combinado con una seguridad interna bien diseñada que facilita su administración, su auditoría y la generación de informes que cumplen con los requerimientos ETSI/CEN para sistemas de Alta Confianza. Es compatible su uso con HSMs de red externos de los 3 principales fabricantes que hayan sido certificados EN 419 221-5.

Observaciones

N/A

INFORMACIÓN IMPORTANTE

SIAVAL Safecert Server Signing Sistema

Versión	v.3
Fabricante	Sistemas Informáticos Abiertos
Familia	Herramientas para firma electrónica
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	01/03/2025

SIA

An Indra company



Descripción

Solución de firma centralizada de la familia SIAVAL orientada a facilitar la gestión y el uso de las claves privadas y públicas de los usuarios finales, también identificados como titulares o firmantes. Está diseñado para funcionar como un dispositivo remoto de creación de firma rQSCD, según los requisitos especificados en el Reglamento (UE) nº 910/2014 del Parlamento Europeo (eIDAS: Anexo II), haciendo posible la generación de firmas electrónicas avanzadas (AdES) y de firmas electrónicas cualificadas o reconocidas (QES) en un servidor remoto.

Observaciones

Procedimiento de empleo pendiente de publicación

Tarjeta Criptográfica TC-FNMT

Versión	5.6
Fabricante	FNMT-RCM
Familia	Herramientas para firma electrónica
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	18/01/2024
Revisión de Validez	31/12/2024



Descripción

La TC-FNMT es una tarjeta criptográfica con la capacidad de realizar firmas electrónicas. Está compuesto de un chip previamente certificado (que proporciona la librería criptográfica y el firmware con el loader para la actualización del código), el sistema operativo y las librerías biométricas. Esta tarjeta implementa un sistema de ficheros que incluye la siguiente aplicación:

- eSign (aplicación de firma [TR03110-2] conforme a los perfiles de protección BSI-CC-PP-0059-2009-MA-01, BSI-CC-PP-0075, BSI-CCPP-0071, BSI-CC-PP-0072 Y BSI-CC-PP-0076.

Además del cumplimiento de los requisitos en la funcionalidad de firma electrónica, la TC-FNMT v5.6 también cumple con los requisitos del Reglamento (UE) nº 910/2014 (eIDAS) en materia de identificación electrónica, requisitos derivados de la Decisión de Ejecución (UE) 2016/650 de la Comisión de 25 de abril de 2016 por la que se fijan las normas para la evaluación de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2 del Reglamento eIDAS.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.6.6 HARDWARE SECURITY MODULE (HSM)

Thales Luna K7 Cryptographic Module	
Versión	7.7.1
Fabricante	Thales
Familia	Hardware Security Module (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	11/12/2024
Revisión de Validez	31/05/2025
Descripción	
	N/A
Observaciones	
	Procedimiento de empleo seguro pendiente de publicación

THALES
Building a future we can all trust



Thales Luna K7 Cryptographic Module	
Versión	7.7.2
Fabricante	Thales
Familia	Hardware Security Module (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	11/12/2024
Revisión de Validez	31/05/2025
Descripción	
	N/A
Observaciones	
	Procedimiento de empleo seguro pendiente de publicación

THALES
Building a future we can all trust



INFORMACIÓN IMPORTANTE

Thales Luna K7 Cryptographic Module

Versión	7.7.0
Fabricante	Thales
Familia	Hardware Security Module (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	11/12/2024
Revisión de Validez	31/05/2025

Descripción

N/A

Observaciones

Procedimiento de empleo seguro pendiente de publicación

THALES
 Building a future we can all trust


Thales Luna K7 Cryptographic Module (808-000048-002, 808-000073-001, 808-000066-001, 808-000069-001 y 808-000070-001)

Versión	7.7.0 (bootloader versions 1.1.1, 1.1.2 y 1.1.4)
Fabricante	Thales
Familia	Hardware Security Module (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	31/03/2026

Descripción

Los Módulos de Seguridad Hardware (HSM) de Thales, son criptoprocesadores dedicados que están diseñados específicamente para la protección del ciclo de vida de las claves criptográficas. La administración, el procesamiento y el almacenamiento de claves criptográficas se realiza dentro del dispositivo reforzado a prueba de manipulaciones, aumentando el rendimiento y manteniendo la seguridad. Con los módulos de seguridad de hardware de Thales, puede: - Abordar los requisitos de cumplimiento con soluciones para Blockchain, GDPR, IoT, iniciativas de papel a digital, PCI DSS, firmas digitales, eIDAS, DNSSEC, almacenamiento de claves en hardware, aceleración transaccional, firma de certificados, firma de código o documentos, generación de claves masivas, cifrado de datos y más. - Las claves siempre se generan y almacenan en el dispositivo validado a prueba de intrusiones y manipulaciones, que proporciona los niveles más altos de control de acceso. - Posibilidad de crear particiones lógicas en los HSM de red, con Oficiales de Seguridad dedicados por partición, y segmentando la gestión con una separación total de las claves.

Observaciones

Solicitar al fabricante la guía de configuración utilizada en la certificación Common Criteria. Configurar el producto para la utilización de funciones, algoritmos y protocolos aprobados por el Centro Criptológico Nacional, según la guía CCN-STIC-807 Criptología de empleo en el ENS

THALES
 Building a future we can all trust
**INFORMACIÓN IMPORTANTE**

Azure Managed HSM

Versión

Fabricante Microsoft

Familia Hardware Security Module (HSM)

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 25/10/2024

Revisión de Validez 31/03/2025



Descripción

Azure Key Vault Managed HSM (Hardware Security Module) es un servicio en la nube de Microsoft totalmente gestionado por el cliente que permite proteger las claves criptográficas para aplicaciones en la nube utilizando HSMs validados por FIPS 140-2 Nivel 3.

Este servicio ofrece gestión centralizada de claves, alta disponibilidad mediante múltiples particiones de HSM, control de acceso granular y monitorización y auditoría integradas con Azure Monitor.

Es ideal para organizaciones que requieren un alto nivel de seguridad y control sobre sus claves criptográficas, especialmente en sectores con estrictos requisitos de cumplimiento.

Azure Key Vault Managed HSM permite tener control total y exclusivo sobre quién puede acceder a las claves y cambiar las políticas de gestión de claves, asegurando que el personal de Microsoft no pueda intervenir.

Observaciones

Proceso de Empleo Seguro pendiente de publicación.

nShield Solo XC Hardware Security Module

Versión v12.60.15

Fabricante Entrust Solutions

Familia Hardware Security Module (HSM)

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/11/2021

Revisión de Validez 30/04/2025



Descripción

Los módulos de seguridad hardware (HSM) nShield XC son dispositivos físicos con certificación FIPS 140-2 nivel 3 y Common Criteria EAL4+ (EN 419 221-5) que permiten realizar operaciones criptográficas de forma segura. A su vez, el diseño de estos equipos, ofrece una serie de funcionalidades que facilita la gestión de material criptográfico: - Protección prácticamente ilimitada de claves privadas. - Flexibilidad en la creación de copias de seguridad de las claves al no necesitar equipos adicionales ni acceso directo a los HSM. - Capacidad de ejecutar código dentro del HSM mediante CodeSafe. Desde un punto de vista funcional, los HSM nShield XC son plataformas resistentes a la manipulación (tamper resistant) que realizan de forma segura funciones de generación y protección de claves y firma digital para una gran variedad de aplicaciones, como: - Autoridades de certificación - Procesos de negocio - Firma de código - Servicios en la nube - Blockchain privadas y públicas - Establecimiento de comunicaciones seguras

Observaciones

Solicitar al fabricante la guía de configuración utilizada en la certificación Common Criteria. Configurar el producto para la utilización de funciones, algoritmos y protocolos aprobados por el Centro Criptológico Nacional, según la guía CCN-STIC-807 Criptología de empleo en el ENS

INFORMACIÓN IMPORTANTE

CryptoServer CP5

Versión	5.1.0.0
Fabricante	UTIMACO
Familia	Hardware Security Module (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	31/12/2024


**Descripción**

Los Módulos de Seguridad Hardware (HSM) UTIMACO constituyen la raíz de confianza ideal para proteger activos sensibles críticos para la seguridad en empresas y administraciones públicas, con casos de uso en finanzas, automoción, IoT, infraestructuras críticas, telecomunicaciones y proveedores de servicios.

CryptoServer CP5 es el HSM certificado para la generación y almacenamiento de Certificados Cualificados para firmas y sellos electrónicos que cuenta con la Certificación Common Criteria acorde al Protection Profile eIDAS EN 419221-5 “Módulo Criptográfico para Servicios de Confianza”.

CryptoServer CP5 dispone de funcionalidades de autorización de clave para creación de firmas cualificadas y firmas remotas compatibles con eIDAS. Otras áreas de aplicación incluyen la emisión de certificados cualificados OCSP y sellado de tiempo.

Características relevantes:

- Almacenamiento y procesamiento seguro de claves dentro de los límites seguros del HSM
- Autenticación de doble factor con tarjetas inteligentes
- Control de acceso basado en roles configurable
- Gestión remota
- Simulador software para evaluación y pruebas.
- En formato appliance y tarjeta PCIe
- Certificaciones FIPS 140-2 nivel 3 y Common Criteria EAL4+ (EN 419 221-5)

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

7.6.7 GESTIÓN DE METADATOS

MetaClean Sync Workstation y MetaClean Sync Server

Versión 2.3.0

Fabricante Adarsus Technologies S.L

Familia Gestión de metadatos

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/11/2023

Revisión de Validez 30/04/2026

Descripción

MetaClean Sync Workstation y MetaClean Sync Server: Herramienta de gestión de metadatos que permite aplicar políticas de seguridad corporativas de prevención de fugas de información, limpiando los metadatos e información sensible oculta en los ficheros ofimáticos generados en una organización.

Realiza una protección continua y en tiempo real de los metadatos de una estación de trabajo o Servidor. Protege la información de manera sencilla y desatendida. Permite configurar reglas y ponerlas en práctica sobre los archivos documentales o multimedia que se considere necesario, ya sea en los equipos de usuario -Workstation- o en carpetas de red compartidas -Server-.

Observaciones

CCN-STIC 1511 Procedimiento de Empleo Seguro metaOLVIDO EndPoint y metaOLVIDO Server



MetaClean Dashboard

Versión 1.3.0

Fabricante Adarsus Technologies S.L

Familia Gestión de metadatos

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/11/2023

Revisión de Validez 30/04/2026

Descripción

MetaClean Dashboard: Consola de administración de MetaClean para las distintas modalidades de despliegue. Administra, centraliza y controla la aplicación de políticas preventivas de seguridad corporativas. Permite obtener estadísticas de los metadatos procesados y controlar la exfiltración de información de forma global.

Observaciones

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard



INFORMACIÓN IMPORTANTE

7.7 PROTECCIÓN DE EQUIPOS Y SERVICIOS

7.7.1 DISPOSITIVOS MÓVILES

Lenovo Tab M8 4th Gen (TB300XU)

Versión	Android 12
Fabricante	Lenovo
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	25/04/2023
Revisión de Validez	30/11/2024



Descripción

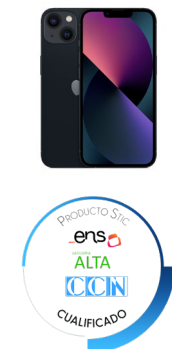
Lenovo Tab M8 4th Gen (TB300XU_S000111_230408_ROW) es una Tablet basada en Android con una pantalla de 8" HD y una batería que extenderá el uso de esta hasta 15 horas. Con conectividad LTE Cat7, Wi-Fi 5 Certified y BT 5.0. Dos altavoces con certificación Dolby. Todo ello con un peso de 318 gr.

Observaciones

CCN-STIC 1639 Procedimiento de empleo seguro Lenovo Tab M8 4th Gen

iPhone 13

Versión	iOS17
Fabricante	Apple
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	15/10/2024
Revisión de Validez	01/09/2026



Descripción

El iPhone 13 basado en el chip de Apple A15 Bionic, combina hardware, software y servicios que se han diseñado para funcionar conjuntamente con el fin de proporcionar seguridad y una experiencia de usuario transparente. El hardware de seguridad y el chip diseñados por Apple potencian las funciones de seguridad críticas. Además, las protecciones de software funcionan para mantener la seguridad del sistema operativo y de las apps de terceros. Los servicios proporcionan un mecanismo para disponer de actualizaciones de software seguras y oportunas, respaldar un ecosistema de apps protegido y facilitar comunicaciones y pagos seguros.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

iPhone 14Pro, 14 Pro Max

Versión	iOS17
Fabricante	Apple
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	15/10/2024
Revisión de Validez	01/09/2027

**Descripción**

El iPhone 14 Pro y el iPhone 14 Pro Max basados en el chip de Apple A16 Bionic, combina hardware, software y servicios que se han diseñado para funcionar conjuntamente con el fin de proporcionar seguridad y una experiencia de usuario transparente. El hardware de seguridad y el chip diseñados por Apple potencian las funciones de seguridad críticas. Además, las protecciones de software funcionan para mantener la seguridad del sistema operativo y de las apps de terceros. Los servicios proporcionan un mecanismo para disponer de actualizaciones de software seguras y oportunas, respaldar un ecosistema de apps protegido y facilitar comunicaciones y pagos seguros.

Observaciones

Procedimiento de empleo pendiente de publicación

iPhone 15, 15 Plus

Versión	iOS17
Fabricante	Apple
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	15/10/2024
Revisión de Validez	01/09/2028

**Descripción**

El iPhone 15 y el iPhone 15 Plus basados en el chip de Apple A16 Bionic, combina hardware, software y servicios que se han diseñado para funcionar conjuntamente con el fin de proporcionar seguridad y una experiencia de usuario transparente. El hardware de seguridad y el chip diseñados por Apple potencian las funciones de seguridad críticas. Además, las protecciones de software funcionan para mantener la seguridad del sistema operativo y de las apps de terceros. Los servicios proporcionan un mecanismo para disponer de actualizaciones de software seguras y oportunas, respaldar un ecosistema de apps protegido y facilitar comunicaciones y pagos seguros.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

iPhone 14, 14 Plus

Versión	iOS17
Fabricante	Apple
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	15/10/2024
Revisión de Validez	01/09/2027

**Descripción**

El iPhone 14 y el iPhone 14 Plus basados en el chip de Apple A15 Bionic, combina hardware, software y servicios que se han diseñado para funcionar conjuntamente con el fin de proporcionar seguridad y una experiencia de usuario transparente. El hardware de seguridad y el chip diseñados por Apple potencian las funciones de seguridad críticas. Además, las protecciones de software funcionan para mantener la seguridad del sistema operativo y de las apps de terceros. Los servicios proporcionan un mecanismo para disponer de actualizaciones de software seguras y oportunas, respaldar un ecosistema de apps protegido y facilitar comunicaciones y pagos seguros.

Observaciones

Procedimiento de empleo pendiente de publicación

Samsung Galaxy Tab Active 5 (SM-X300 | SM-X306B)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	31/01/2032

**Descripción**

Galaxy Tab Active 5 es una tableta ruggedizada basada en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android 14

INFORMACIÓN IMPORTANTE

Samsung Galaxy Tab S8 (SM-X706B/X700), Tab S8+ 5G (SM-X806B/X800), Tab S8 Ultra (SM-X906B/X900)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	12/01/2027

**Descripción**

La familia de dispositivos de la gama TAB S8 son tabletas empresariales basada en Android que incorpora la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basados en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android 14

Samsung Galaxy Tab Active4 Pro (SM-T636 / SM-T630)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	01/08/2027

**Descripción**

Galaxy Tab Active 4 Pro es una tableta ruggedizada basada en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android 14

INFORMACIÓN IMPORTANTE

Samsung Galaxy XCover6 Pro (SM-G736B)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	01/07/2027

**Descripción**

Galaxy Xcover6 Pro son dispositivos empresariales ruggedizados basados en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android 14

Samsung Galaxy S24 5G (SM-S921B), Galaxy S24+ 5G (SM-S926B), Galaxy S24 Ultra 5G (SM-S928B)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	31/01/2031

**Descripción**

La familia de dispositivos de la gama Galaxy S24 5G son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android 14

INFORMACIÓN IMPORTANTE

Samsung Galaxy S21 5G (SM-G991B), S21+ 5G (SM-G996B), S21 Ultra+ 5G (SM-G998B) ,S21 5G FE (SM-G990B)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	28/01/2026



Descripción

La familia de dispositivos de la gama Galaxy S21 son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android 14

Samsung Galaxy S22 5G (SM-S901B), S22+ 5G (SM-S906B), S22 Ultra 5G (SM-S908B)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	21/01/2027



Descripción

La familia de dispositivos de la gama Galaxy S22 son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basado en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android 14

INFORMACIÓN IMPORTANTE

Samsung Galaxy S23 5G (SM-S911B), S23+ 5G (SM-S916B), S23 Ultra 5G (SM-S918B), S23 FE (SM-S711B)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	31/12/2026

**Descripción**

La familia de dispositivos de la gama Galaxy S23 5G son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android 14

Samsung Galaxy Z Fold4 5G (SM-F936B)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	01/08/2027

**Descripción**

La familia de dispositivos de la gama Galaxy Z Fold4 son dispositivos empresariales plegables basados en Android que incorpora la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basados en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android14

INFORMACIÓN IMPORTANTE

Samsung Galaxy Z Flip4 5G (SM-F721B)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	07/08/2027

**Descripción**

La familia de dispositivos de la gama Galaxy Z Flip 4 son dispositivos empresariales plegables basados en Android que incorpora la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basados en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android14

Samsung Galaxy Z Flip5 5G (SM-F731B)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	31/05/2026

**Descripción**

La familia de dispositivos de la gama Galaxy Z Flip 5 son dispositivos empresariales plegables basados en Android que incorpora la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basados en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android14

INFORMACIÓN IMPORTANTE

Samsung Galaxy Tab S9 (SM-X716B | SM-X710), Tab S9+ (SM-X816B/SM-X810), Tab S9 Ultra (SM-X916B/SMX-910)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	31/05/2026



Descripción

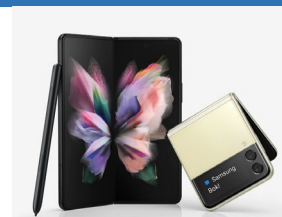
La familia de dispositivos de la gama TAB S9 son tabletas empresariales basada en Android que incorpora la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basados en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android14

Samsung Galaxy Z Fold3 5G (SM-F926B)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	16/08/2026



Descripción

La familia de dispositivos de la gama Galaxy Z son dispositivos empresariales plegables basados en Android que incorpora la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basados en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android14

INFORMACIÓN IMPORTANTE

Samsung Galaxy Z Fold5 5G (SM-F946B)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	31/05/2026

**Descripción**

La familia de dispositivos de la gama Galaxy Z Fold 5 son dispositivos empresariales plegables basados en Android que incorpora la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basados en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android14

Samsung Galaxy A53 5G (SM-A536B)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	01/03/2027

**Descripción**

Galaxy A53 5G son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basado en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1631 PES Samsung Galaxy Android 13

INFORMACIÓN IMPORTANTE

Samsung Galaxy A52 5G (SM-526B)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	18/12/2023
Revisión de Validez	10/02/2025

**Descripción**

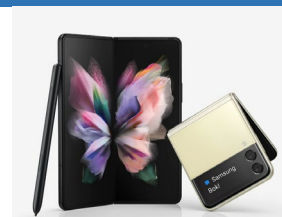
El modelo Galaxy A52 5G es un teléfono móvil basado en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1631 PES Samsung Galaxy Android13

Samsung Galaxy Z Flip3 5G (SM-F711B)

Versión	Android 14
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	13/08/2026

**Descripción**

La familia de dispositivos de la gama Galaxy Z son dispositivos empresariales plegables basados en Android que incorpora la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basados en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

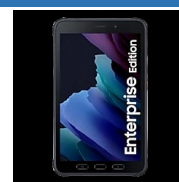
Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android 14

INFORMACIÓN IMPORTANTE

Samsung Galaxy Tab Active 3 (SM-T575 | SM-T570)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	18/12/2023
Revisión de Validez	31/05/2026

**Descripción**

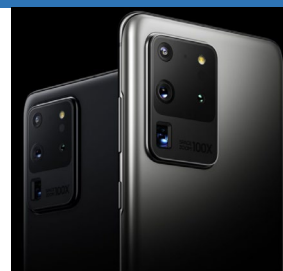
Galaxy Tab Active 3 es una tableta ruggedizada basada en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1631 PES Samsung Galaxy Android13

Samsung Galaxy S20+ 5G (SM-G986B), S20 5G (SM-G981B), S20 Ultra 5G (SM-G988B), S20+ 4G (SM-G985F), S20 4G (SM-G980F)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2020
Revisión de Validez	24/01/2025

**Descripción**

La familia de dispositivos de la gama Galaxy S20 son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Fecha fin de soporte prevista:

- SM-G986B Enterprise Edition: 24/01/2025
- SM-G986B: 24/01/2024
- SM-G981B: 24/01/2024
- SM-G988B: 24/01/2024
- SM-G985F Enterprise Edition: 24/01/2025
- SM-G985F: 24/01/2024
- SM-G980F Enterprise Edition: 24/01/2025
- SM-G980F: 24/01/2024

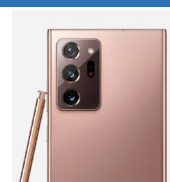
Observaciones

CCN-STIC 1631 PES Samsung Galaxy Android 13

INFORMACIÓN IMPORTANTE

Samsung Galaxy Note20 4G (SM-N980F), Note20 5G (SM-N981B), Note20 Ultra 5G (SM-N986B)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	24/08/2025

**Descripción**

La familia de dispositivos de la gama Galaxy Note20 son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1631 PES Samsung Galaxy Android 13

Sotera Phone H1U

Versión	0.455
Fabricante	Sotera Digital Security Corporation
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2024
Revisión de Validez	31/01/2027

**Descripción**

El SecurePhone es un teléfono móvil de propiedad exclusiva de Sotera que funciona con el sistema operativo INTEGRITY. El SecurePhone permite que se realicen comunicaciones de voz y texto seguras en cualquier lugar del mundo y utilizando cualquier red pública, brindando privacidad a sus usuarios. Diseñado con la idea de brindar un nivel único de protección, el SecurePhone fue fabricado desde cero con el propósito de proteger su hardware, software y aplicaciones de mensajería contra ciberataques sofisticados. Para más detalles, visitar www.soteradigital.com/es.

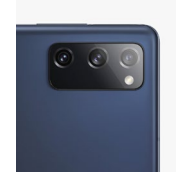
Observaciones

CCN-STIC-1640 Procedimiento de empleo seguro Sotera Phone H1U

INFORMACIÓN IMPORTANTE

Samsung Galaxy S20 FE 4G (SM-G780F), S20 FE 5G (SM-G781B)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	17/10/2025

**Descripción**

La familia de dispositivos de la gama Galaxy S20 FE son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1631 PES Samsung Galaxy Android 13

INFORMACIÓN IMPORTANTE

7.7.2 SISTEMAS OPERATIVOS

SUSE Linux Enterprise Server

Versión	Version 15 SP4
Fabricante	SUSE Software Solutions Germany GmbH
Familia	Sistemas Operativos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2024
Revisión de Validez	30/06/2026



Descripción

SUSE® Linux Enterprise Server (SLES) 15 SP4 es un sistema operativo (SO) modular que ayuda a simplificar el entorno IT, modernizar la infraestructura IT y acelerar la innovación. SLES se adapta a cualquier entorno operativo a la vez que satisface los requisitos de rendimiento, seguridad y confiabilidad. Es una plataforma fácil de administrar para desarrolladores y administradores que permite implementar cargas de trabajo críticas para el negocio en las instalaciones, en la nube y en el perímetro.

Observaciones

CCN-STIC 1615 Procedimiento de Empleo Seguro SUSE 15 SP4

Windows Server 2016

Versión	Datacenter Edition
Fabricante	Microsoft Corporation
Familia	Sistemas Operativos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2018
Revisión de Validez	12/01/2027



Descripción

Sistema Operativo para servidores

Observaciones

CCN-STIC-570A, CCN-STIC-570B Anexo A

INFORMACIÓN IMPORTANTE

SUSE Linux Enterprise

Versión	Server 15 SP2
Fabricante	SUSE Software Solutions
Familia	Sistemas Operativos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2021
Revisión de Validez	31/12/2024

**Descripción**

SUSE® Linux Enterprise Server (SLES) 15 SP2 es un sistema operativo (SO) modular que ayuda a simplificar el entorno IT, modernizar la infraestructura IT y acelerar la innovación. SLES se adapta a cualquier entorno operativo a la vez que satisface los requisitos de rendimiento, seguridad y confiabilidad. Es una plataforma fácil de administrar para desarrolladores y administradores que permite implementar cargas de trabajo críticas para el negocio en las instalaciones, en la nube y en el perímetro.

Observaciones

CCN-STIC-1615 Procedimiento de empleo seguro SUSE 15 SP2

INFORMACIÓN IMPORTANTE

7.7.3 PROTECCIÓN DE CORREO ELECTRÓNICO

Microsoft Defender for Office 365 (Email Protection)

Versión
Fabricante Microsoft Iberica SRL

Familia Protección de correo electrónico

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/04/2023

Revisión de Validez 31/03/2025

Descripción

Microsoft Defender para Office 365 es una solución de seguridad en la nube que protege el correo electrónico en Office365 o en local y los servicios de Office 365 (Microsoft Teams, SharePoint, OneDrive y aplicaciones de Office) contra amenazas como phishing, malware, spam y compromiso de correo electrónico empresarial. También ofrece herramientas para educar a los empleados sobre cómo detectar correos electrónicos de phishing y protege contra descargas de archivos maliciosos a través de navegadores web. Además, utiliza tecnologías para bloquear remitentes no deseados y analiza el contenido de los correos electrónicos para detectar y bloquear contenido inapropiado o no deseado. En resumen, Microsoft Defender para Office 365 es una solución completa y efectiva para proteger a las empresas de las amenazas de correo electrónico y servicios de Office 365 (Microsoft Teams, SharePoint, OneDrive y aplicaciones de Office).

Observaciones

CCN-STIC 1629-Procedimiento de Empleo Seguro MS Defender for Office 365.

INFORMACIÓN IMPORTANTE

Email Guardian

Versión	2.5.7
Fabricante	Iberlayer
Familia	Protección de correo electrónico
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	16/12/2024
Revisión de Validez	31/05/2025



Descripción

Iberlayer Email Guardian es una solución de protección integral para el correo electrónico desde la nube. Proporciona una capa avanzada de seguridad que protege las comunicaciones corporativas contra una amplia gama de ciber-amenazas, como Fraudes, Fake News, Phishing, Spam, Scam, Malware, y APTs entre otros. El servicio ofrece una solución completa de seguridad que bloquea los correos electrónicos maliciosos antes de que lleguen a la bandeja de entrada del usuario. Utiliza técnicas avanzadas de filtrado y análisis, que incluyen capacidades como control de SPF, DKIM, ARC y DMARC, inspección de adjuntos cifrados, el análisis detallado y seguimiento de las URLs en los mensajes y archivos adjuntos, parseo de códigos QR y códigos de barras (incluso en videos), integración cifrada con SIEMs, Parches virtuales, detección de criptomonedas fraudulentas, seguimiento de conversaciones, etc. También detecta la creación de dominios sospechosos, realiza simulaciones de errores y ofrece protección específica contra fraudes dirigidos (con o sin BEC) como fraudes de CEO, fraudes de nóminas, fraudes en cambios de cuentas bancarias, fraudes de clonado de tarjetas SIM, y es capaz de detectar las comunicaciones con servidores de comando y control (C&C) de bots y troyanos para bloquearlas y alertar sobre ellas.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

Harmony Email & Collaboration

Versión	
Fabricante	Check Point Software Technologies
Familia	Protección de correo electrónico
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/09/2024
Revisión de Validez	28/02/2025



Descripción

Check Point Harmony Email & Collaboration es una solución de seguridad avanzada que protege correo electrónico y aplicaciones de colaboración contra phishing, malware, ransomware, pérdida de datos y toma de control de cuentas. Con capacidades avanzadas de emulación y reescritura de URL, análisis dinámico de ficheros en sandbox, limpiado de documentos, análisis de anomalías, análisis de comprimidos con contraseña, códigos QR, o añadido de banners inteligentes, entre otros, utiliza inteligencia artificial y aprendizaje automático para bloquear amenazas avanzadas y accesos no autorizados, además de gestionar DMARC para prevenir suplantación de identidad. Está integrado de forma nativa con Check Point ThreatCloud AI de forma que se retroalimenta de toda la plataforma de inteligencia de Check Point.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Fortimail

Versión	7.4
Fabricante	Fortinet
Familia	Protección de correo electrónico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2024
Revisión de Validez	28/02/2025

FORTINET®**Descripción**

FortiMail protege a las organizaciones contra el espectro completo de amenazas basadas en correo electrónico, como suplantación de identidad, ransomware, ataques de día cero y ataques de compromiso de correo electrónico comercial (BEC). Aprovecha los servicios de seguridad impulsados por IA de FortiGuard desarrollados por FortiGuard Labs, que proporcionan tecnología de seguridad de vanguardia para prevenir, detectar y responder a amenazas basadas en correo electrónico en tiempo real.

Mas información: <https://docs.fortinet.com/product/fortimail/7.4>

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

Proofpoint Email Protection & Targeted Email Protection

Versión	
Fabricante	Proofpoint, Inc.
Familia	Protección de correo electrónico
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	31/10/2025

proofpoint.**Descripción**

Proofpoint Email Protection (PPS+TAP) es una solución avanzada de Protección del Correo Electrónico. Con su aproximación centrada en las personas, permite a las organizaciones proteger a los usuarios de las amenazas que llegan por el correo electrónico, tanto las más básicas como campañas de spam y correo masivo, suplantaciones de identidad (BEC), phishing o malware, así como aquellas más avanzadas que necesitan de un análisis estático y dinámico de ficheros adjuntos o enlaces web. Además, aprovecha toda la inteligencia de proteger el mayor vector de entrada de amenazas para ofrecer una visibilidad centrada en las personas del panorama de amenazas de cada cliente, proporcionando información detallada en tiempo real de los riesgos de los usuarios, las amenazas que reciben y los actores maliciosos que puedan estar atacando la organización.

Observaciones

CCN-STIC-1636-Procedimiento de Empleo Seguro de Proofpoint Email Protection y Targeted Attack Protection

INFORMACIÓN IMPORTANTE

Cisco Email Security Appliance (C190, C195, C390, C395, C690, C690X, C695, C695F, C100v, C300v y C600v)

Versión	AsyncOS 13.0
Fabricante	Cisco Systems
Familia	Protección de correo electrónico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	31/05/2025

**Descripción**

Cisco Email Security Appliance es una pasarela de seguridad para el correo electrónico. Está diseñado para detectar y bloquear una amplia variedad de amenazas transmitidas por correo electrónico, como malware, spam e intentos de phishing.

Observaciones

CCN-STIC 1623 Procedimiento de Empleo Seguro Cisco Email Security Appliance

INFORMACIÓN IMPORTANTE

7.7.4 BALANCEADORES DE CARGA

A10 Networks VThunder (vTH-1Gbps, vTH-4Gbps, vTH-8Gbps, vTH-10Gbps, vTH-20Gbps, vTH-40Gbps, vTH-100Gbps, FlexPool)

Versión	ACOS 5.2.1-P3
Fabricante	A10 Networks, Inc
Familia	Balanceadores de carga
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

A10



Descripción

A10 Networks Thunder Series Appliances es la familia de productos necesaria para asegurar la disponibilidad de servidores y aplicaciones, ayuda en la protección de aplicaciones vulnerables, optimiza y acelera la entrega de contenido. Basado en el sistema operativo ACOS, sistema de supercomputación que no utiliza memoria dedicada sino compartida, otorga una alta eficiencia en rendimiento de los equipos con una baja huella energética.

Disponible en las siguientes opciones:

Licencia ADC – Incluye balanceo de carga, GSLB, full-proxy, balanceo de líneas, presentación de aplicaciones https (SSL Offloading), autenticación, routing avanzado, aFlex para programación de opciones avanzadas, permite alta densidad de particiones en función del modelo llegando hasta 1023 particiones, renovación automática de certificados mediante protocolo ACME y protección AntiDDoS.

Licencia CGN – Añade opciones de CGNAT avanzadas y ayuda a la adopción de IPv6.

Licencia SSLi – Permite tener visibilidad al tráfico SSL para elementos de seguridad en la red de clientes y así descargarles de esa tarea computacionalmente costosa y reducir la latencia.

Licencia cFW – Añade capacidades de FW tipo stateful e incluye capacidad de VPN IPSec y proxy de navegación.

Observaciones

CCN-STIC-1635 Procedimiento de empleo seguro A10 Thunder

INFORMACIÓN IMPORTANTE

A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655, TH-940, TH-1040, TH-3350E, TH-3350, TH-4440 TH-5440, TH-5840, TH-5845, TH-6440, TH-6655S, TH-7440, TH-7440-11, TH-7650, TH-14045)

Versión	ACOS 5.2.1-P3
Fabricante	A10 Networks, Inc
Familia	Balanceadores de carga
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

A10



Descripción

A10 Networks Thunder Series Appliances es la familia de productos necesaria para asegurar la disponibilidad de servidores y aplicaciones, ayuda en la protección de aplicaciones vulnerables, optimiza y acelera la entrega de contenido. Basado en el sistema operativo ACOS, sistema de supercomputación que no utiliza memoria dedicada sino compartida, otorga una alta eficiencia en rendimiento de los equipos con una baja huella energética.

Disponible en las siguientes opciones:

Licencia ADC – Incluye balanceo de carga, GSLB, full-proxy, balanceo de líneas, presentación de aplicaciones https (SSL Offloading), autenticación, routing avanzado, aFlex para programación de opciones avanzadas, permite alta densidad de particiones en función del modelo llegando hasta 1023 particiones, renovación automática de certificados mediante protocolo ACME y protección AntiDDoS.

Licencia CGN – Añade opciones de CGNAT avanzadas y ayuda a la adopción de IPv6.

Licencia SSLi – Permite tener visibilidad al tráfico SSL para elementos de seguridad en la red de clientes y así descargarles de esa tarea computacionalmente costosa y reducir la latencia.

Licencia cFW – Añade capacidades de FW tipo stateful e incluye capacidad de VPN IPsec y proxy de navegación.

Observaciones

CCN-STIC-1635 Procedimiento de empleo seguro A10 Thunder

INFORMACIÓN IMPORTANTE

7.7.5 CASB

Microsoft Defender for Cloud Apps

Versión**Fabricante** Microsoft**Familia** CASB**Tipo** Servicio**Categoría ENS** ALTA**Fecha Inclusión** 10/12/2024**Revisión de Validez** 31/05/2025**Descripción**

Microsoft Defender for Cloud Apps proporciona protección integral para aplicaciones SaaS ayudando a monitorizar y proteger datos y aplicaciones en la nube mediante funcionalidades de CASB como el descubrimiento de Shadow IT, visibilidad en el uso de aplicaciones, protección contra amenazas basadas en aplicaciones y evaluaciones de protección de información y cumplimiento incluyendo características de gestión de la postura de seguridad SaaS (SSPM). Además, proporciona funcionalidades para la protección avanzada contra amenazas como parte de la solución XDR de Microsoft. Incluye funcionalidades para la correlación de señales y visibilidad de las cadenas de ataques y protección entre aplicaciones extendiendo los escenarios a aplicaciones que utilicen OAuth con permisos y privilegios para el acceso a datos y recursos críticos. Defender for Cloud Apps proporciona también una visión general de los riesgos del entorno. Proporciona funcionalidades para clasificar las aplicaciones descubiertas y capacidades para evaluar la postura de seguridad y cumplimiento de una organización mediante políticas de monitorización continua. Incluye funcionalidades de alertas y guiado para aplicar correcciones ante comportamientos anómalos como el acceso a ficheros, picos de uso inusuales y quién accede a ellos.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.7.6 HIPERCONVERGENCIA

HPE SimpliVity		
Versión	4.2.0.97	  
Fabricante	HPE	
Familia	Hiperconvergencia	
Tipo	Producto	
Categoría ENS	ALTA	
Fecha Inclusión	01/09/2024	
Revisión de Validez	28/02/2025	
Descripción	HPE SimpliVity es una plataforma hiperconvergente inteligente que optimiza las operaciones combinando infraestructura, servicios de datos avanzados y operaciones impulsadas por la IA en una única solución integrada. HPE SimpliVity reduce la complejidad y la sobrecarga para empresas que ejecutan cargas de trabajo de uso general. Su infraestructura y servicios de datos avanzados se integran en un solo bloque de creación escalable, lo que permite que los usuarios empiecen a pequeña escala y vayan ampliando a medida que lo necesiten. HPE SimpliVity simplifica y reduce la pila de TI eliminando los silos con resiliencia, copias de seguridad y recuperación ante desastres integradas. HPE SimpliVity reduce los dispositivos del centro de datos, genera ahorros de capacidad en producción y almacenamiento de copia de seguridad y contrae el TCO en comparación con la infraestructura tradicional.	
Observaciones	Procedimiento de Empleo Seguro pendiente de publicación	

INFORMACIÓN IMPORTANTE

KATUA SDI PLATFORM

Versión	1.0
Fabricante	KRC ESPAÑOLA S.A.
Familia	Hiperconvergencia
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	31/01/2025

**Descripción**

Katua®SDI Platform es una plataforma hiperconvergente escalable y segura, basada en el concepto Software Define Infrastructure, donde todos los elementos que conforman un CPD se definen en una única plataforma hardware y software. Permite el despliegue rápido de servicios (xaaS), consolidación de CPDs, SDN y tiene capacidad de instalación desde equipos móviles hasta grandes centros de procesos de datos. Su flexibilidad permite que se puedan desplegar servicios cloud sobre la plataforma de forma sencilla y eficiente. Dispone de la capacidad para generar bibliotecas de sistemas preconfigurados para su despliegue con un click a través de su interfaz web. Las capacidades de optimización del hipervisor aseguran un rendimiento máximo de la plataforma, haciendo uso de todos los recursos disponibles y ofreciendo de esta forma capacidad de instalación en nodos pequeños y configuraciones hardware básicas. Su capacidad para integrarse con sistemas de almacenamiento masivos, ya sean locales o remotos permite escalar la solución en función de las necesidades. Para más información de la plataforma, vista nuestra web <https://www.krc.es>

Observaciones

CCN-STIC-1610 Procedimiento de Empleo Seguro KATUA SDI Platform

INFORMACIÓN IMPORTANTE

7.7.7 HERRAMIENTAS DE VIDEOIDENTIFICACIÓN

Veridas Identity verification Platform

Versión	2024-01
Fabricante	Veridas Digital Authentication Solutions, S.L.
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	30/08/2024
Revisión de Validez	31/07/2026

VeriDas



Descripción

Solución biométrica de verificación digital de la identidad consistente en una validación del documento acreditativo de la identidad presentado (DNI, pasaporte, etc.), una comparación biométrica entre la foto incluida en el documento y un selfie de la persona que realiza el proceso, una prueba de vida activa y un proceso de vídeo identificación. Adicionalmente, la solución también incluye una herramienta de monitorización preparada para la revisión manual de todos los procesos realizados por parte de un agente.

A través de todos estos pasos, Veridas es capaz de verificar, de manera completamente automática, la identidad de la persona que realiza este proceso en remoto. Toda la tecnología incluida en la solución, sin excepción, ha sido diseñada y producida por Veridas, apostando por la privacidad por defecto y desde el diseño como un pilar fundamental.

Observaciones

CCN-STIC-1619 Procedimiento de Empleo Seguro Veridas Identity Verification Service

TrustCloud VideoID

Versión	4.0
Fabricante	TrustCloud VideoID
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	18/12/2024
Revisión de Validez	31/05/2025

TrustCloud



Descripción

TrustCloud VideoID es una solución SaaS de video identificación segura que permite a las empresas verificar la identidad de sus clientes de forma remota y en tiempo real, a través de llamadas automáticas o asistidas. La tecnología ofrece múltiples capas de autenticación, garantizando seguridad, fluidez y una experiencia de usuario óptima tanto para las empresas como para sus clientes.

TrustCloud, como Prestador Cualificado de Servicios Electrónicos de Confianza conforme al reglamento eIDAS, asegura el cumplimiento de la regulación española Orden Ministerial ETD/743/2022 con esta solución de video identificación. Toda la tecnología ha sido desarrollada internamente por TrustCloud, con sesiones ágiles de 150 segundos en promedio para llamadas automáticas y 210 segundos para llamadas asistidas.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Signaturit VideoID by Ivnosys

Versión	v1.0
Fabricante	IVNOSYS SOLUCIONES
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/07/2023
Revisión de Validez	26/06/2025

**Descripción**

Signaturit VideoID by Ivnosys', es una solución API desarrollada por IVNOSYS SOLUCIONES, SLU (Grupo Signaturit), que realiza procesos desasistidos (o asíncronos) de video identificación de individuos, para onboarding remoto y para identificación de solicitantes de certificados electrónicos cualificados (conforme la Orden ETD/465/2021, de 6 de mayo), utilizando el componente biométrico de la herramienta "Veridas Identity Verification Service".

Permite generar y gestionar procesos de video identificación y proceder mediante intermediación manual de un operador si lo requiere la norma, a la validación o el rechazo de las identificaciones en función de las evidencias biométricas recabadas (imágenes, videos) y scores procesados por Veridas.

Está constituido por dos componentes: 'Signaturit VideoID API', que permite realizar integraciones de forma sencilla y adaptarse a paneles de terceros con personalización propia, garantizando la configuración requerida por la normativa aplicable al caso de uso, y 'Signaturit VideoID Gateway', aplicación web que despliega la funcionalidad necesaria para realizar la video identificación de un individuo.

Observaciones

CCN-STIC-1638 Procedimiento de Empleo Seguro Signaturit VideoID

INFORMACIÓN IMPORTANTE

NebulaID Engine

Versión	2.0 con XpressID version V2
Fabricante	VINTEGRIS
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	21/11/2025

neBulaID

**Descripción**

neBulaID es la solución software desarrollada por VínTEGRIS que permite la ejecución de procesos de vídeo identificación para la emisión de certificados electrónicos cualificados.

neBulaID hace las funciones de Portal de Registro y está integrado en la solución SaaS nebulaSUITE desarrollada por VínTEGRIS, lo que permite la gestión del ciclo de vida de los certificados electrónicos y ofrece los servicios de firma electrónica avanzada y cualificada.

La solución combina diversos mecanismos de identificación biométrica y de autenticación multi factor, lo que la convierte en una opción válida para la obtención de certificados cualificados con validez legal. Este procedimiento permite a los usuarios verificar su identidad desde cualquier lugar por medio de un dispositivo electrónico con cámara, aportando la tranquilidad de estar cumpliendo con el reglamento europeo eIDAS y la regulación específica española (Orden Ministerial ETD/743/2022). Para vídeo identificarse, sólo se necesita de unos minutos y de la utilización del documento de identidad acreditativo del usuario.

Observaciones

CCN-STIC-1634 NebulaID Engine

INFORMACIÓN IMPORTANTE

Daon Identity Verification

Versión	1.16.4
Fabricante	Daon
Familia	Herramientas de videoidentificación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	18/12/2024
Revisión de Validez	31/05/2025

**Descripción**

Daon Identity Verification, combina varios componentes tecnológicos de última generación que permiten el máximo nivel de seguridad, la mejor experiencia de cliente y un tiempo optimizado de despliegue gracias a nuestra tecnología de orquestación sin código.

Su funcionalidad se basa en la captura de un selfi, junto con un documento de identidad válido. Ambos se comprueban y comparan para garantizar la coincidencia de las imágenes del sujeto y la incluida en el documento, además de aplicar diversos controles de forma ágil y transparente para el usuario.

También se lleva a cabo un conjunto de acciones basadas en algoritmos de Inteligencia Artificial, que incluyen procesos biométricos, prueba de vida pasiva, análisis para bloquear ataques de presentación, inyección o deepfakes, así como chequeos para detectar la alteración de documentos o intentos de fraude. La solución cuenta con la certificación ISO30107-3 iBeta Nivel 2.

Los documentos verificables incluyen DNI, pasaportes, carnés de conducir, permisos de residencia y otros documentos de identificación oficiales emitidos por más de 200 entidades soberanas. La solución de videoidentificación de Daon, además de la verificación automática de la identidad, también ofrece la revisión manual como opción desde una consola intuitiva y de fácil manejo.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Entrust VIRA

Versión	14.1.0 (VIRA) / 9.12.8 (JIRA)
Fabricante	Entrust Solutions
Familia	Herramientas de videoidentificación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2026



Descripción

Producto software que implementa la gestión segura de evidencias de video identificación obtenidas desde el Servicio de Verificación de la Identidad de Veridas. Entrust VIRA ha sido diseñado para cumplir con todas las medidas de seguridad aplicables a este tipo de productos, y para su uso en un QTSP que cumpla con la Orden Ministerial ETD/743/2022, de 26 de julio, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

El producto Entrust VIRA está basado en un caso de uso en el que el operador no está presente en el proceso de identificación (proceso desatendido). En este caso, el operador de video identificación no interacciona con el usuario que se debe identificar, sino que éste solo consulta y analiza las evidencias (imágenes, videos y resultados de las validaciones automáticas) previamente almacenadas en los sistemas de información de la plataforma. El operador accede al panel de control en el cual se muestran las evidencias necesarias para la aprobación, y aprueba o rechaza la identificación de la persona, basándose en el análisis de las evidencias.

Observaciones

No se considera necesaria la publicación del Procedimiento de Empleo Seguro asociado.

LOQR Platform

Versión	Backoffice 3.1, SDK 3.0
Fabricante	LOQR, SA
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/05/2024
Revisión de Validez	31/12/2024



Descripción

LOQR es una empresa de tecnología en el ámbito de la identidad digital. LOQR ofrece una plataforma que utiliza inteligencia artificial para ampliar y diversificar el perfil de los clientes que acceden a servicios digitales, con el objetivo de fortalecer a las organizaciones y acelerar su negocio digital. La Plataforma de LOQR proporciona flujos de trabajo (Journeys) de Verificación de Identidad y para mejorar la experiencia del cliente y proporcionar información única que pueda evolucionar hacia una transformación digital proactiva. La solución de LOQR cumple con todos los requisitos regulatorios y estándares de calidad.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

IQP VideoID and SelfID_BO products

Versión	V13.3.0
Fabricante	Infocert Spa
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	19/05/2023
Revisión de Validez	30/04/2025

**Descripción**

Remote-ID by InfoCert es un sistema de verificación de identidad remota que guía al sujeto en la toma de selfi y fotografías de su documento de identidad para que puedan ser procesados y comparados con su biometría facial y así verificar si es quien dice ser.

Hay dos procesos de identificación disponibles:

- asistido con operador (videoID)
- desasistido sin operador (selfID)

El resultado se pone a disposición de los operadores a través de la plataforma Identity Qualification Plaform, IQP, donde pueden llevar a cabo la revisión de las evidencias y así concluir la identificación del sujeto.

Los procesos han sido diseñados para cumplir con la Orden Ministerial ETD/743/2022, de 26 de julio, donde quedan regulados los métodos de identificación remota para la emisión de certificados electrónicos cualificados.

La solución se puede contratar a través de AC Camerfirma S.A.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Inetum Digital Onboarding

Versión	1.0
Fabricante	INETUM
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/09/2023
Revisión de Validez	30/09/2025

**Descripción**

Producto en modalidad SaaS que implementa la video-identificación para el procedimiento que debe seguirse en la identificación remota por vídeo de un ciudadano. Este servicio incorpora la tecnología para verificar la autenticidad, vigencia e integridad de los documentos de identificación, verificar la correspondencia del titular con la persona que realiza el proceso y verificar que este es una persona viva que no está siendo suplantada.

Se incluye también el portal de revisión manual de las evidencias llevado a cabo por un operador especialista. Además, esta herramienta permite el uso en canal Web del procedimiento de video-identificación. Esta diseñado especialmente para cumplir la Orden Ministerial ETD/743/2022, de 26 de julio, por la que se regulan los métodos de identificación remota por vídeo.

Observaciones

CCN-STIC 1630 Procedimiento de Empleo Seguro Inetum Digital Onboarding Platform

INFORMACIÓN IMPORTANTE

certificadoelectronico.es

Versión	1.0
Fabricante	Bewor Tech
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/03/2025


**Descripción**

Solución de verificación de identidad por videoidentificación a través de la cual, de manera automática, es verificada la identidad de la persona que realiza el proceso. Esta verificación consiste en la comparación biométrica entre la foto del documento acreditativo y el rostro de la persona que realiza el proceso, esta verificación biométrica contiene prueba de vida pasiva. Además, han sido desarrolladas comprobaciones en relación a la veracidad del documento acreditativo mostrado durante el proceso, analizando las dos caras del documento y el holograma. La solución cuenta con una plataforma de verificación a través de la cual, un agente formado para ello realiza una revisión manual de todas las evidencias recogidas durante cada proceso de videoidentificación. En definitiva, con esta solución, Bewor verifica de manera remota la identidad de la persona que realiza el proceso.

Observaciones

CCN-STIC-1627 Procedimiento de empleo seguro CertificadoElectronico.es

Alice Onboarding

Versión	
Fabricante	Alice Biometrics
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/03/2025


**Descripción**

Alice Onboarding es un sistema de verificación de identidad remota no asistido y multiplataforma para un caso de uso desatendido, en el que el usuario interactúa directamente con el sistema sin necesidad de establecer una videoconferencia con un operador. Esto se consigue mediante la captura guiada y procesado automático de selfie y documento de identidad, que son analizados con tecnología de inteligencia artificial desarrollada por Alice Biometrics. También se proporciona un dashboard de supervisión en el que un operador dispone de toda la información necesaria para la revisión del proceso y sus evidencias.

Todas las tecnologías involucradas han sido desarrolladas por Alice Biometrics, entre ellas: extracción del perfil biométrico facial para cotejar la identidad contra las fotografías del documento; análisis PAD pasivo y activo (Presentation Attack Detection o Liveness) para detectar ataques de suplantación de identidad; lectura automática del anverso y el reverso del documento; y análisis automático de seguridad documental.

Observaciones

CCN-STIC-1626 Procedimiento de Empleo Seguro Alice Biometrics

INFORMACIÓN IMPORTANTE

ElectronicID VideoID High Solution

Versión	3.1
Fabricante	Signicat SLU (anteriormente ElectronicID)
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	28/02/2025

**Descripción**

Solución de videoidentificación y verificación de identidad que permite la identificación remota del solicitante mediante la comparación de la información biométrica facial extraída del documento de identidad y la biometría facial de la persona que realiza el proceso. VideoID combina tecnologías de transmisión de vídeo con algoritmos de inteligencia artificial para garantizar la identificación biométrica del sujeto, así como la evaluación de ciertas características del documento de identidad.

El proceso a seguir incluye la acreditación de identidad mediante la muestra de las dos caras del documento, su holograma y una prueba de vida. Adicionalmente, el sistema permite la validación de una OTP dentro del propio proceso de videoidentificación.

Se incluye también la plataforma de verificación de identidad por parte de un agente donde se realiza la revisión manual de las evidencias recogidas, así como la evaluación de diferentes elementos de seguridad que apoyen la verificación. El proceso de identificación, por lo tanto, es desasistido y asíncrono.

Observaciones

CCN-STIC-1620 Procedimiento de empleo seguro ElectronicID VideoID High Solution

INFORMACIÓN IMPORTANTE

Mi eID eSIGN

Versión	1.2
Fabricante	ANF Certification Authority
Familia	Herramientas de videoidentificación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/10/2023
Revisión de Validez	31/03/2026

**Descripción**

Sistema de identificación remota no asistido, multiplataforma y multi-idioma para la emisión de certificados cualificados, onboarding, contratación en línea, certificación de manifestaciones de voluntad y actos de presencia en remoto. Incorpora inteligencia artificial y tecnología NFC (lectura chip DNIE y en NIE).

Verifica de manera automática la identidad de la persona; comprueba la autenticidad, vigencia e integridad de los documentos de identificación y su correspondencia con la persona que está en su posesión, obtiene evidencia certificada de video y sonido. Comprueba que el sujeto está vivo, no utiliza máscaras, ni emplea instrumentos de falsificación de imagen.

Cumple la Orden ETD/743/2022, relativa a los métodos de identificación remota para la expedición de certificados electrónicos cualificados.

Incorpora servicio de firma y sellado electrónico cualificado, estampación de tiempo electrónico cualificado, servicio cualificado de conservación de evidencias a largo plazo, y servicio cualificado de validación de firmas y sellos electrónicos, en la generación de sus evidencias con plena eficacia jurídica.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

MobbScan

Versión	2.25
Fabricante	Mobbeel, SL
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	11/07/2023
Revisión de Validez	31/12/2024


**Descripción**

MobbScan es una herramienta que permite la autenticación y videoidentificación remota de usuarios de manera segura y confiable. Para ello incorpora una serie de módulos que posibilitan recabar y validar la información personal de un usuario mediante el análisis de su documento de identidad y posteriormente comprobar mediante biometría facial que la persona que realiza el trámite es la propietaria del mismo. Durante todo el proceso se generan una serie de muestras y evidencias que son almacenadas temporalmente de manera segura hasta que un agente autorizado pueda revisarlas y validarlas a través de un portal web que asiste en esa tarea (proceso desasistido o asíncrono). El sistema utiliza tecnologías de inteligencia artificial para realizar comprobaciones sobre el documento de identidad que permitan determinar su integridad (validez de los datos) o posible uso fraudulento (uso de copias o reproducciones digitales). El motor biométrico cuenta con tecnologías avanzadas que permiten detectar intentos de ataques de suplantación mediante el uso de instrumentos como máscaras, pantallas, caracterización o deepfake. Las conclusiones de estos análisis se muestran igualmente al agente encargado de tomar la decisión sobre la validez del proceso para facilitar su tarea y añadir una capa extra de seguridad y robustez a la solución."

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.7.8 CONMUTADORES KVM

KVS4-4004DHVX

Versión	4.11.111
Fabricante	Black Box
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	31/05/2025



Descripción

Conmutadores KVM (Keyboard, Video and Mouse) seguros de Black Box, con conectividad de vídeo DVI/HDMI/DisplayPort, que proporcionan aislamiento de puertos entre redes garantizando que no existan fugas de datos entre los puertos seguros y el mundo exterior. Estos dispositivos permiten controlar múltiples ordenadores desde un solo teclado, monitos y ratón, incluso con varios canales de vídeo y una combinación de periféricos USB.

Además, disponen de un puerto CAC (Common Access Card), que permite a los administradores autenticados registrar y asignar dispositivos periféricos específicos al puerto CAC.

Observaciones

Black Box Secure KVM Administration and Security Management Tool Guide (CAC) (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd1.pdf) ADVANCED 4-PORT DP, HDMI & DVI-I SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd2.pdf)

KVS4-2002VX, KVS4-2004VX, KVS4-4004VX, KVS4-1008VX, KVS4-2008VX

Versión	4.11.001
Fabricante	Black Box
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	31/05/2025



Descripción

Conmutadores KVM (Keyboard, Video and Mouse) seguros de Black Box, con conectividad de vídeo DisplayPort, que proporcionan aislamiento de puertos entre redes garantizando que no existan fugas de datos entre los puertos seguros y el mundo exterior. Estos dispositivos permiten controlar múltiples ordenadores desde un solo teclado, monitos y ratón, incluso con varios canales de vídeo y una combinación de periféricos USB.

Además, disponen de un puerto CAC (Common Access Card), que permite a los administradores autenticados registrar y asignar dispositivos periféricos específicos al puerto CAC.

Observaciones

Black Box Secure KVM Administration and Security Management Tool Guide (CAC) https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd1.pdf ADVANCED 2/4/8-PORT DISPLAYPORT SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd3.pdf)

INFORMACIÓN IMPORTANTE

KVS4-8004VPX

Versión	4.11.004
Fabricante	Black Box
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	31/05/2025

**Descripción**

Conmutadores KVM (Keyboard, Video and Mouse) seguros de Black Box, con conectividad de vídeo DisplayPort y funcionalidad de multivisor, que proporcionan aislamiento de puertos entre redes garantizando que no existan fugas de datos entre los puertos seguros y el mundo exterior. Estos dispositivos permiten controlar múltiples ordenadores desde un solo teclado, monitos y ratón, incluso con varios canales de vídeo y una combinación de periféricos USB.

Además, disponen de un puerto CAC (Common Access Card), que permite a los administradores autenticados registrar y asignar dispositivos periféricos específicos al puerto CAC.

Observaciones

Black Box Secure KVM Administration and Security Management Tool Guide (CAC) (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd1.pdf) ADVANCED 4-PORT DP SECURE KVM SWITCH W/ PREVIEW (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd6.pdf)

INFORMACIÓN IMPORTANTE

KVS4-2002VX, KVS4-2002HVX, KVS4-1004HVX, KVS4-2004HVX

Versión	4.11.202
Fabricante	Black Box
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	31/05/2025

**Descripción**

Conmutadores KVM (Keyboard, Video and Mouse) seguros de Black Box, con conectividad de vídeo DisplayPort/HDMI, que proporcionan aislamiento de puertos entre redes garantizando que no existan fugas de datos entre los puertos seguros y el mundo exterior. Estos dispositivos permiten controlar múltiples ordenadores desde un solo teclado, monitos y ratón, incluso con varios canales de vídeo y una combinación de periféricos USB.

Además, disponen de un puerto CAC (Common Access Card), que permite a los administradores autenticados registrar y asignar dispositivos periféricos específicos al puerto CAC.

Observaciones

Black Box Secure KVM Administration and Security Management Tool Guide (CAC) (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd1.pdf) ADVANCED 4-PORT DP, HDMI & DVI-I SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd2.pdf) ADVANCED 2/4/8-PORT DISPLAYPORT SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd3.pdf) ADVANCED 2/4-PORT DP/HDMI SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd4.pdf) ADVANCED 2/4-PORT DP MST SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd5.pdf) ADVANCED 2/4/8-PORT DVI-I SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd7.pdf)

INFORMACIÓN IMPORTANTE

KVS4-2004DX, KVS4-1008DX, KVS4-2008DX

Versión	4.11.010
Fabricante	Black Box
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	31/05/2025

**Descripción**

Conmutadores KVM (Keyboard, Video and Mouse) seguros de Black Box, con conectividad de vídeo DVI, que proporcionan aislamiento de puertos entre redes garantizando que no existan fugas de datos entre los puertos seguros y el mundo exterior. Estos dispositivos permiten controlar múltiples ordenadores desde un solo teclado, monitos y ratón, incluso con varios canales de vídeo y una combinación de periféricos USB.

Además, disponen de un puerto CAC (Common Access Card), que permite a los administradores autenticados registrar y asignar dispositivos periféricos específicos al puerto CAC.

Observaciones

Black Box Secure KVM Administration and Security Management Tool Guide (CAC) (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd1.pdf) ADVANCED 2/4/8-PORT DISPLAYPORT SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd3.pdf) ADVANCED 2/4/8-PORT DVI-I SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd7.pdf)

INFORMACIÓN IMPORTANTE

7.7.9 SISTEMAS DE GESTIÓN DE BASES DE DATOS (DBMS)

Oracle Database 19c Enterprise Edition - Relational Database Management System

Versión	19.11 with Critical Patch Update April 2021
Fabricante	Oracle America Inc.
Familia	Sistemas de Gestión de Bases de Datos (DBMS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2023
Revisión de Validez	30/11/2024




Descripción

La base de datos (BD) es una recopilación organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema informático. Normalmente, una base de datos está controlada por un sistema de gestión de bases de datos (DBMS). En conjunto, los datos y el DBMS, junto con las aplicaciones asociadas a ellos, reciben el nombre de sistema de bases de datos, abreviado normalmente a simplemente base de datos. Un DBMS sirve como interfaz entre la base de datos y sus programas o usuarios finales, lo que permite a los usuarios recuperar, actualizar y gestionar cómo se organiza y se optimiza la información.

La DB de Oracle de autogestión está preparada para proporcionar un impulso significativo a estas capacidades. Dado que las bases de datos de autogestión automatizan procesos manuales costosos y tediosos, liberan a los usuarios empresariales para que puedan ser más proactivos con sus datos. Al tener control directo sobre la capacidad de crear y utilizar bases de datos, los usuarios ganan control y autonomía al mismo tiempo que mantienen importantes estándares de seguridad.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.8 OTRAS HERRAMIENTAS

7.8.1 OTRAS HERRAMIENTAS

AWS DynamoDB	
Versión	
Fabricante	AWS
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	07/11/2024
Revisión de Validez	30/04/2025
Descripción	  Amazon DynamoDB es una base de datos de valores clave y documentos que ofrece un desempeño de milisegundos de un solo dígito a cualquier escala. Se trata de una base de datos multiregión totalmente administrada con seguridad integrada, backup y restauración, y almacenamiento en caché en memoria para aplicaciones a escala de Internet. Observaciones Procedimiento de empleo seguro pendiente de publicación.

Microsoft Purview Information Protection	
Versión	N/A
Fabricante	Microsoft
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	02/12/2024
Revisión de Validez	31/05/2025
Descripción	  Microsoft Purview Information Protection es una solución integral para la protección de datos sensibles. Ofrece capacidades como el descubrimiento de datos mediante escaneo y detección, clasificación de datos con identificación gráfica de elementos etiquetados, y etiquetas de sensibilidad que proporcionan una solución única de etiquetado a través de aplicaciones, servicios y dispositivos. Además, incluye etiquetas visuales que proporcionan información sobre la sensibilidad del contenido, capacidades de cifrado con acciones de protección flexibles, y administración de derechos para gestionar el acceso y uso de la información sensible. También se integra con aplicaciones de Microsoft 365 para una experiencia de etiquetado y protección de información integrada, utiliza clasificadores potenciados por IA para una clasificación precisa, y ofrece un explorador de contenido y actividad que proporciona información sobre las acciones de los usuarios en elementos clasificados. Finalmente, se integra con Microsoft Purview DLP y emplea políticas con clasificadores y etiquetas de sensibilidad para bloquear la exfiltración y el uso compartido excesivo de datos sensibles. Todas estas funcionalidades permiten conocer toda la superficie de datos, proteger la información y prevenir la pérdida de datos dentro de un marco unificado y sencillo. Observaciones Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Sheld Plus

Versión	1.2
Fabricante	DORLET
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	18/12/2024
Revisión de Validez	31/05/2025

**Descripción**

El sistema Sheld Plus, es una solución desarrollada por DORLET para la gestión centralizada de accesos físicos. Este sistema proporciona una plataforma segura para la autorización de accesos, integrando componentes de hardware y software diseñados para optimizar el control y monitorización en entornos críticos. El sistema se compone de un centro de gestión (DASSnet®) encargado de monitorizar y consultar el estado del sistema. Incluye software puestos cliente y un servidor central para la administración integral, una unidad de control (ASDx) responsable de validar los accesos de los usuarios conforme a los derechos otorgados capaz de proporcionar información en tiempo real sobre el estado del sistema, lectores de tarjetas RFID, tarjetas MIFARE® DESFire® EV2/EV3, módulos de Seguridad MIFARE® Secure Access Module (SAM) y un módulo biométrico.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

AWS Systems Manager

Versión	Agent 3.2
Fabricante	AWS
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	29/11/2024
Revisión de Validez	30/04/2025

**Descripción**

AWS Systems Manager es el centro de operaciones para las aplicaciones y los recursos de AWS y una solución de administración integral y segura para entornos híbridos y multinube que permite efectuar operaciones seguras a escala. Este servicio hace uso del software Systems Manager Agent (SSM Agent) que se ejecutara sobre nodos gestionados y permite implementar las siguientes características:

- Respuesta ante incidentes. AWS Systems Manager proporciona la gestión y orquestación de planes de respuesta, los cuales definen las acciones iniciales que se deben seguir cuando un incidente es detectado a través de la funcionalidad de Monitorización.
- Monitorización. AWS Systems Manager permite a los usuarios obtener información sobre los nodos gestionados y controlarlos para obtener información sobre el cumplimiento. Adicionalmente, se hace uso de elementos de trabajo operativos (OpsItems) para generar incidentes.
- Automatización. AWS Systems Manager proporciona las herramientas necesarias para organizar y generar la ejecución de flujos para objetivos específicos, automatizando tareas y actualizaciones recurrentes, permitiendo a los usuarios autorizados mantener el estado de cumplimiento de sus recursos.
- Gestión. AWS Systems Manager permite gestionar otras capacidades del servicio que permitan a los usuarios complementar las funcionalidades de seguridad descritas anteriormente.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

AWS Route53

Versión**Fabricante** AWS**Familia** Otras Herramientas**Tipo** Servicio**Categoría ENS** ALTA**Fecha Inclusión** 02/09/2024**Revisión de Validez** 28/02/2025**Descripción**

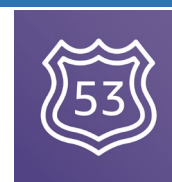
Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) en la nube altamente disponible y escalable. Está diseñado para ofrecer a los desarrolladores y las empresas una forma de dirigir a los usuarios a las aplicaciones de Internet mediante la traducción de nombres legibles por humanos, como www.example.com, en direcciones IP numéricas, como 192.0.2.1, que los equipos utilizan para conectarse entre sí. Amazon Route 53 también es totalmente compatible con IPv6.

Amazon Route 53 conecta las solicitudes de los usuarios con la infraestructura que se ejecuta en AWS, como instancias EC2, balanceadores de carga elásticos o buckets de Amazon S3, y también se puede utilizar para dirigir a los usuarios a la infraestructura fuera de AWS. Puede utilizar Amazon Route 53 para configurar comprobaciones de estado de DNS con el fin de dirigir el tráfico a puntos de enlace en buen estado o para monitorizar de forma independiente el estado de su aplicación y sus puntos de enlace.

El flujo de tráfico de Amazon Route 53 facilita la administración global del tráfico a través de diversos tipos de direccionamiento, incluidos el direccionamiento basado en la latencia, el DNS geográfico y el round robin ponderado, todo lo cual puede combinarse con la conmutación por error de DNS para habilitar diversas arquitecturas de baja latencia y tolerantes a errores. Con el sencillo editor visual del flujo de tráfico de Amazon Route 53, puede administrar fácilmente cómo se enrutan los usuarios finales a los puntos de enlace de su aplicación, ya sea en una única región de AWS o distribuidos por todo el mundo. Amazon Route 53 también ofrece registro de nombres de dominio: puede adquirir y administrar nombres de dominio como example.com y Amazon Route 53 configurará automáticamente los ajustes DNS para sus dominios. Para más información consulte <https://aws.amazon.com/es/route53/>

Observaciones

N/A

**INFORMACIÓN IMPORTANTE**

Microsoft Defender for Identity

Versión**Fabricante** Microsoft Iberica SRL**Familia** Otras Herramientas**Tipo** Servicio**Categoría ENS** ALTA**Fecha Inclusión** 01/02/2023**Revisión de Validez** 31/01/2025**Descripción**

Microsoft Defender for Identity es una solución de seguridad basada en la nube que aprovecha las señales de Active Directory locales para identificar, detectar e investigar amenazas avanzadas, identidades comprometidas y acciones internas maliciosas dirigidas a una organización.

Microsoft Defender for Identity permite a los analistas de operaciones de seguridad y a los profesionales de la seguridad, que pueden tener problemas para detectar ataques avanzados en entornos híbridos, identificar e investigar las actividades sospechosas de usuarios y ataques avanzados. Defender for Identity utiliza perfiles del comportamiento del usuario y el aprendizaje automático para crear una línea base normalizada para cada usuario. A continuación, identifica anomalías con indicadores adaptativos que asignan un peso a cada anomalía según el nivel de riesgo asociado.

Microsoft Defender for Identity es una solución que se integra con otras soluciones de seguridad como Microsoft 365 Defender, Microsoft Cloud App Security o Azure Sentinel para ofrecer una visión más completa del estado de seguridad y facilitar la respuesta a incidentes. Se puede implementar mediante sensores instalados en controladores de dominio o mediante un agente integrado en Windows Server 2019 o posterior. Defender for Identity es un producto que se utiliza para proteger las infraestructuras críticas contra ataques sofisticados como el robo o el uso indebido de credenciales, el movimiento lateral o el acceso no autorizado a recursos sensibles ayudando a prevenir estos ataques al alertar sobre actividades sospechosas, proporcionando información detallada sobre los actores y las técnicas involucradas y sugerir acciones correctivas para mitigar el impacto.

Observaciones

CCN-STIC-1112 Procedimiento de empleo seguro de Microsoft Defender for Identity.

INFORMACIÓN IMPORTANTE

Amazon Macie

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 07/05/2024

Revisión de Validez 31/12/2024



Descripción

Amazon Macie es un servicio de seguridad y privacidad de datos totalmente administrado que utiliza evaluaciones de inventario, aprendizaje automático y coincidencia de patrones para descubrir datos confidenciales y accesibilidad en su entorno de Amazon S3. Macie soporta trabajos escalables de descubrimiento de datos confidenciales bajo demanda y automatizados que rastrean automáticamente los cambios en el bucket y solo evalúan los objetos nuevos o modificados a lo largo del tiempo. Con Macie, puede detectar una lista amplia y creciente de tipos de datos confidenciales para muchos países y regiones, incluidos varios tipos de datos financieros, información sanitaria personal (PHI) e información de identificación personal (PII), así como tipos personalizados. Macie también evalúa continuamente su entorno Amazon S3 para proporcionar un resumen de recursos S3 y una evaluación de la seguridad en todas sus cuentas. Puede buscar, filtrar y ordenar los buckets de S3 por variables de metadatos, como nombres de buckets, etiquetas y controles de seguridad como el estado de cifrado o la accesibilidad pública. En el caso de los buckets sin cifrar, los buckets de acceso público o los buckets compartidos con cuentas de AWS que no sean las que ha definido en Organizaciones de AWS, puede recibir una alerta para que actúe. Para más información: <https://aws.amazon.com/es/macie/>

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

AWS Config

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/08/2022

Revisión de Validez 31/12/2024

Descripción

AWS Config es un servicio totalmente administrado que proporciona un inventario de recursos de AWS, un historial de configuración y notificaciones de cambios de configuración para permitir la seguridad y la gobernanza. La función AWS Config Rules permite crear reglas que comprueban automáticamente la configuración de los recursos de AWS registrados por AWS Config. El servicio permite descubrir los recursos de AWS existentes y eliminados, determinar su conformidad general con las reglas y profundizar en los detalles de configuración de un recurso en cualquier momento. Estas capacidades permiten la auditoría de conformidad, el análisis de seguridad, el seguimiento de los cambios en los recursos y la resolución de problemas.

Para más información sobre AWS Config, vea https://aws.amazon.com/config/?nc1=h_ls

Observaciones

CCN-STIC-887A Guía de configuración segura AWS



AWS Firewall Manager

Versión 2018-01-01

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/11/2024

Revisión de Validez 30/04/2025

Descripción

AWS Firewall Manager es un servicio de administración de seguridad que le permite configurar y administrar de forma centralizada reglas de firewall en todas sus cuentas y aplicaciones en las organizaciones de AWS. A medida que se crean nuevas aplicaciones, Firewall Manager facilita la conformidad de las nuevas aplicaciones y recursos mediante la aplicación de un conjunto común de reglas de seguridad. Ahora dispone de un único servicio para crear reglas de firewall, crear políticas de seguridad y aplicarlas de forma coherente y jerárquica en toda su infraestructura, desde una cuenta de administrador central.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

AWS
Firewall
Manager

INFORMACIÓN IMPORTANTE

Google Sensitive Data Protection (formerly Cloud Data Loss Prevention or DLP)

Versión	N/A
Fabricante	Google
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	05/11/2024
Revisión de Validez	30/04/2025

**Descripción**

La protección de datos sensibles proporciona acceso a una potente plataforma de inspección, clasificación y desidentificación de datos sensibles.

La protección de datos sensibles incluye lo siguiente:

- Más de 150 detectores de tipo de información (o “infoType”) integrados.
- La capacidad para definir detectores de InfoType personalizados con diccionarios, expresiones regulares y elementos contextuales.
- Técnicas de desidentificación que incluyen el ocultamiento, el enmascaramiento, la encriptación para preservar el formato, el cambio de fecha y mucho más.
- La capacidad de detectar datos sensibles en transmisiones de datos, texto estructurado, archivos en repositorios de almacenamiento como Cloud Storage y BigQuery, y también dentro de imágenes.
- Análisis de datos estructurados para ayudar a comprender el riesgo de la reidentificación, que incluye el procesamiento de métricas como el k-anonimato, la l-diversidad y mucho más.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Amazon S3 Glacier

Versión	
Fabricante	AWS
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/02/2024
Revisión de Validez	31/12/2024



Amazon Glacier

**Descripción**

AWS S3 Glacier es un servicio de almacenamiento seguro, duradero y de bajo costo que habilita el archivado y la realización de copias de seguridad de los datos a largo plazo en almacenes (llamados vaults).

Para más información, consultar https://docs.aws.amazon.com/es_es/amazonglacier/latest/dev/introduction.html

Observaciones

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Amazon EC2 Auto Scaling

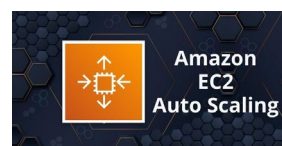
Versión**Fabricante** AWS**Familia** Otras Herramientas**Tipo** Servicio**Categoría ENS** ALTA**Fecha Inclusión** 01/02/2024**Revisión de Validez** 31/12/2024**Descripción**

Amazon EC2 Auto Scaling le ayuda a mantener la disponibilidad de las aplicaciones y le permite añadir o eliminar automáticamente instancias de EC2 según las condiciones que defina. Puede utilizar las funciones de administración de flotas de Amazon EC2 Auto Scaling para mantener el estado y la disponibilidad de su flota. También puede utilizar las funciones de escalado dinámico y predictivo de Amazon EC2 Auto Scaling para añadir o eliminar instancias de EC2. El escalado dinámico responde a los cambios en la demanda y el escalado predictivo programa automáticamente el número correcto de instancias de EC2 en función de la demanda prevista.

Para más información: <https://aws.amazon.com/es/ec2/autoscaling/>

Observaciones

Procedimiento de empleo seguro pendiente de publicación



Cisco Unified Communications Manager IM & Presence Service (C220 M5 y C240 M5)

Versión 12.5 y 14 (con Centos 7.7)**Fabricante** Cisco Systems**Familia** Otras Herramientas**Tipo** Producto**Categoría ENS** ALTA**Fecha Inclusión** 01/03/2023**Revisión de Validez** 31/08/2025**Descripción**

Sistema de comunicaciones empresarial que suministra voz y videollamadas sobre una red IP.

Observaciones

CCN-STIC-1460 Procedimiento de Empleo Seguro Cisco Unified Communications Manager (C220 M5 y C240 M5)

**INFORMACIÓN IMPORTANTE**

TrustCloud

Versión	4
Fabricante	TrustCloud Tech SL
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	MEDIA
Fecha Inclusión	01/01/2023
Revisión de Validez	31/12/2024

**Descripción**

La plataforma Trustcloud es un 'Coreógrafo de Transacciones digitales seguras'. Trustcloud es un Orquestador de orquestadores, y los Servicios son proporcionados en modelo SaaS: Software as a Service. TrustCloud orquesta y blinda las transacciones digitales llevadas a cabo entre los distintos casos de uso de los clientes. Es una plataforma única de orquestación y custodia de todas las evidencias generadas por las transacciones digitales, que permite preservar cualificadamente los activos digitales, garantizando su identidad, integridad e intención de todos los participantes en cualquier parte del mundo, y con ello se consigue que sean seguras, ya que por sí solas no lo son.

Observaciones

CCN-STIC-1622 Procedimiento de empleo seguro TrustCloud

Microsoft Purview Communication Compliance

Versión	
Fabricante	Microsoft
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	30/10/2024
Revisión de Validez	31/03/2025

**Descripción**

Microsoft Purview Communication Compliance es una solución de gestión de riesgos internos que ayuda a las organizaciones a detectar, capturar y actuar sobre mensajes potencialmente inapropiados dentro de la empresa. Para ello utiliza análisis de contenido y algoritmos de aprendizaje automático para identificar comunicaciones que puedan violar las políticas corporativas o regulaciones. Esta solución se integra con servicios de Microsoft 365 y soluciones de terceros a través de conectores, permitiendo a investigar y tomar medidas correctivas sobre los mensajes detectados. Está diseñada con el fin de garantizar la privacidad, utilizando seudonimización de nombres de usuario, controles de acceso basados en roles y registros de auditoría.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

metaOLVIDO Dashboard (modalidad on-premise)

Versión	1.3.0
Fabricante	Adarsus Technologies S.L
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/04/2026

**Descripción**

metaOLVIDO Dashboard: Consola de administración de metaOLVIDO para las distintas modalidades de despliegue. Administra, centraliza y controla la aplicación de políticas preventivas de seguridad corporativas. Permite obtener estadísticas de los metadatos procesados y controlar la exfiltración de información de forma global.

Observaciones

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard

AWS Organizations

Versión	
Fabricante	AWS
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/03/2023
Revisión de Validez	28/02/2025



AWS Organizations

**Descripción**

AWS Organizations le ayuda a administrar y gobernar de forma centralizada su entorno a medida que crece y escala sus recursos de AWS. Con AWS Organizations, se puede crear mediante programación nuevas cuentas de AWS y asignar recursos, agrupar cuentas para organizar sus flujos de trabajo, aplicar políticas a cuentas o grupos para y simplificar la facturación utilizando un único método de pago para todas sus cuentas.

Además, AWS Organizations se integra con otros servicios de AWS para que pueda definir configuraciones centrales, mecanismos de seguridad, requisitos de auditoría y recursos compartidos entre las cuentas de su organización. AWS Organizations está disponible para todos los clientes de AWS sin cargo adicional. Para más información acerca AWS Organizations, visite <https://aws.amazon.com/es/organizations/>

Observaciones

CCN-STIC-887A Guía de configuración segura AWS

INFORMACIÓN IMPORTANTE

Amazon EC2

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/02/2024

Revisión de Validez 31/12/2024

Descripción

Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona una capacidad informática segura y de tamaño variable en la nube. Está diseñado para facilitar a los desarrolladores recursos de computación escalables basados en Web. La sencilla interfaz web de Amazon EC2 le permite obtener y configurar la capacidad con una fricción mínima. Proporciona un control completo sobre los recursos de computación y puede ejecutarse en el entorno de computación de Amazon.

Para más información: <https://aws.amazon.com/es/ec2/>

Observaciones

Procedimiento de empleo seguro pendiente de publicación



AWS Certificate Manager

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 21/10/2024

Revisión de Validez 31/03/2025

Descripción

AWS Certificate Manager es un servicio que le permite aprovisionar, administrar e implementar fácilmente certificados SSL/TLS (Secure Sockets Layer/Transport Layer Security) para utilizarlos con los servicios de AWS y sus recursos internos conectados. Los certificados SSL/TLS se utilizan para proteger las comunicaciones de red y establecer la identidad de los sitios web en Internet, así como los recursos en redes privadas. AWS Certificate Manager elimina el largo proceso manual de compra, carga y renovación de certificados SSL/TLS.

Con AWS Certificate Manager, puede solicitar rápidamente un certificado, implementarlo en recursos de AWS integrados en ACM, como Elastic Load Balancing, distribuciones de Amazon CloudFront y API en API Gateway, y dejar que AWS Certificate Manager gestione las renovaciones de certificados. También le permite crear certificados privados para sus recursos internos y administrar el ciclo de vida de los certificados de forma centralizada.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.



INFORMACIÓN IMPORTANTE

AWS Security Hub

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/09/2022

Revisión de Validez 31/12/2024

Descripción

AWS Security Hub es un servicio de gestión de la seguridad en la nube que realiza comprobaciones automatizadas y continuas de las mejores prácticas de seguridad de los recursos de sus cuentas AWS de acuerdo al estándar AWS Foundational Security Best Practices y otros marcos de conformidad.

Para mantener una visión completa de su postura de seguridad, Security Hub genera una puntuación de seguridad consolidada en todas sus cuentas de AWS, para lo cual necesita integrar múltiples herramientas y servicios, incluidas detecciones de amenazas de Amazon GuardDuty, vulnerabilidades de Amazon Inspector, clasificaciones de datos confidenciales de Amazon Macie, problemas de configuración de recursos de AWS Config y productos de la red de socios de AWS.

Security Hub agrega todos estos hallazgos de seguridad en un solo lugar y formato a través del formato de hallazgos de seguridad de AWS, y reduce su tiempo medio de reparación (MTTR) con respuesta automatizada y soporte de reparación.

También puede integrarse con herramientas de emisión de tickets, chat, SIEM, SOAR, GRC y gestión de incidentes para proporcionar a sus usuarios un flujo de trabajo completo de operaciones de seguridad.

Para más información acerca de AWS Security Hub, visite: <https://aws.amazon.com/es/security-hub/>

Observaciones

CCN-STIC-887A Guía de configuración segura AWS



AWS Security Hub



metaOLVIDO Endpoint y metaOLVIDO Server

Versión 2.3.0

Fabricante Adarsus Technologies S.L

Familia Otras Herramientas

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/11/2023

Revisión de Validez 30/04/2026

Descripción

metaOLVIDO EndPoint y metaOLVIDO Server: Herramienta de gestión de metadatos que permite aplicar políticas de seguridad corporativas de prevención de fugas de información, limpiando los metadatos e información sensible oculta en los ficheros ofimáticos generados en una organización.

Realiza una protección continua y en tiempo real de los metadatos de una estación de trabajo o Servidor. Protege la información de manera sencilla y desatendida. Permite configurar reglas y ponerlas en práctica sobre los archivos documentales o multimedia que se considere necesario, ya sea en los equipos de usuario -EndPoint- o en carpetas de red compartidas -Server-.

Observaciones

CCN-STIC 1511 Procedimiento de Empleo Seguro metaOLVIDO EndPoint y metaOLVIDO Server



INFORMACIÓN IMPORTANTE

AWS Secrets Manager

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/02/2024

Revisión de Validez 31/12/2024

Descripción

AWS Secrets Manager le ayuda a proteger los secretos necesarios para acceder a sus aplicaciones, servicios y recursos de IT. El servicio le permite rotar, administrar y recuperar fácilmente las credenciales de las bases de datos, las claves de API y otros datos secretos a lo largo de su ciclo de vida. Los usuarios y las aplicaciones recuperan los datos confidenciales con una llamada a las API de Secrets Manager, lo que elimina la necesidad de codificar la información confidencial en texto plano. Secrets Manager ofrece una rotación de secretos con una integración incorporada para Amazon RDS, Amazon Redshift y Amazon DocumentDB. El servicio también se puede extender a otros tipos de secretos, incluidas las claves de API y los tokens de OAuth. Además, Secrets Manager le permite controlar el acceso a los datos secretos mediante permisos detallados y auditar la rotación de secretos de forma centralizada para los recursos en los Nube de AWS servicios de terceros y en las instalaciones.

Para más información: <https://aws.amazon.com/es/secrets-manager/>

Observaciones

Procedimiento de empleo seguro pendiente de publicación



Cloud Trail

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/06/2022

Revisión de Validez 31/12/2024

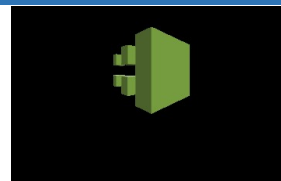
Descripción

AWS CloudTrail es un servicio web que registra las llamadas al API de AWS de su cuenta y le entrega archivos de registro. La información registrada incluye la identidad de la persona que llama a la API, la hora de la llamada a la API, la dirección IP de origen de la persona que llama a la API, los parámetros de la solicitud y los elementos de respuesta devueltos por el servicio de AWS.

Con CloudTrail, se puede obtener un historial de llamadas a la API de AWS para su cuenta, incluidas las llamadas a la API realizadas mediante la consola de administración de AWS, los SDK de AWS, las herramientas de línea de comandos y los servicios de AWS de nivel superior (como AWS CloudFormation). El historial de llamadas a la API de AWS producido por CloudTrail permite el análisis de seguridad, el seguimiento de los cambios en los recursos y la auditoría de conformidad.

Observaciones

CCN-STIC-887A Guía de configuración segura AWS



INFORMACIÓN IMPORTANTE

CloudFront

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/02/2024

Revisión de Validez 31/12/2024

Descripción

Amazon CloudFront es un servicio de red de entrega de contenido (CDN) rápido que envía de forma segura datos, vídeos, aplicaciones y API a clientes de todo el mundo con baja latencia y altas velocidades de transferencia, todo ello en un entorno fácil de usar para los desarrolladores. CloudFront está integrado con AWS, tanto con ubicaciones físicas conectadas directamente a la infraestructura global de AWS como con otros servicios de AWS. CloudFront funciona a la perfección con servicios como AWS Shield para la mitigación de DDoS, Amazon S3, Elastic Load Balancing o Amazon EC2 como orígenes para sus aplicaciones, y Lambda para ejecutar código personalizado más cerca de los usuarios de los clientes y personalizar la experiencia del usuario.

Puede comenzar a utilizar la red de entrega de contenido en cuestión de minutos, utilizando las mismas herramientas de AWS con las que ya está familiarizado: API, consola de administración de AWS, AWS CloudFormation, CLI y SDK. Amazon CDN ofrece un modelo de precios sencillo, de pago por uso, sin cuotas iniciales ni contratos a largo plazo, y el soporte para la CDN está incluido en su suscripción existente a AWS Support.

Para más información consulte <https://aws.amazon.com/es/cloudfront/>

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación



Amazon CloudFront



authUsb safeDoor

Versión 2.0.0.11

Fabricante AUTHUSB

Familia Otras Herramientas

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/05/2019

Revisión de Validez 30/12/2024

Descripción

AuthUsb safeDoor es un dispositivo hardware que actúa como barrera entre las memorias USB y los equipos de una organización, identificando amenazas a tres niveles:

- Eléctrico: identificando y deteniendo ataques destructivos de sobretensión tipo UsbKiller.
- Hardware: detectando y desactivando ataques de la familia BadUsb, ataques HID (rubber ducky y similares), falsas tarjetas de red, interfaces compuestas, etc.
- Software: antivirus integrado que realiza un análisis previo a la descarga de cualquier contenido.

Observaciones

CCN-STIC 1201 Procedimiento de Empleo Seguro AuthUsb SafeDoor



INFORMACIÓN IMPORTANTE

Personal Code

Versión	2020.3
Fabricante	HUBOX
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/09/2021
Revisión de Validez	31/03/2026

PERSONAL
CODE®

Descripción

PERSONAL CODE es una solución de identidad digital que resuelve el problema de fraudes por suplantación de identidad. Véase la solución como una secuencia de bits que almacena, de forma segura, características biométricas e información biográfica de un individuo. Estos datos son firmados y reconocidos por una autoridad y se protegen mediante criptografía asimétrica para su posterior verificación a través de una aplicación que no requiere conectividad ni consultas a bases de datos. PERSONAL CODE implementa su solución en forma de dos librerías o DLLs, una librería de generación que se encarga de procesar la información del individuo y otra de verificación para la posterior extracción y validación de los datos.

Observaciones

CCN-STIC-1218 Procedimiento de empleo seguro Personal Code de HUBOX

INFORMACIÓN IMPORTANTE

7.9 SEGURIDAD OT

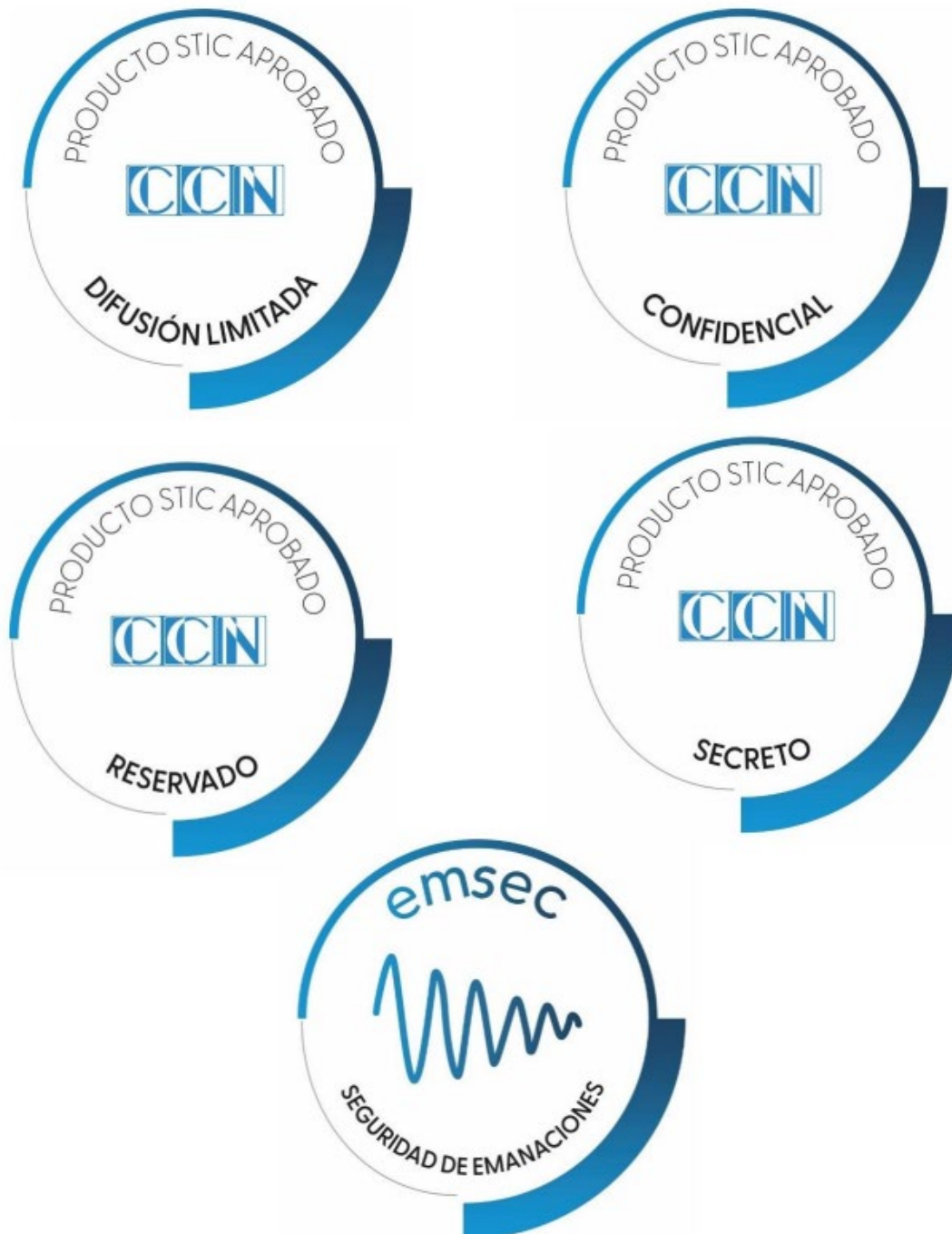
7.9.1 SEGURIDAD OT

Ágata	
Versión	2.3.3
Fabricante	Ágata Technology
Familia	Seguridad OT
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/12/2025
Descripción	Ágata es una plataforma software que permite la digitalización, optimización y automatización de procesos de negocio, poniendo la tecnología al servicio de las personas. Ágata integra en un único entorno tecnológico todos los procesos y servicios de una organización permitiendo gestionarlos de manera sencilla, eficiente, sostenible y segura. Observaciones CCN-STIC 1305 Procedimiento de empleo seguro AGATA



8. PRODUCTOS APROBADOS

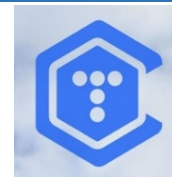
PRODUCTOS APROBADOS



8.1 HERRAMIENTAS PARA EL DESARROLLO DE PRODUCTOS DE SEGURIDAD

Módulo criptográfico para aplicaciones móviles Telcryp

Versión	1.11
Fabricante	Cryptographic and Security System (CS2)
Familia	-
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/10/2025



Descripción

Este módulo provee los servicios de cifrado y seguridad para garantizar la comunicación tanto con el servidor IMS como con los terminales remotos con un cifrado extremo a extremo.

Este módulo criptográfico está diseñado como una librería criptográfica e incorporado a aplicaciones de comunicaciones en entorno de movilidad debidamente aprobadas, e instaladas en plataformas confiables.

Observaciones

Procedimiento de empleo pendiente de publicación

8.2 CONTROL DE ACCESO

8.2.1 CONTROL DE ACCESO A RED (NAC)

Forescout 8.3 (CT-R, CT-100, CT-1000, CT-2000, CT-4000, CT-10000, CEM-5, CEM-10, CEM-25, CEM-50, CEM-100, CEM-150, CEM-200, 4130, 5110, 5120, 5140, 5160)

Versión 8.4

Fabricante Forescout

Familia Control de acceso a red (NAC)

Tipo Producto

Clasificación TODOS LOS NIVELES

Fecha Inclusión 01/05/2023

Revisión de Validez 31/10/2025

Descripción

La plataforma Forescout es una plataforma unificada de seguridad que permite a las empresas y organismos oficiales obtener información completa sobre el estado de sus entornos empresariales ampliados y orquestar medidas destinadas a reducir el riesgo operativo y de ciberseguridad. Se despliega de forma rápida y segura en entornos de campus, centros de datos, la nube y redes de OT. Ofrece descubrimiento, clasificación en tiempo real y evaluación continua de estado, sin necesidad de agentes. Para más información, véase: <https://forescouttechnologies.es>

Observaciones

CCN-STIC-1106 Procedimiento de empleo seguro Forescout

 **FORESCOUT.**



8.2.2 GESTIÓN DE IDENTIDADES (IM)

SailPoint IdentityIQ	
Versión	V8.3p2
Fabricante	Sailpoint
Familia	Gestión de identidades (IM)
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/02/2024
Revisión de Validez	31/12/2025
Descripción Sailpoint es una plataforma de Gestión de Identidades y Accesos que ofrece una amplia gama de funcionalidades, lo que lo convierte en una solución integral para la gestión de la identidades en las organizaciones. • Provisionamiento: onboarding de nuevos usuarios, cambios y des provisionamiento, automatización en los procesos. Para usuarios internos, colaboradores y/o proveedores. • Gobierno de acceso: Visibilidad completa de los accesos de la organización, certificación de acceso, cumplimiento de acceso según políticas de usuarios a aplicaciones y datos. • Gestión de contraseñas. • Segregación de funciones. • Gobierno de nube.	
Observaciones CCN-STIC-1111 SAILPOINT IdentityIQ	



8.3 SEGURIDAD EN LA EXPLOTACIÓN

8.3.1 ANTI-VIRUS / EPP (ENDPOINT PROTECTION PLATFORM)

Stormshield Endpoint Security Evolution

Versión	2.5.3
Fabricante	Stormshield
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2024
Revisión de Validez	30/11/2026



Descripción

Stormshield Endpoint Security Evolution ofrece una ciberseguridad de nueva generación para garantizar la protección completa de terminales y servidores. Basado en la tecnología de análisis de comportamiento sin firmas, el agente reconoce las técnicas de ataque, como la explotación de las vulnerabilidades de las aplicaciones o las acciones características del ransomware. Una vez identificada la amenaza, se puede tomar cualquier acción deseada, como el cierre de procesos o el bloqueo de las conexiones de red (cuarentena de equipos infectados, restricción de túnel VPN o de uso de redes Wi-Fi).

Observaciones

CCN-STIC-1221 Procedimiento de empleo seguro Stormshield Endpoint Security Evolution

Deep Security (Manager y Agente/Relay Linux/Windows)

Versión	11
Fabricante	Trend Micro
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2021
Revisión de Validez	31/03/2025



Descripción

Deep Security es la respuesta de Trend Micro para proteger el cloud híbrido ya sean servidores físicos o virtuales.

Gracias a su agente ligero, el cual incorpora funcionalidades: EDR (con respuesta frente a amenazas conocidas, zero-day), envío de telemetría a la plataforma XDR de Trend Micro (VisionOne), reputación web, control de aplicaciones, supervisión de logs, Supervisión de Integridad (FIM), Firewall de Host y Host IPS (que incorpora la tecnología de parchado virtual), ayuda a mejorar la postura de seguridad proporcionando seguridad, visibilidad y control. La cualificación abarca los siguientes componentes: Manager, Agente/Relay Linux y el Agente/Relay Windows. El Virtual Appliance no está cualificado.

Observaciones

CCN-STIC-1216 PES Trendmicro Deep Security

8.3.2 EDR (ENDPOINT DETECTION AND RESPONSE)

Stormshield Endpoint Security Evolution

Versión	2.5.3
Fabricante	Stormshield
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2024
Revisión de Validez	30/11/2026



Descripción

Stormshield Endpoint Security Evolution ofrece una ciberseguridad de nueva generación para garantizar la protección completa de terminales y servidores. Basado en la tecnología de análisis de comportamiento sin firmas, el agente reconoce las técnicas de ataque, como la explotación de las vulnerabilidades de las aplicaciones o las acciones características del ransomware. Una vez identificada la amenaza, se puede tomar cualquier acción deseada, como el cierre de procesos o el bloqueo de las conexiones de red (cuarentena de equipos infectados, restricción de túnel VPN o de uso de redes Wi-Fi).

Observaciones

CCN-STIC-1221 Procedimiento de empleo seguro Stormshield Endpoint Security Evolution

Deep Security (Manager y Agente/Relay Linux/Windows)

Versión	11
Fabricante	Trend Micro
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2021
Revisión de Validez	31/03/2025



Descripción

Deep Security es la respuesta de Trend Micro para proteger el cloud híbrido ya sean servidores físicos o virtuales.

Gracias a su agente ligero, el cual incorpora funcionalidades: EDR (con respuesta frente a amenazas conocidas, zero-day), envío de telemetría a la plataforma XDR de Trend Micro (VisionOne), reputación web, control de aplicaciones, supervisión de logs, Supervisión de Integridad (FIM), Firewall de Host y Host IPS (que incorpora la tecnología de parchado virtual), ayuda a mejorar la postura de seguridad proporcionando seguridad, visibilidad y control. La cualificación abarca los siguientes componentes: Manager, Agente/Relay Linux y el Agente/Relay Windows. El Virtual Appliance no está cualificado.

Observaciones

CCN-STIC-1216 PES Trendmicro Deep Security

8.3.3 HERRAMIENTAS DE FILTRADO DE NAVEGACIÓN

Cisco Web Security Appliance (S690, S690X, S695, S695F, S680, S390, S380, S395, S190, S195)

Versión	AsyncOS 11.8
Fabricante	Cisco Systems
Familia	Herramientas de filtrado de navegación
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2022
Revisión de Validez	31/05/2025



Descripción

Cisco Secure Web Appliance proxy protege a las organizaciones en cuanto a navegación se refiere, evaluando las webs desconocidas antes de permitir que los usuarios accedan a ellas y bloqueando automáticamente las páginas de riesgo. Utilizando funciones de alto rendimiento, Cisco Secure Web Appliance mantiene seguros a los usuarios.

Observaciones

CCN-STIC-1625 Procedimiento de Empleo Seguro Cisco Web Security Appliance

8.3.4 SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM)

MONICA

Versión	7.1
Fabricante	Grupo ICA Sistemas y Seguridad
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2024
Revisión de Validez	31/12/2024



Descripción

La plataforma española Mónica permite a los analistas de ciberseguridad recopilar logs e información ilimitada de seguridad, detectar ataques basados en anomalías y comportamientos desconocidos así como automatizar la respuesta ante incidentes en entornos IT, OT e IoT. Mónica recopila información de cualquier fuente interna y externa a la empresa (comercial, propietaria, aplicaciones, cloud), correlando y analizando en tiempo real esa información, permitiendo contextualizar y priorizar los incidentes de seguridad tanto internos como externos. Combina los casos de uso de detección más sofisticados con la información más precisa de amenazas y vulnerabilidades zero day gracias a la información de fuentes externas de inteligencia, threat hunting y anomalías de red/usuario.

Observaciones

CCN-STIC-1206 PES NGSIEM LogICA

Gloria

Versión	v6.6.1
Fabricante	S2 GRUPO / CCN
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2023
Revisión de Validez	30/06/2026



Descripción

Gloria es una plataforma para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos. Basado en los sistemas SIEM, va un paso más allá de las capacidades de monitorización, almacenamiento e interpretación de los datos relevantes. Así, mediante técnicas de correlación compleja de varias fuentes de eventos o análisis de patrones para la identificación de anomalías, permite una orientación muy flexible hacia la vigilancia del mundo IP. La plataforma permite las siguientes funcionalidades a través de distintos módulos:

- Monitorización de entornos tecnológicos (IT/OT).
 - Inteligencia.
 - Gestión del servicio.
 - Automatización, orquestación y reducción de tiempos de respuesta.
- Para más información, (<https://ccn-cert.cni.es/soluciones-seguridad/gloria.html>)

Observaciones

CCN-STIC-1215 Procedimiento de empleo seguro GLORIA

MONSE

Versión	Probe 1.0, Agente 8.3.2
Fabricante	GRUPO CIES
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	N/A
Revisión de Validez	01/11/2024

**Descripción**

MONSE (Monitorización de la Seguridad) es una solución SIEM que permite recopilar y correlacionar de forma centralizada múltiples fuentes de eventos de seguridad. La solución permite analizar eventos basados en logs, procesos, comportamiento e IOCs. Dispone de técnicas de Inteligencia Artificial que facilitan la detección de anomalías, integración de fuentes de inteligencia de amenazas, posibilidad de definir reglas de alerta adaptadas a la particularidad de cada organización, así como la posibilidad de crear cuadros de mando personalizables. La plataforma permite un despliegue modular en función del tipo de madurez de la organización. Dispone de múltiples funcionalidades orientadas a la mejora en el cumplimiento del Esquema Nacional de Seguridad.

Observaciones

CCN-STIC 1223 Procedimiento de empleo seguro MONSE

NetWitness Platform

Versión	11.6
Fabricante	Netwitness, an RSA Business.
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/07/2022
Revisión de Validez	31/12/2024

**Descripción**

La plataforma XDR de Netwitness (an RSA Business), es la solución de SIEM evolucionado o XDR (eXtended Detection and Response), con capacidades de visibilidad completa gracias a su modelo de datos unificado pudiendo capturar logs, netflows, tráfico de red, actividad en los end points, además de información de inteligencia de seguridad, de forma integrada, bajo un único motor de análisis y correlación avanzada. Además, incluye funcionalidades necesarias por un SOC para hacer frente a amenazas complejas. Netwitness Platform XDR cuenta además con componentes adicionales como UEBA (User and Entity Behaviour Analytics) y SOAR (Security Orchestration and Automation Response). La solución permite capturar todo tipo de información, permitiendo el análisis avanzado de amenazas, priorización en base al contexto de negocio y haciendo más eficiente el trabajo del analista. Es una plataforma que, gracias a su capacidad de análisis, muestra el alcance completo de un ataque a los analistas. Además, gracias a su estrategia Run Anywhere, la plataforma se puede desplegar en cualquier entorno (virtual, cloud, físico o híbrido), así como hacer frente a arquitecturas altamente distribuidas. RSA Netwitness incluye en todos sus clientes +50 feeds de inteligencia, agente para endpoints ilimitados, así como el despliegue ilimitado de dispositivos para cubrir cualquier forma de despliegue. <https://www.netwitness.com/en-us/solutions/evolved-siem/>

Observaciones

CCN-STIC-1210 Procedimiento de Empleo Seguro RSA Netwitness Platform

NetWitness Platform

Versión	11.7
Fabricante	Netwitness, an RSA Business.
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2024
Revisión de Validez	31/12/2025

**Descripción**

La plataforma XDR de Netwitness (an RSA Business), es la solución de SIEM evolucionado o XDR (eXtended Detection and Response), con capacidades de visibilidad completa gracias a su modelo de datos unificado pudiendo capturar logs, netflows, tráfico de red, actividad en los end points, además de información de inteligencia de seguridad, de forma integrada, bajo un único motor de análisis y correlación avanzada. Además, incluye funcionalidades necesarias por un SOC para hacer frente a amenazas complejas. Netwitness Platform XDR cuenta además con componentes adicionales como UEBA (User and Entity Behaviour Analytics) y SOAR (Security Orchestration and Automation Response). La solución permite capturar todo tipo de información, permitiendo el análisis avanzado de amenazas, priorización en base al contexto de negocio y haciendo más eficiente el trabajo del analista. Es una plataforma que, gracias a su capacidad de análisis, muestra el alcance completo de un ataque a los analistas. Además, gracias a su estrategia Run Anywhere, la plataforma se puede desplegar en cualquier entorno (virtual, cloud, físico o híbrido), así como hacer frente a arquitecturas altamente distribuidas. RSA Netwitness incluye en todos sus clientes +50 feeds de inteligencia, agente para endpoints ilimitados, así como el despliegue ilimitado de dispositivos para cubrir cualquier forma de despliegue. <https://www.netwitness.com/en-us/solutions/evolved-siem/>

Observaciones

CCN-STIC-1210 Procedimiento de Empleo Seguro RSA Netwitness Platform

LogICA5 Next Generation SIEM

Versión	v7.1
Fabricante	Grupo ICA Sistemas y Seguridad
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/01/2020
Revisión de Validez	31/12/2024

**Descripción**

La plataforma española Next Generation SIEM LogICA permite a los analistas de ciberseguridad recopilar logs e información ilimitada de seguridad, detectar ataques basados en anomalías y comportamientos desconocidos así como automatizar la respuesta ante incidentes en entornos IT, OT e IoT. LogICA NG SIEM recopila información de cualquier fuente interna y externa a la empresa (comercial, propietaria, aplicaciones, cloud), correlando y analizando en tiempo real esa información, permitiendo contextualizar y priorizar los incidentes de seguridad tanto internos como externos. Combina los casos de uso de detección más sofisticados con la información más precisa de amenazas y vulnerabilidades zero day gracias a la información de fuentes externas de inteligencia, threat hunting y anomalías de red/usuario. Incorpora, además, un cuadro de mando de gestión del servicio, centralizando la información y facilitando su consumo por parte de la organización. LogICA permite adaptarse a las necesidades de despliegue de las organizaciones, en modo on-premise, virtual o entorno cloud.

Observaciones

CCN-STIC-1206 PES NGSiem LogICA

8.3.5 DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS

EP543N

Versión	V.1.7
Fabricante	Epicom
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Producto
Clasificación	RESERVADO
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2024



Descripción

Centro de Gestión de cifradores IP EP430GN sobre ordenador seguro EP1140.

Observaciones

EP543X

Versión	SW v 4.15
Fabricante	Epicom
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Producto
Clasificación	SECRETO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2024



Descripción

Centro de Gestión sobre la plataforma EP1140, que da soporte a los cifradores de la familia EP430, incluidos los modelos EP430TX y EP430GX.

Observaciones

Utilización según PE-2012-49 Procedimiento de Empleo EP430GX v2

EP543U/B

Versión	2.01
Fabricante	Epicom
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	01/09/2020
Revisión de Validez	31/12/2025

**Descripción**

El Centro de Gestión EP543U/B es el elemento de gestión remota del cifrador EP430 GU/B. El único procedimiento permitido para gestionar de manera remota un EP430GU/B es a través de una conexión remota segura (Canal Seguro) desde la aplicación del Centro de Gestión.

Observaciones

Utilización según PE-2019-9 Procedimiento de Empleo EP430GU/B

8.4 MONITORIZACIÓN DE LA SEGURIDAD

8.4.1 CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO

GigaVUE (GVS-HC301, GVS-HC302, GVS-HC2A1, GVS-HC2A2, GVS-HC101 y GVS-HC102)

Versión	6.1
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	28/06/2023
Revisión de Validez	30/11/2025



Descripción

Network Packet Brokers HC Series. Network Packet Brokers de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1g/10g en cobre y funcionalidades de filtrado de tráfico L2-3-4-7 con motor de DPI, generación de Netflow/IPFix/Metadatos, Cifrado/Descifrado de SSL/TLS (incluyendo protocolos RSA, DHE, ECC, y PFS), Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Truncado de paquetes, Eliminación de cabeceras, Enmascarado, De-Duplicación, Clustering, Balanceo, Captura de tráfico para entornos virtuales (VMWare ESX/NSX, Openstack, Kubernetes, AWS, GCP, Azure, Nutanix), simetrización de tráfico para arquitectura HA, Inline Bypass con Heartbeat positivo y negativo, Cambio de medio y velocidad, Bypass HW, TAPs integrados.

Observaciones

CCN-STIC-1301 Procedimiento de Empleo Seguro GigaVUE-OS

GigaVUE (GVS-TAX21-HW, GVS-TAX22-HW, GVS-TAX21A-HW, GVS-TAX22A-HW, GVS-TAC21, GVS-TAC22, GTP-ATX21, GTP-ASF21)

Versión	6.1
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	28/06/2023
Revisión de Validez	30/11/2025



Descripción

Network Packet Brokers HC Series. Network Packet Brokers de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1g/10g en cobre y funcionalidades de filtrado de tráfico L2-3-4-7 con motor de DPI, generación de Netflow/IPFix/Metadatos, Cifrado/Descifrado de SSL/TLS (incluyendo protocolos RSA, DHE, ECC, y PFS), Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Truncado de paquetes, Eliminación de cabeceras, Enmascarado, De-Duplicación, Clustering, Balanceo, Captura de tráfico para entornos virtuales (VMWare ESX/NSX, Openstack, Kubernetes, AWS, GCP, Azure, Nutanix), simetrización de tráfico para arquitectura HA, Inline Bypass con Heartbeat positivo y negativo, Cambio de medio y velocidad, Bypass HW, TAPs integrados.

Observaciones

CCN-STIC-1301 Procedimiento de Empleo Seguro GigaVUE-OS

CARMEN

Versión	Versión 7.24.3
Fabricante	S2 GRUPO / CCN
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2022
Revisión de Validez	31/07/2026

**Descripción**

CARMEN (Centro de Análisis de Registros y Minería de EveNtos) es una solución software de adquisición, procesamiento y análisis de información para soportar el proceso de identificación de Amenazas Persistentes Avanzadas (APT) a partir del tráfico de red interno y saliente de una forma eficiente, apoyando la toma de decisiones a partir de la información generada y procesada. Se compone de agentes que recopilan los flujos de tráfico, un motor de almacenamiento en el que se inserta la información, un sistema de detección de anomalías que se encarga de procesar la información almacenada y una aplicación web que permite la representación y consulta tanto de la información obtenida como de la procesada. Para más información, se puede consultar la web del CCN-CERT (<https://ccn-cert.cni.es/soluciones-seguridad/carmen.html>)

Observaciones

CCN-STIC-1304 Procedimiento de empleo seguro CARMEN

8.5 PROTECCIÓN DE LAS COMUNICACIONES

8.5.1 ENRUTADORES

Dell EMC Networking SmartFabric OS10.5.4 en Switches de las series N, S y Z (N3248TE, S41xx, S52xx, S54xx, Z91xx, Z92xx, Z93xx, Z94xx, Z96xx)

Versión	OS10.5.4
Fabricante	DELL COMPUTER, S.A.
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2024
Revisión de Validez	31/03/2026

Descripción

Dell EMC Smart Fabric OS10 es el sistema operativo de red (NOS) que se utiliza en las familias de enrutadores y conmutadores de las serie N (algunos modelos), serie S, serie Z y serie MX de Dell EMC Networking (las plataformas HW que actualmente soportan OS10 son N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n y MX9116n). Dell EMC SmartFabric OS10 es un sistema operativo de red (NOS) que admite múltiples arquitecturas y entornos. La solución SmartFabric OS10 permite la desagregación en varias capas de la funcionalidad de red. SmartFabric OS10 comprende la administración, monitorización y funcionalidad completa y estándar de la industria de redes de nivel 2 y nivel 3 a través de interfaces CLI, SNMP y REST. Los usuarios pueden elegir sus propias aplicaciones de organización, gestión, supervisión y redes de terceros. Para desarrollar redes escalables L2 y L3, SmartFabric OS10 ofrece una solución modular y desagregada en una única imagen binaria.

Observaciones

CCN-STIC-1429 PES DELL EMC Networking



Cisco ASR9000 Series y NCS4200 Series (ASR902, ASR903, ASR907, ASR920 y NCS4201, NCS4202, NCS4206, NCS4216)

Versión	IOS-XE 16.9
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2023
Revisión de Validez	30/04/2025

Descripción

Las familias ASR900 y NCS4200 son equipos hechos a propósito como plataformas de routing, soportando adicionalmente cifrado MACsec.

Observaciones

CCN-STIC 1454 Procedimiento de Empleo Seguro Routers CISCO ASR9000 y NCS4200 Series



Cisco Nexus 9200 Series Switches (92348GC-X, 92160YC-X, 92300YC, 9272Q)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 3200 Series Switches (3232C, 3264C-E)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 3500 Series Switches (3524-X/XL, 3548-X/XL)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 3600 Series Switches (36180YC-R, 3636C-R)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 3400 Series Switches (34180-YC, 3464C, 3432D-S, 3408-S)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 9300 Series Switches (93108TC-EX, 93108TC-FX, 9348GC-FXP, 93216TC-FX2, 93180LC-EX, 93180YC-EX, 93180YC-FX, 93240YC-FX2, 93360YC-FX2, 9364C, 9332C, 9336C-FX2, 9364C-GX, 9316D-GX, 93600CD-GX)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	04/10/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 9500 Series Switches (9504, 9508, 9516, Supervisor 9500-Sup-A , Supervisor 9500-Sup-A +, Supervisor 9500-Sup-B , Supervisor 9500-Sup-B +, System Controller N9k-SC-A)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	04/10/2025



Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9

8.5.2 SWITCHES

Dell EMC Networking SmartFabric OS10.5.4en Switches de las series N, S y Z (N3248TE, S41xx, S52xx, S54xx, Z91xx, Z92xx, Z93xx, Z94xx, Z96xx)

Versión	OS10.5.4
Fabricante	DELL COMPUTER, S.A.
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2024
Revisión de Validez	31/03/2026



Descripción

Dell EMC Smart Fabric OS10 es el sistema operativo de red (NOS) que se utiliza en las familias de enrutadores y conmutadores de las serie N (algunos modelos), serie S, serie Z y serie MX de Dell EMC Networking (las plataformas HW que actualmente soportan OS10 son N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n y MX9116n). Dell EMC SmartFabric OS10 es un sistema operativo de red (NOS) que admite múltiples arquitecturas y entornos. La solución SmartFabric OS10 permite la desagregación en varias capas de la funcionalidad de red. SmartFabric OS10 comprende la administración, monitorización y funcionalidad completa y estándar de la industria de redes de nivel 2 y nivel 3 a través de interfaces CLI, SNMP y REST. Los usuarios pueden elegir sus propias aplicaciones de organización, gestión, supervisión y redes de terceros. Para desarrollar redes escalables L2 y L3, SmartFabric OS10 ofrece una solución modular y desagregada en una única imagen binaria.

Observaciones

CCN-STIC-1429 PES DELL EMC Networking

Cisco Nexus 9200 Series Switches (92348GC-X, 92160YC-X, 92300YC, 9272Q)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	10/04/2025



Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9

Switches EXOS: x440-G2, x460-G2, x465, x435, x695, 5520, 5420

Versión	EXOS 31.3.100
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2023
Revisión de Validez	31/05/2025

**Descripción**

Familia de conmutadores apilables de alto rendimiento, que proporcionan conectividad gigabit, multigigabit, 10G, 25G, 40G y 100G. Los equipos pueden posicionarse tanto en el acceso como en la agregación en el núcleo, soportando protocolos de routing avanzado (BGP, MPLS, VXLAN, etc). También proporciona soluciones de implementación de Fabric

Observaciones

CCN-STIC-1446 PES Switches EXoS

Alcatel-Lucent Enterprise OmniSwitch Serie 6360 (OS6360-10, OS6360-P10, OS6360-24, OS6360-P24, OS6360-PH24, OS6360-P24X, OS6360-48, OS6360-P48, OS6360-P48X, OS6360-PH48)

Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2022
Revisión de Validez	28/02/2026

**Descripción**

OS6360: Familia de conmutadores L2+ apilables con puertos 1G y enlaces 1G/10G. Diseñados como equipos de acceso en redes convergentes de alta capacidad.

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Cisco Nexus 3200 Series Switches (3232C, 3264C-E)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 3500 Series Switches (3524-X/XL, 3548-X/XL)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 3600 Series Switches (36180YC-R, 3636C-R)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 3400 Series Switches (34180-YC, 3464C, 3432D-S, 3408-S)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	10/04/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 9300 Series Switches (93108TC-EX, 93108TC-FX, 9348GC-FXP, 93216TC-FX2, 93180LC-EX, 93180YC-EX, 93180YC-FX, 93240YC-FX2, 93360YC-FX2, 9364C, 9332C, 9336C-FX2, 9364C-GX, 9316D-GX, 93600CD-GX)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	04/10/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Cisco Nexus 9500 Series Switches (9504, 9508, 9516, Supervisor 9500-Sup-A , Supervisor 9500-Sup-A +, Supervisor 9500-Sup-B , Supervisor 9500-Sup-B +, System Controller N9k-SC-A)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2023
Revisión de Validez	04/10/2025

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.

Observaciones

CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9



Alcatel-Lucent Enterprise OmniSwitch Serie 6560 (OS6560-P24Z8, OS6560-P24Z24, OS6560-P48Z16, OS6560-24Z8, OS6560-24Z24, OS6560-24X4, OS6560-P24X4, OS6560-48X4, OS6560-P48X4 y OS6560-X10)

Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026



Descripción

Familia de conmutadores L3 compactos apilables con alta densidad de puertos 1GE, Multigigabit ethernet 1/2.5 GigE y enlaces 10GE, diseñados como equipos de acceso en redes convergentes de alta capacidad. <https://www.al-enterprise.com/es-es/productos/conmutadores>

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6900 (OS6900-X20, OS6900-X40, OS6900-T20, OS6900-T40, OS6900-X72, OS6900-Q32, OS6900-V72, OS6900-C32, OS6900-C32E, OS6900-X48C6, OS6900-T48C6, OS6900-X48C4E, OS6900-V48C8, OS6900-X24C2, OS6900-T24C2)

Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026



Descripción

OS6900: Familia de conmutadores L3+ compactos apilables de alta densidad 10GE, 25GE, 40GE y 100GE. Diseñadas para que sean flexibles. Pueden instalarse como conmutadores convergentes situados en la parte superior del bastidor (TOR) o tipo spine para entornos de Data Centers y también como dispositivos de agregación y de núcleo en una red de campus. <https://www.al-enterprise.com/es-es/productos/conmutadores>

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6865 (OS6865-P16X, OS6865-U12X y OS6865-U28X)

Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026

**Descripción**

OS6865: Familia de conmutadores L3+ con puertos 1G y 10G, preparados para entorno industrial o redes de misión crítica como transportes y utilities, con amplio rango de temperaturas de funcionamiento (-40°C a +75°C). <https://www.al-enterprise.com/es-es/productos/conmutadores>

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6860 (OS6860E-24, OS6860E-P24, OS6860E-48, OS6860E-P48, OS6860E-U28, OS6860E-P24Z8, TA6860E-P48, OS6860N-U28, OS6860N-P48Z, OS6860N-P48M, OS6860N-P24M, OS6860N-P24Z)

Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026

**Descripción**

OS6860: Familia de conmutadores L3+ compactos apilables con alta densidad de puertos 1GE, Multigigabit ethernet 1/2.5/5/10 GigE y enlaces 10GE, 25GE y 100GE, diseñadas para redes convergentes. Con funciones de Acceso unificado avanzadas que permiten la creación de redes orientadas a las aplicaciones. Puede supervisar y controlar las aplicaciones de la red mediante capacidades de Deep Packet Inspection (DPI). <https://www.al-enterprise.com/es-es/productos/conmutadores>

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 9900 (OS9907-CFM, OS99-CMM, OS99-XNI-48, OS99-XNI-U48, OS99-GNI-48, OS99-GNI-P48, OS99-CNI-U8, OS99-XNI-P24Z8, OS99-XNI-P48Z16, OS99-XNI-U12Q, OS99-XNI-U24, OS99-XNI-U48, OS99-GNI-U48, y OS99-XNI-UP24Q2)

Versión AOS 8.9.R01

Fabricante Alcatel-Lucent Enterprise

Familia Switches

Tipo Producto

Clasificación TODOS LOS NIVELES

Fecha Inclusión 01/04/2021

Revisión de Validez 28/02/2026

Descripción

OS9900: Conmutador LAN L3+ con chasis modular de alta capacidad de interfaces 1GE, 10GE y 100GE para conmutación segura y con alta disponibilidad en el núcleo de las redes empresariales, campus y redes Metro Ethernet. <https://www.al-enterprise.com/es-es/productos/conmutadores>

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS



Alcatel-Lucent Enterprise OmniSwitch Serie 6465 (OS6465-P6, TA6465-P6, OS6465-P12, TA6465-P12, OS6465-P28, TA6465-P28, OS6465T-P12 y OS6465T-12)

Versión AOS 8.9.R01

Fabricante Alcatel-Lucent Enterprise

Familia Switches

Tipo Producto

Clasificación TODOS LOS NIVELES

Fecha Inclusión 01/04/2021

Revisión de Validez 28/02/2026

Descripción

OS6465: Familia de conmutadores L2+ con puertos 1G y 10G, preparados para entorno industrial, con amplio rango de temperaturas de funcionamiento (-40°C a +75°C). Diseñados como equipos de acceso en redes de tipo industrial, transportes o utilities. <https://www.al-enterprise.com/es-es/productos/conmutadores>

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS



8.5.3 CORTAFUEGOS

Stormshield Network Security UTM/NG-Firewall (Appliances desde SN210 a SN6100 en 4 compilaciones distintas: S, M, L y XL).

Versión	4.3
Fabricante	Stormshield
Familia	Cortafuegos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2024
Revisión de Validez	31/03/2025



Descripción

Firewalls de nueva generación de capa 7, IPS y concentrador de túneles VPN. Con capacidades de bloqueo de amenazas avanzadas, ataques de día cero, filtrado de navegación web o gestión de vulnerabilidades. El mismo equipamiento realiza inspección profunda de protocolos OT, además de IT.

Observaciones

Procedimiento de Empleo Seguro Pendiente de publicación.

8.5.4 PASARELAS SEGURAS DE INTERCAMBIO DE DATOS

Pasarelas de intercambio seguro de información para sistemas específicos militares

Versión	No aplica
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2022
Revisión de Validez	01/05/2025



Descripción

Pasarelas desarrolladas ad-hoc para sistemas / protocolos específicos militares. ISR, Asterix, Datalink, ADEXP, etc. Consultar disponibilidad y estado de aprobación en itsec.ccn@cni.es o cpstic.ccn@cni.es.

Observaciones

N/A

PSTfile

Versión	v4.4.2
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2025



Descripción

PSTfile es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de ficheros entre dominios de seguridad. Se establece una correspondencia entre carpetas, en servidores de ficheros de ambas redes y PSTfile, automáticamente, mueve o copia los ficheros del origen al destino. Soporta los protocolos FTP, FTPS, SFTP y SMB. La transferencia de ficheros desde el dominio de alta seguridad al de baja requiere autorización mediante firma digital.

Observaciones

Procedimiento de empleo seguro: CCN-STIC-1401 Configuración segura de pasarelas de AUTEK

PSTmail

Versión	v3.0.5
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2025

**Descripción**

PSTmail es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de correo electrónico entre dominios de seguridad. Posibilita el empleo de direcciones de correo de redes externas, desde una red interna, más segura. Soporta las versiones seguras de los protocolos de correo. Los mensajes de salida requieren autorización mediante firma digital (S/MIME).

Observaciones

Procedimiento de empleo seguro: CCN-STIC-1401 Configuración segura de pasarelas de AUTEK

8.5.5 DIODOS DE DATOS

PSTdiode

Versión	v1.3.1-A
Fabricante	Autek Ingeniería
Familia	Diodos de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2019
Revisión de Validez	31/12/2024



Descripción

El diodo de datos hardware PSTdiode es un dispositivo de protección de perímetro que permite la transferencia de información en un único sentido entre dos dominios de seguridad con garantía física de transmisión unidireccional. Su aplicación principal es la introducción de información en una red aislada en entornos clasificados. También se puede aplicar para extraer información de una red de control industrial en entornos de infraestructuras críticas. En ambos casos se garantiza que no existe tráfico en el sentido inverso. Existen modelos de transferencia de ficheros y tráfico UDP.

Observaciones

Procedimiento de empleo seguro: CCN-STIC 1408 Procedimiento de empleo seguro Diodo Autek Ingeniería

8.5.6 HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA (IM)

COMSec Admin +

Versión	v4.2
Fabricante	Indra
Familia	Herramientas de mensajería instantánea (IM)
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/12/2024



Descripción

COMSec Admin+ es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con su alto nivel de seguridad, gran calidad de audio y facilidad de uso protege de forma eficaz información clasificada (hasta difusión limitada) de la organización. Las llamadas y los datos intercambiados por COMSec son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: comsec.indracompany.com

Observaciones

Utilización según el PE-2018-24 Procedimiento de empleo COMSec Admin + v2 Para su empleo en entornos tácticos o desplegables, este producto deberá emplearse sobre un dispositivo móvil perteneciente a la familia "plataformas y dispositivos tácticos confiables"

8.5.7 HERRAMIENTAS VOZ IP

COMSec Admin +

Versión	v4.2
Fabricante	Indra
Familia	Herramientas Voz IP
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/12/2024

Descripción

COMSec Admin+ es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con su alto nivel de seguridad, gran calidad de audio y facilidad de uso protege de forma eficaz información clasificada (hasta difusión limitada) de la organización. Las llamadas y los datos intercambiados por COMSec son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: comsec.indracompany.com

Observaciones

Utilización según el PE-2018-24 Procedimiento de empleo COMSec Admin + v2 Para su empleo en entornos tácticos o desplegables, este producto deberá emplearse sobre un dispositivo móvil perteneciente a la familia "plataformas y dispositivos tácticos confiables"



8.5.8 CIFRADORES IP

EP430GU/B

Versión	2.01
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	01/09/2020
Revisión de Validez	31/12/2025



Descripción

El cifrador IP EP430 GU/B está basado en el cifrador IP EP430GU, sobre el que se han sustituido los mecanismos criptográficos por algoritmos tipo B. Está compuesto por una plataforma de comunicaciones EP430G+ y un módulo cripto EP940+ programado como EP940U/B (software y firmware). Es un cifrador a 1Gbps, diseñado para operar en la capa 3 del modelo OSI, lo que permite el despliegue de redes privadas virtuales (VPN, Virtual Private Networks) de una forma completamente segura.

Observaciones

Utilización según PE-2019-9 Procedimiento de Empleo EP430GU/B

EP430TX

Versión	1.04
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Clasificación	SECRETO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2024



Descripción

Cifrador de comunicaciones IP hasta 200 Mbps, interoperable con el resto de cifradores de la familia EP430.

Observaciones

Utilización según PE-2016-28 Procedimiento de empleo EP430TX.

EP430GX

Versión	v.1.08
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Clasificación	SECRETO
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2024

**Descripción**

Cifrador de redes IP a 2 Gbps (agregados), interoperable con el resto de cifradores de la familia EP430.

Observaciones

Utilización según PE-2012-49 Procedimiento de Empleo EP430GX.

EP430GN

Versión	v2.04
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Clasificación	RESERVADO
Fecha Inclusión	01/12/2022
Revisión de Validez	31/12/2024

**Descripción**

Cifrador de redes IP a 2 Gbps (agregados).

Observaciones

Este modelo no es compatible con el resto de la familia de cifradores EP430 de EPICOM. Utilización según P029-PE-2011-33 Operational doctrine EP430GN v2.

EP430GN

Versión	1.12
Fabricante	EPICOM S.A.
Familia	Cifradores IP
Tipo	Producto
Clasificación	RESERVADO
Fecha Inclusión	01/12/2022
Revisión de Validez	31/12/2024

**Descripción**

Cifrador de redes IP a 2 Gbps (agregados).

Observaciones

Este modelo no es compatible con el resto de la familia de cifradores EP430 de EPICOM. Utilización según P029-PE-2011-33 Operational doctrine EP430GN v2.

EP430GN

Versión	2.5
Fabricante	EPICOM S.A.
Familia	Cifradores IP
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/06/2024
Revisión de Validez	31/12/2026

**Descripción**

Cifrador de redes IP a 2 Gbps (agregados).

Observaciones

Este modelo no es compatible con el resto de la familia de cifradores EP430 de EPICOM. Utilización según P029-PE-2011-33 Operational doctrine EP430GN v2.

EP430GN

Versión	1.08.29
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Clasificación	RESERVADO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2024

**Descripción**

Cifrador de redes IP a 2 Gbps (agregados).

Observaciones

Este modelo no es compatible con el resto de la familia de cifradores EP430 de EPICOM. Utilización según P029-PE-2011-33 Operational doctrine EP430GN v2.

8.6 PROTECCIÓN DE LA INFORMACIÓN Y LOS SOPORTES DE LA INFORMACIÓN

8.6.1 CIFRADO Y COMPARTICIÓN SEGURA DE INFORMACIÓN

EP852	
Versión	3.05
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2025
Descripción El EP852 es un cifrador de ficheros fuera de línea que permite el cifrado y descifrado de ficheros y el transporte de información cifrada en el dispositivo. Mejora las prestaciones en cuanto a almacenamiento y velocidad de las versiones anteriores de los Token USB así como la puesta en marcha del dispositivo, carga y distribución de claves.	
Observaciones Utilización según el PE-2020-4 -Procedimiento de Empleo Seguro EP852 -(ESP)	



EP880	
Versión	V2.08.36 y V2.09.35
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2026
Descripción El EP880 es una aplicación software que se ejecuta sobre ordenador con sistema operativo Windows y que permite realizar, en origen, el cifrado y firma de ficheros de datos "off-line" almacenados en el disco duro del ordenador o dispositivos de almacenamiento externos conectados al ordenador, para su posterior almacenamiento y/o envío de forma segura desde el correo electrónico u otro medio y, en destino, el descifrado y verificación de la integridad de los datos.	
Observaciones CCN-STIC-1506 Procedimiento de Empleo Seguro EP880	



EP852

Versión	3.04
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2025

**Descripción**

El EP852 es un cifrador de ficheros fuera de línea que permite el cifrado y descifrado de ficheros y el transporte de información cifrada en el dispositivo. Mejora las prestaciones en cuanto a almacenamiento y velocidad de las versiones anteriores de los Token USB así como la puesta en marcha del dispositivo, carga y distribución de claves.

Observaciones

Utilización según el PE-2020-4 -Procedimiento de Empleo Seguro EP852 -(ESP)

8.6.2 HERRAMIENTAS DE BORRADO SEGURO

OLVIDO Windows	
Versión	1.0.6
Fabricante	authUSB
Familia	Herramientas de borrado seguro
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2022
Revisión de Validez	28/02/2025
Descripción	  OLVIDO es una herramienta de borrado seguro que realiza tareas de sobreescritura y borrado sobre los sistemas de archivos y discos reconocidos. Ofrece al usuario la posibilidad de borrar de forma segura distintos elementos guardados en los dispositivos de almacenamiento: - Ficheros y carpetas - Espacio Libre - Fragmentos de clúster no utilizados - Discos y volúmenes Dispone de un módulo de planificación con el que se permite al usuario programar la ejecución de las tareas de borrado. OLVIDO implementa distintos algoritmos estándar de borrado y permite al usuario seleccionar el algoritmo de borrado a aplicar en cada tarea. Así mismo, ofrece la posibilidad al administrador de definir algoritmos de borrado personalizados, especificando el número de pases y el patrón de sobreescritura. Permite la integración con un servidor Syslog para el envío de registros de actividad y estado de las tareas de borrado realizadas. La versión aprobada permite, con el algoritmo de borrado CCN-Clasificado, la reclasificación y desclasificación de: - Discos magnéticos hasta RESERVADO o equivalente. - Discos SSD hasta DIFUSIÓN LIMITADA o equivalente. Se ejecuta sobre Windows 10, Windows Server 2016 y Windows Server 2021. Observaciones CCN-STIC-1508 Procedimiento de empleo seguro OLVIDO

8.6.3 GESTIÓN DE METADATOS

MetaClean Sync Workstation y MetaClean Sync Server

Versión	2.3.0
Fabricante	Adarsus Technologies S.L
Familia	Gestión de metadatos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2024
Revisión de Validez	30/04/2026



Descripción

MetaClean Sync Workstation y MetaClean Sync Server: Herramienta de gestión de metadatos que permite aplicar políticas de seguridad corporativas de prevención de fugas de información, limpiando los metadatos e información sensible oculta en los ficheros ofimáticos generados en una organización. Realiza una protección continua y en tiempo real de los metadatos de una estación de trabajo o Servidor. Protege la información de manera sencilla y desatendida. Permite configurar reglas y ponerlas en práctica sobre los archivos documentales o multimedia que se considere necesario, ya sea en los equipos de usuario -Workstation- o en carpetas de red compartidas -Server-.

Observaciones

CCN-STIC 1511 Procedimiento de Empleo Seguro metaOLVIDO EndPoint y metaOLVIDO Server

MetaClean Dashboard

Versión	1.3.0
Fabricante	Adarsus Technologies S.L
Familia	Gestión de metadatos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/05/2024
Revisión de Validez	30/04/2026



Descripción

MetaClean Dashboard: Consola de administración de MetaClean para las distintas modalidades de despliegue. Administra, centraliza y controla la aplicación de políticas preventivas de seguridad corporativas. Permite obtener estadísticas de los metadatos procesados y controlar la exfiltración de información de forma global.

Observaciones

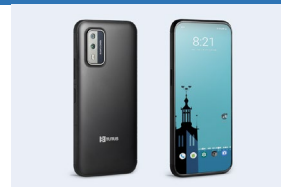
CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard

8.7 PROTECCIÓN DE EQUIPOS Y SERVICIOS

8.7.1 DISPOSITIVOS MÓVILES

Färist Mobile en Nokia XR21 (FM T140)

Versión	7.7
Fabricante	Tutus
Familia	Dispositivos móviles
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	26/01/2024
Revisión de Validez	26/04/2026



Descripción

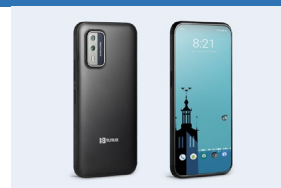
Sistema de comunicación seguro de terminales móviles basado en S.O. Android. El Färist Mobile System además de proteger la comunicación protege la plataforma (Nokia XR21) para almacenar información clasificada hasta el grado de Difusión Limitada.

Observaciones

Utilización según PE-2022-2 Comercializado en España por la empresa Epicom.

Färist Mobile en Nokia XR21 (FM T140)

Versión	7.4
Fabricante	Tutus
Familia	Dispositivos móviles
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	26/01/2024
Revisión de Validez	26/04/2026



Descripción

Sistema de comunicación seguro de terminales móviles basado en S.O. Android. El Färist Mobile System además de proteger la comunicación protege la plataforma (Nokia XR21) para almacenar información clasificada hasta el grado de Difusión Limitada.

Observaciones

Utilización según PE-2022-2 Comercializado en España por la empresa Epicom.

Färist Mobile en Bittium Tough Mobile 2 (FM T200)

Versión	7.4
Fabricante	Tutus
Familia	Dispositivos móviles
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	26/01/2024
Revisión de Validez	26/04/2026

**Descripción**

Sistema de comunicación seguro de terminales móviles basado en S.O. Android. El Färist Mobile System además de proteger la comunicación protege la plataforma (Bittium Tough Mobile 2) para almacenar información clasificada hasta el grado de Difusión Limitada.

Observaciones

Utilización según PE-2022-2 Comercializado en España por la empresa Epicom.

Färist Mobile en Google Pixel 4A 5G (FM T120)

Versión	7.4
Fabricante	Tutus
Familia	Dispositivos móviles
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	26/01/2024
Revisión de Validez	14/07/2025

**Descripción**

Sistema de comunicación seguro de terminales móviles basado en S.O. Android. El Färist Mobile System además de proteger la comunicación protege la plataforma (Google Pixel 4A 5G) para almacenar información clasificada hasta el grado de Difusión Limitada.

Observaciones

Utilización según PE-2022-2 Comercializado en España por la empresa Epicom.

8.7.2 SISTEMAS OPERATIVOS

Windows Server 2016

Versión	Datacenter Edition
Fabricante	Microsoft Corporation
Familia	Sistemas Operativos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2018
Revisión de Validez	12/01/2027



Descripción

Sistema Operativo para servidores

Observaciones

CCN-STIC-570A, CCN-STIC-570B Anexo A

SUSE Linux Enterprise

Versión	Server 15 SP2
Fabricante	SUSE Software Solutions
Familia	Sistemas Operativos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2022
Revisión de Validez	31/12/2024



Descripción

SUSE® Linux Enterprise Server (SLES) 15 SP2 es un sistema operativo (SO) modular que ayuda a simplificar el entorno IT, modernizar la infraestructura IT y acelerar la innovación. SLES se adapta a cualquier entorno operativo a la vez que satisface los requisitos de rendimiento, seguridad y confiabilidad. Es una plataforma fácil de administrar para desarrolladores y administradores que permite implementar cargas de trabajo críticas para el negocio en las instalaciones, en la nube y en el perímetro.

Observaciones

CCN-STIC-1615 Procedimiento de empleo seguro SUSE 15 SP2

8.7.3 PROTECCIÓN DE CORREO ELECTRÓNICO

Cisco Email Security Appliance (C190, C195, C390, C395, C690, C690X, C695, C695F, C100v, C300v y C600v)

Versión	AsyncOS 13.0
Fabricante	Cisco Systems
Familia	Protección de correo electrónico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2023
Revisión de Validez	31/05/2025



Descripción

Cisco Email Security Appliance es una pasarela de seguridad para el correo electrónico. Está diseñado para detectar y bloquear una amplia variedad de amenazas transmitidas por correo electrónico, como malware, spam e intentos de phishing.

Observaciones

CCN-STIC 1623 Procedimiento de Empleo Seguro Cisco Email Security Appliance

8.7.4 HIPERCONVERGENCIA

KATUA SDI PLATFORM

Versión	1.0
Fabricante	KRC ESPAÑOLA S.A.
Familia	Hiperconvergencia
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2021
Revisión de Validez	31/01/2025



Descripción

Katua®SDI Platform es una plataforma hiperconvergente escalable y segura, basada en el concepto Software Define Infrastructure, donde todos los elementos que conforman un CPD se definen en una única plataforma hardware y software. Permite el despliegue rápido de servicios (xaaS), consolidación de CPDs, SDN y tiene capacidad de instalación desde equipos móviles hasta grandes centros de procesos de datos. Su flexibilidad permite que se puedan desplegar servicios cloud sobre la plataforma de forma sencilla y eficiente. Dispone de la capacidad para generar bibliotecas de sistemas preconfigurados para su despliegue con un click a través de su interfaz web. Las capacidades de optimización del hipervisor aseguran un rendimiento máximo de la plataforma, haciendo uso de todos los recursos disponibles y ofreciendo de esta forma capacidad de instalación en nodos pequeños y configuraciones hardware básicas. Su capacidad para integrarse con sistemas de almacenamiento masivos, ya sean locales o remotos permite escalar la solución en función de las necesidades. Para más información de la plataforma, visita nuestra web <https://www.krc.es>

Observaciones

CCN-STIC-1610 Procedimiento de Empleo Seguro KATUA SDI Platform

8.8 OTRAS HERRAMIENTAS

8.8.1 OTRAS HERRAMIENTAS

STSKTA-MIN-TP

Versión
Fabricante KRC ESPAÑOLA S.A.

Familia Otras Herramientas

Tipo Producto

Clasificación SDIP-27/2 Level B

Fecha Inclusión 17/10/2024

Revisión de Validez 17/10/2026

Descripción

Servidor de almacenamiento (NAS/SAN) con capacidades avanzadas en la compartición de recursos y en formato de 1U extra corto para despliegue en zonas de clasificación ZONA 1, o donde se requiera de protección a una distancia libre de más 20 metros y a una distancia equivalente a través de paredes y obstáculos.

Observaciones

N/A



metaOLVIDO Dashboard (modalidad on-premise)

Versión 1.3.0

Fabricante Adarsus Technologies S.L

Familia Otras Herramientas

Tipo Producto

Clasificación TODOS LOS NIVELES

Fecha Inclusión 01/05/2024

Revisión de Validez 30/04/2026

Descripción

metaOLVIDO Dashboard: Consola de administración de metaOLVIDO para las distintas modalidades de despliegue. Administra, centraliza y controla la aplicación de políticas preventivas de seguridad corporativas. Permite obtener estadísticas de los metadatos procesados y controlar la exfiltración de información de forma global.

Observaciones

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard



metaOLVIDO Endpoint y metaOLVIDO Server

Versión	2.3.0
Fabricante	Adarsus Technologies S.L
Familia	Otras Herramientas
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2024
Revisión de Validez	30/04/2026

**Descripción**

metaOLVIDO EndPoint y metaOLVIDO Server: Herramienta de gestión de metadatos que permite aplicar políticas de seguridad corporativas de prevención de fugas de información, limpiando los metadatos e información sensible oculta en los ficheros ofimáticos generados en una organización.

Realiza una protección continua y en tiempo real de los metadatos de una estación de trabajo o Servidor. Protege la información de manera sencilla y desatendida. Permite configurar reglas y ponerlas en práctica sobre los archivos documentales o multimedia que se considere necesario, ya sea en los equipos de usuario -EndPoint- o en carpetas de red compartidas -Server-.

Observaciones

CCN-STIC 1511 Procedimiento de Empleo Seguro metaOLVIDO EndPoint y metaOLVIDO Server

authUsb safeDoor

Versión	2.0.0.11
Fabricante	AUTHUSB
Familia	Otras Herramientas
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2019
Revisión de Validez	31/12/2024

**Descripción**

AuthUsb safeDoor es un dispositivo hardware que actúa como barrera entre las memorias USB y los equipos de una organización, identificando amenazas a tres niveles: -Eléctrico: identificando y deteniendo ataques destructivos de sobretensión tipo UsbKiller. -Hardware: detectando y desactivando ataques de la familia BadUsb, ataques HID (rubber ducky y similares), falsas tarjetas de red, interfaces compuestas, etc. -Software: antivirus integrado que realiza un análisis previo a la descarga de cualquier contenido.

Observaciones

CCN-STIC 1201 Procedimiento de Empleo Seguro AuthUsb SafeDoor

8.9 COMUNICACIONES TÁCTICAS SEGURAS

8.9.1 PLATAFORMAS Y DISPOSITIVOS TÁCTICOS CONFIABLES

GETAC F110

Versión	G6 con firmware 15.0.35.1951
Fabricante	GETAC
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/10/2023
Revisión de Validez	14/10/2025



Descripción

Tableta robusta diseñada para dar soporte a usuarios civiles y militares. Este dispositivo se considera una plataforma confiable donde ejecutar aplicaciones software de forma protegida (p.ej.: aplicaciones de mando y control). El sistema operativo de la tableta es Windows 10 IoT Enterprise 21H2 LTSB. La tableta incluye un TPM 2.0.

Observaciones

CCN-STIC-1628 Procedimiento de empleo seguro GETAC F110G6

GETAC F110

Versión	G4 con firmware GETAC R1.12.070520
Fabricante	GETAC
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/06/2019
Revisión de Validez	14/10/2025



Descripción

Tableta robusta diseñada para dar soporte a usuarios civiles y militares. Este dispositivo se considera una plataforma confiable donde ejecutar aplicaciones software de forma protegida (p.ej.: aplicaciones de mando y control). El sistema operativo de la tableta es Windows 10 Enterprise 1607 LTSB. La tableta incluye un TPM 2.0.

Observaciones

Configuración y empleo seguro según la CCN-STIC-1605. Para protección de las comunicaciones en tránsito es necesario un producto aprobado perteneciente a la familia "soluciones para protección de las comunicaciones tácticas".

GETAC F110

Versión	G5 con firmware GETAC 12.0.45.1509
Fabricante	GETAC
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/06/2021
Revisión de Validez	14/10/2025

**Descripción**

Tableta robusta diseñada para dar soporte a usuarios civiles y militares. Este dispositivo se considera una plataforma confiable donde ejecutar aplicaciones software de forma protegida (p.ej.: aplicaciones de mando y control). El sistema operativo de la tableta es Windows 10 Enterprise 1607 LTSB. La tableta incluye un TPM 2.0.

Observaciones

Configuración y empleo seguro según la CCN-STIC-1609. Para protección de las comunicaciones en tránsito es necesario un producto aprobado perteneciente a la familia "soluciones para protección de las comunicaciones tácticas".

HP Elitebook 840

Versión	G7 y G8
Fabricante	HP PRINTING AND COMPUTING SOLUTIONS SL
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/09/2021
Revisión de Validez	14/10/2025

**Descripción**

Equipos portátiles con sistema operativo Windows 10 Enterprise, Versión 20H2, Compilación (19042.1023) securizable mediante la aplicación de las guías STIC para manejo de información clasificada.

Observaciones

Plataforma bastionada según CCN-STIC 599B19

8.9.2 SOLUCIONES PARA PROTECCIÓN DE LAS COMUNICACIONES TÁCTICAS

Bittium SafeMove VPN Client for Android

Versión	Android (genérico): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb
Fabricante	Bittium
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/06/2025

Bittium



Descripción

SafeMove Mobile VPN forma parte de la Bittium Secure Suite. Proporciona los servicios de firewall y VPN IPSec a las plataformas Android y Windows conectadas de forma remota a la infraestructura corporativa, y está concebido para ser un servicio siempre activo y aplicado a todo el tráfico de red que entra y sale del dispositivo. Nada sensible se escapa, nada dañino puede entrar. La SafeMove Mobile VPN es una solución cliente-servidor. El cliente instalado en el dispositivo se conecta a la puerta de enlace Bittium SafeMove VPN Gateway instalada en el servidor, con el resto de los componentes de la Bittium Secure Suite, que son el gestor de dispositivos (MDM), el gestor de las aplicaciones instaladas en los dispositivos (solo Android) y los servicios de comprobación de la integridad (solo Android). Usado en combinación con los smartphones de la familia Bittium Tough Mobile proporciona servicios de recuperación de los registros de auditoría y actualización OTA del firmware de los dispositivos. Más información de Bittium SafeMove® Mobile VPN: <https://www.bittium.com/secure-communications-connectivity/bittium-safemove-mobile-vpn>

Observaciones

PE-2021-7-Procedimiento de empleo seguro Bittium SafeMove VPN (Android y Windows)

TZ-2001R-MC

Versión	SW 1.8 y 1.8.1
Fabricante	TECNOBIT
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/06/2025

**Descripción**

El TZ-2001R-MC es una aplicación de cifrado software para sistemas Windows que se ejecuta como un servicio del Sistema Operativo a disposición de otras aplicaciones (típicamente aplicaciones de mando y control). Proporciona las siguientes capacidades de cifrado:

- a) Cifrado de voz táctica ("push to talk") según varios estándares (SCIP multipunto, STaC-IS 2400, TSVCIS 600, TSVCIS 1200, TSVCIS 600/2400 y TSVCIS 1200/2400).
- b) Cifrado de datos IP en modo transporte (solo "payload"), estando disponible un modo autenticado (AES-GCM) y un modo no autenticado (AES-CTR).
- c) Cifrado no autenticado (AES-CTR) de los datos DAP del Sistema BMS-ET que se transmiten por el TDMA de la radio F@stnet PR4G.

En sus modos de cifra de voz táctica y datos IP, el TZ-2001R-MC es interoperable con otros productos de la familia CIFPECOM, tales como el TZ-1001R o la Unidad de Comunicaciones Seguras con módulo de seguridad TZ-501. El TZ-2001R-MC se configura con el mismo centro de gestión (CMAP) que el TZ-1001R y el TZ-501.

Observaciones

Según su procedimiento de empleo, el TZ-2001R-MC deberá ejecutarse sobre una plataforma Windows cualificada como confiable, o en su defecto en una estación de trabajo bastionada conforme a lo requerido en la CCN-STIC-599 para manejar información DIFUSIÓN LIMITADA. La mayor parte de las funciones de seguridad lógica residen en la plataforma Windows que se emplee. Utilización según el Procedimiento de Empleo Seguro T00741700PDE001 Ed. 01.

TZ-1001R

Versión	V4.26
Fabricante	TECNOBIT
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/10/2020
Revisión de Validez	31/12/2024

**Descripción**

El TZ-1001R es un cifrador táctico de pequeño tamaño para la protección de las comunicaciones sobre redes de bajo ancho de banda y sin estabilidad de enlace garantizada. Cuenta con dos modos de operación diferenciados: como cifrador en línea (modo “tactical crypto”), o alternativamente en modo “slave crypto” como elemento de cifra esclavo de otro elemento que gestiona la interacción con los medios de transmisión y con el usuario (caso del Gestor de Comunicaciones del ET). El TZ-1001R tiene capacidad para cifrar de forma simultánea varios flujos de voz táctica (“push to talk”) según varios estándares OTAN, pudiendo elegirse en cada caso el más adecuado según el tipo de radio por el que se va a realizar la transmisión. Simultáneamente también puede cifrar datos IP unicast y multicast. Cuando el cifrador se configura en modo “tactical crypto” implementa IPsec con asociaciones de seguridad manuales. En configuración “slave crypto” el TZ-1001R implementa un protocolo específico de cifra IP para facilitar la integración con los sistemas CIS de dotación. En modo “slave crypto” la cifra del TZ-1001R es interoperable con la cifra del TZ-501 (módulo de seguridad de la UCS) y con la aplicación de cifrado para S.O. Windows TZ-2001.

Observaciones

Utilización según el Procedimiento de empleo T90431000PDE003 v2.0

Bittium SafeMove VPN Client for Windows

Versión	4.11.722
Fabricante	Bittium
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/06/2025


**Descripción**

SafeMove Mobile VPN forma parte de la Bittium Secure Suite. Proporciona los servicios de firewall y VPN IPSec a las plataformas Android y Windows conectadas de forma remota a la infraestructura corporativa, y está concebido para ser un servicio siempre activo y aplicado a todo el tráfico de red que entra y sale del dispositivo. Nada sensible se escapa, nada dañino puede entrar. La SafeMove Mobile VPN es una solución cliente-servidor. El cliente instalado en el dispositivo se conecta a la puerta de enlace Bittium SafeMove VPN Gateway instalada en el servidor, con el resto de los componentes de la Bittium Secure Suite, que son el gestor de dispositivos (MDM), el gestor de las aplicaciones instaladas en los dispositivos (solo Android) y los servicios de comprobación de la integridad (solo Android). Usado en combinación con los smartphones de la familia Bittium Tough Mobile proporciona servicios de recuperación de los registros de auditoría y actualización OTA del firmware de los dispositivos. Más información de Bittium SafeMove® Mobile VPN: <https://www.bittium.com/secure-communications-connectivity/bittium-safemove-mobile-vpn>

Observaciones

PE-2021-7-Procedimiento de empleo seguro Bittium SafeMove VPN (Android y Windows)

COMSec Admin +

Versión	v4.2
Fabricante	Indra
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/12/2024

**Descripción**

COMSec Admin+ es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con su alto nivel de seguridad, gran calidad de audio y facilidad de uso protege de forma eficaz información clasificada (hasta difusión limitada) de la organización. Las llamadas y los datos intercambiados por COMSec son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: comsec.indracompany.com

Observaciones

Utilización según el PE-2018-24 Procedimiento de empleo COMSec Admin + v2 Para su empleo en entornos tácticos o desplegables, este producto deberá emplearse sobre un dispositivo móvil perteneciente a la familia "plataformas y dispositivos tácticos confiables"

Unidad de Comunicaciones Seguras (UCS) con módulo de seguridad TZ-501

Versión	UCS v2.4 con TZ-501 (versión SW 4.26)
Fabricante	TECNOBIT y RF Española
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/09/2021
Revisión de Validez	31/12/2024

**Descripción**

La UCS es un gestor de comunicaciones para su uso en entornos tácticos militares en los que se requiere contar con comunicaciones seguras tanto de voz táctica CNR como de de datos IP. La UCS permite la conexión de varias radios tácticas, u otros medios CIS, que actúan como medio de transporte. El sistema incorpora un módulo de gestión de radiofonía, un módulo para la gestión de la interfonía y un servidor de telefonía de Voz IP para la integración con equipos telefónicos SIP, todo ello acompañado de un módulo de cifrado seguro, denominado TZ-501. El TZ-501 es el módulo encargado de cifrar la voz táctica según estándares OTAN, así como los datos IP unicast y multicast. La UCS cuenta con una "Crypto Ignition Key" (CIK) para el arranque seguro del equipo, y que además facilita el transporte y almacenamiento del equipo (sin la CIK la UCS se considera un equipo no clasificado). La cifra del TZ-501 es compatible con la cifra del TZ-1001R en modo "slave-crypto" y con la cifra del TZ-2001.

Observaciones

Utilización según el Procedimiento de Empleo Seguro T00741600PDE001 V3

8.10 TEMPEST

8.10.1 ARMARIOS APANTALLADOS

P.AT-02D

Versión

Fabricante CONSUEGRA S. COOP.

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2025

Descripción

Armario apantallado de 19" y hasta 730 mm de longitud. Puertas delanteras acristaladas y puertas laterales ciegas. Filtros de alimentación independientes de 6A. Aireación mediante electroventiladores. Apto para instalación en locales con clasificación de ZONA 0 con equipos clasificados ZONA 2.

Observaciones


P.AT-06D

Versión

Fabricante CONSUEGRA S. COOP.

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2025

Descripción

Armario apantallado ciego de 25U. Dimensiones 1524x625x1000 mm. Ventilación a través de 2 ventiladores con termostatos independientes con caudal de hasta 2.700 m3/h. Distribuidor interno con diferencial y automático. Apto para instalación en locales con clasificación de ZONA 0.

Observaciones


P.AT-06E

Versión**Fabricante** CONSUEGRA S. COOP.**Familia** Armarios apantallados**Tipo** Producto**Clasificación** Apto ZONA 0**Fecha Inclusión** 01/12/2017**Revisión de Validez** 30/06/2025**Descripción**

Armario apantallado ciego de 38U. Dimensiones 2102x625x1000 mm. Ventilación a través de 2 ventiladores con termostatos independientes con caudal de hasta 2.700 m3/h. Distribuidor interno con diferencial y automático. Apto para instalación en locales con clasificación de ZONA 0.

Observaciones

P.AT-07

Versión

—

Fabricante CONSUEGRA S. COOP.**Familia** Armarios apantallados**Tipo** Producto**Clasificación** Apto ZONA 0**Fecha Inclusión** 01/12/2017**Revisión de Validez** 31/05/2025**Descripción**

Armario apantallado para CPU. Dispone de bandeja extraíble, ventilación y filtrado de las líneas de datos y alimentación. Apto para instalación en locales con clasificación ZONA 0.

Observaciones

SHATEM - SHELTER ARPA TEMPEST MULTIPROPOSITO

Versión**Fabricante** ARPA, EQUIPOS MÓVILES DE CAMPAÑA**Familia** Armarios apantallados**Tipo** Producto**Clasificación** Apto ZONA 0**Fecha Inclusión** 01/01/2020**Revisión de Validez** 31/05/2025**Descripción**

Contenedor shelter para alojamiento y/o operación de equipos informáticos, electrónicos, optrónicos de telecomunicaciones y asimilables para entornos CIS. Equipado con los elementos de filtrado y protección EMI necesarios en acometidas de potencia, datos y servicios para disponer de apantallamiento intergral TEMPEST frente a emanaciones comprometedoras radiadas y conducidas.

Observaciones

P.AT07D

Versión

—

Fabricante CONSUEGRA S. COOP.**Familia** Armarios apantallados**Tipo** Producto**Clasificación** Apto ZONA 0**Fecha Inclusión** 01/04/2019**Revisión de Validez** 31/10/2025**Descripción**

Armario Tempest de sobremesa de dimensiones reducidas con dos posibles opciones. El armario PAT 07D ofrece alta protección electromagnética para que el cliente incluya su propia CPU, convirtiendo el conjunto en una CPU Tempest aceptada para procesar información clasificada en locales ZONA 0. CONSUEGRA se ocupa de las adaptaciones necesarias para su correcta instalación y funcionamiento. Posteriormente, si el cliente deseara cambiar la CPU por una más actualizada, CONSUEGRA también puede ocuparse de su instalación y funcionamiento. CONSUEGRA también ofrece la posibilidad de suministrar e instalar la CPU solicitada por el cliente como parte del pedido, en este caso, el producto se codifica como P.COMPT0-03.

Observaciones

8.10.2 MONITORES

P.MONT0-11

Versión	—
Fabricante	CONSUEGRA S. COOP.
Familia	Monitores
Tipo	Producto
Clasificación	SDIP-27 Level A
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2025



Descripción

Monitor LED Full HD de 22" y resolución 1920 x 1080p con formato panorámico.

Observaciones

8.10.3 PERIFÉRICOS

P.KVMT0-01

Versión
Fabricante CONSUEGRA S. COOP.

Familia Periféricos

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2025

Descripción

Conmutador KVM para dos sistemas. Basado en BELKIN SECURE OMNIVIEW F1DN102Uea con certificación NIAP EAL 4+.

Observaciones


P.TECT0-07

Versión
Fabricante CONSUEGRA S. COOP.

Familia Periféricos

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2025

Descripción

Teclado QWERTY español. Conexión USB.

Observaciones


P.RATT0-04

Versión	—
Fabricante	CONSUEGRA S. COOP.
Familia	Periféricos
Tipo	Producto
Clasificación	SDIP-27 Level A
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2025

**Descripción**

Ratón óptico USB

Observaciones

8.10.4 CPU

P.COMPT0-06

Versión	—
Fabricante	CONSUEGRA S. COOP.
Familia	CPU
Tipo	Producto
Clasificación	SDIP-27 Level A
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2025

**Descripción**

CPU de sobremesa tempestizada del modelo comercial HP PRODESK 600 G5 SFF. Aprobado para su uso combinado con periféricos TEMPEST de la empresa CONSUEGRA S.COOP. en locales con clasificación de ZONA 0.

Observaciones

P.COMT0-01

Versión	—
Fabricante	CONSUEGRA S. COOP.
Familia	CPU
Tipo	Producto
Clasificación	SDIP-27 Level A
Fecha Inclusión	01/06/2018
Revisión de Validez	31/01/2025

**Descripción**

CPU de sobremesa tempestizada del modelo comercial HP ELITE 8000. Aprobado para su uso combinado con periféricos TEMPEST de la empresa CONSUEGRA S. COOP. en locales con clasificación de ZONA 0.

Observaciones

8.10.5 IMPRESORAS

P.IMPT0-04

Versión

—

Fabricante

CONSUEGRA S. COOP.

Familia

Impresoras

Tipo

Producto

Clasificación

SDIP-27 Level A

Fecha Inclusión

01/12/2021

Revisión de Validez

31/05/2025

Descripción

Impresora TEMPEST basada en el model HP Color LaserJet Enterprise M553dn.

Observaciones



8.10.6 SERVIDOR

SOC-1-TP

Versión	-
Fabricante	KRC ESPAÑOLA S.A.
Familia	Servidor
Tipo	Producto
Clasificación	SDIP-27/2 Level B
Fecha Inclusión	15/10/2023
Revisión de Validez	26/10/2025



Descripción

Servidor multipropósito de alto rendimiento orientado a despliegues en entornos móviles, donde el consumo y el espacio son elementos críticos.

Sus capacidades le permiten actuar como servidor multifuncional e incluso ofrecer servicios de virtualización en una red con requerimientos medios. Compatible con distintos sistemas operativos.

Observaciones

N/A

9. PRODUCTOS Y SERVICIOS DE CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD

PRODUCTOS Y SERVICIOS DE CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD



9.1 GOBERNANZA Y PLANIFICACIÓN DE LA SEGURIDAD

LightHouse Vulnerability Manager

Versión
Fabricante INNOTECH SYSTEM

Familia Gobernanza y Planificación de la Seguridad

Tipo Servicio

Fecha Inclusión 01/04/2023

Revisión de Validez 31/03/2025

Descripción

LightHouse VM (Vulnerability Management) de Innotec Security es la plataforma de auditoría continua para la detección y priorización de riesgos de una organización, permitiendo optimizar esfuerzos y personalizar la gestión, acortando el tiempo de exposición frente a las amenazas.

LightHouse es la herramienta perfecta para la gestión de vulnerabilidades y la reducción de la superficie de exposición de los organismos minimizando los tiempos de gestión a través de una eficiente detección de vulnerabilidades y notificación de alertas, así como, ofreciendo recomendaciones para un tratamiento oportuno de estas.

Con su enfoque Asset Centric, LightHouse VM permite, entre otros:

- Gestionar vulnerabilidades durante su ciclo de vida.
- Obtener el nivel de riesgo de una organización.
- Alertar y evaluar el riesgo de una organización de forma temprana.
- Agrupar en grupos lógicos de gestión a medida.
- Planificar los ciclos de revisión de vulnerabilidades.
- Medir el nivel de desempeño en la mitigación de las vulnerabilidades con sus cuadros de mandos de seguimiento y SLAs.
- Integrarse con sistemas de escaneo líderes del mercado y las principales herramientas de ticketing para la gestión directa de las vulnerabilidades.

Observaciones

No aplica Procedimiento de Empleo Seguro

9.2 ANÁLISIS Y GESTIÓN DE RIESGOS

Archer Suite	
Versión	6.11 (con IRM Mobile v1.4)
Fabricante	RSA
Familia	Análisis y Gestión de Riesgos
Tipo	Producto
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025
  Descripción Archer es una solución de Gestión Integral de Riesgos (o también conocida como GRC) que permite unificar las actividades de gobierno corporativo, riesgo y cumplimiento de normas en una sola plataforma integrada. Actúa como una protección perimetral para aplicar una cultura de administración de riesgo y responsabilidad compartida en toda la institución. Les permite instituir programas eficaces para fomentar las mejores prácticas y estandarizar los procesos directamente a través de su tecnología. Tiene plena visibilidad para responder preguntas de la junta directiva y generar claridad entorno al estado del cumplimiento de normas y de los riesgos para toda la institución. Contamos con modalidad servicio SaaS y también on-premises. Dentro de Archer, los dominios de riesgo principales que se cubren son: • Gestión de Riesgos de Seguridad e IT (incluyendo gestión para cumplimiento del ENS) • Continuidad de Negocio y Resiliencia Operacional • Gestión de Riesgos de Terceros • Cumplimiento (incluyendo GDPR) • Gestión de Riesgo Operacional • Auditoría Interna • ESG (Environmental, Social and Governance) • Cuantificación de Riesgos Para más información: https://www.archerirm.com/ Observaciones Procedimiento de Empleo Seguro pendiente de publicación	

9.3 NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES

LUCIA		
Versión	4.1	
Fabricante	Centro Criptológico Nacional	
Familia	Notificación y Gestión de Ciberincidentes	
Tipo	Producto	
Fecha Inclusión	01/10/2021	
Revisión de Validez	31/12/2024	
Descripción	LUCIA es una herramienta para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Con ella, se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora. LUCIA ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el seguimiento del mismo. El sistema permite, además, automatizar las tareas e integrarse con otros sistemas ya implantados.	
Observaciones	Para más información, contactar con lucia@ccn-cert.cni.es.	



9.4 FORMACIÓN Y CONCENCIACIÓN

Cyber Guru s.r.l

Versión	2.0
Fabricante	Cyber Guru
Familia	Formación y Concenciación
Tipo	Servicio
Fecha Inclusión	04/12/2024
Revisión de Validez	30/11/2026



Descripción

Cyber Guru es una plataforma SaaS de concienciación en ciberseguridad integral que logra un cambio de comportamiento y aprendizaje permanente gracias al uso de las metodologías de aprendizaje más sofisticadas, gamificación y un modelo único de Machine Learning para proporcionar a los usuarios una formación adaptativa, eficaz y atractiva. Ofrece contenidos en más de 15 idiomas orientados a transformar el factor humano de eslabón más débil de la cadena a primera línea de defensa contra la ciberdelincuencia.

Observaciones

N/A

ATTACK Simulator

Versión	1.0.0
Fabricante	Attack Simulator S.R.L.
Familia	Formación y Concenciación
Tipo	Servicio
Fecha Inclusión	21/10/2024
Revisión de Validez	30/09/2026



Descripción

Attack Simulator, combina un entrenamiento interactivo continuo con simulaciones de ciberataques aleatorias mediante un programa completo automatizado y desatendido, con la posibilidad de hacer simulaciones de phishing y smishing a discreción.

Observaciones

N/A

SMARTFENSE

Versión	3 y 4
Fabricante	Defense Balance
Familia	Formación y Concenciación
Tipo	Servicio
Fecha Inclusión	01/10/2022
Revisión de Validez	31/01/2025

**Descripción**

SMARTFENSE es la plataforma online de concienciación en Seguridad de la Información que permite generar comportamientos seguros en los usuarios, favoreciendo la creación de una cultura cibersegura. SMARTFENSE provee catálogos de contenidos predefinidos 100% editables para adecuarse a la cultura de la organización y además, posibilita la creación de contenido propio. Ofrece también herramientas de simulación de Phishing y Ransomware para medir la efectividad de las acciones realizadas y conocer la evolución en las respuestas de los usuarios.

Observaciones

No aplica la publicación de procedimiento de empleo seguro.

Ángeles

Versión	1.0
Fabricante	CSA / CCN
Familia	Formación y Concenciación
Tipo	Servicio
Fecha Inclusión	01/09/2023
Revisión de Validez	31/12/2024

**Descripción**

Ángeles, plataforma de formación, capacitación y talento en ciberseguridad, con una oferta formativa completa, incluyendo cursos online, webinars y diferente documentación en función del perfil del usuario. La plataforma, disponible en Google Play y App Store, dispone de un área privada, con acceso a través del sistema Cl@ve, desde el que acceder al expediente de cada alumno, con las horas de formación recibidas, así como los cursos y sesiones de concienciación realizadas en la plataforma.

Observaciones

N/A

Kymatio

Versión	Kymatio 4.6.1
Fabricante	Kymatio
Familia	Formación y Concenciación
Tipo	Servicio
Fecha Inclusión	01/02/2024
Revisión de Validez	31/01/2026

**Descripción**

Kymatio® automatiza la concienciación de los empleados y la evaluación de su estado de alerta de forma desatendida y personalizada, al tiempo que proporciona una herramienta de gestión de riesgo asociado al elemento humano, proporcionando métricas, evolución en el tiempo y planes de acción. Permite alcanzar la visibilidad necesaria sobre la exposición de la plantilla a incidentes de seguridad de la información y su mitigación incluyendo los siguientes servicios:

- Servicio automático de evaluación y concienciación personalizada, diseñado para aumentar el nivel de alerta de los empleados en aquellas áreas clave como son: puesto de trabajo, cumplimiento, protección de datos, comunicaciones, malware, gestión de contraseñas e ingeniería social.
- Account Breach Scanner (ABS), que conecta la vigilancia de credenciales expuestas con el programa de concienciación, analizando repositorios en línea para detectar filtraciones y notificando a la organización y empleados para su mitigación.
- Las Simulaciones de Ingeniería Social (Trickster) permiten evaluar la preparación de los empleados ante diferentes tipos de ataques, incluyendo phishing, spear phishing, smishing, y QRs entre otros, identificando ratios de respuesta y áreas de mejora.

La plataforma de gestión del ciberriesgo humano integra datos de los servicios descritos anteriormente, proporcionando insights valiosos para la mejora continua. Con métricas en tiempo real y evaluación 360º, Kymatio fortalece la cultura de ciberseguridad, reduciendo riesgos y asegurando la conformidad normativa para una gestión proactiva del ciberriesgo humano.

Observaciones

CCN-STIC 1703. Procedimiento de Empleo Seguro Kymatio

PSAT-Proofpoint Security Awareness Training

Versión**Fabricante** Proofpoint, Inc**Familia** Formación y Concenciación**Tipo** Producto**Fecha Inclusión** 01/03/2022**Revisión de Validez** 31/12/2024**proofpoint.****Descripción**

PSAT -Proofpoint Security Awareness Training- es una solución de formación y capacitación de concienciación en materia de seguridad.

La solución, basada en un enfoque cíclico de evaluación, educación, refuerzo y medición, enseña a los usuarios las mejores prácticas y les muestra cómo emplearlas cuando se enfrentan a amenazas de seguridad, ayudándoles a evitar que los ciberataques consigan su objetivo y convirtiéndolos en la última línea de defensa de las organizaciones.

Características Principales:

- Identifica el riesgo de los usuarios mediante Simulaciones de Phishing y evaluaciones de conocimiento.
- Permite cambiar el comportamiento de los usuarios, mediante más 350 módulos de formación interactivos que ofrecen ejercicios prácticos para que los usuarios reconozcan y eviten los ataques de phishing y otros fraudes de ingeniería social.
- Reduce la exposición de la organización, mediante un complemento para cliente de correo, los usuarios pueden denunciar los mensajes sospechosos con un solo clic
- Evalúa y analiza los resultados, la solución ofrece una visibilidad detallada y de alto nivel que permite medir el progreso, evaluar el desempeño e identificar el riesgo a nivel de organización, departamento y usuario.

Observaciones

CCN-STIC-1701 Procedimiento de Empleo Seguro PSAT

10. REFERENCIAS

[1]	CCN-STIC-106 Procedimiento de inclusión de productos de seguridad TIC cualificados en el CPSTIC.
[2]	CCN-STIC-140 Taxonomía de referencia para productos de Seguridad TIC.
[3]	CCN-STIC-102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada.
[4]	CCN-STIC-130 Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada.
[5]	CCN-STIC-151 Evaluación y Clasificación TEMPEST de equipos.

11. ABREVIATURAS

CC	<i>Common Criteria</i>
CCN	<i>Centro Criptológico Nacional</i>
CPSTIC	<i>Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación</i>
EDR	<i>Endpoint Detection and Response</i>
ENECSTI	<i>Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información</i>
ENS	<i>Esquema Nacional de Seguridad.</i>
EPP	<i>Endpoint Protection Platform</i>
IDS	<i>Intrusion Detection System</i>
IPS	<i>Intrusion Prevention System</i>
PES	<i>Procedimiento de Empleo Seguro</i>
RFS	<i>Requisitos Fundamentales de Seguridad</i>
STIC	<i>Seguridad de las Tecnologías de la Información y la Comunicación</i>
TIC	<i>Tecnologías de la Información y la Comunicación</i>

