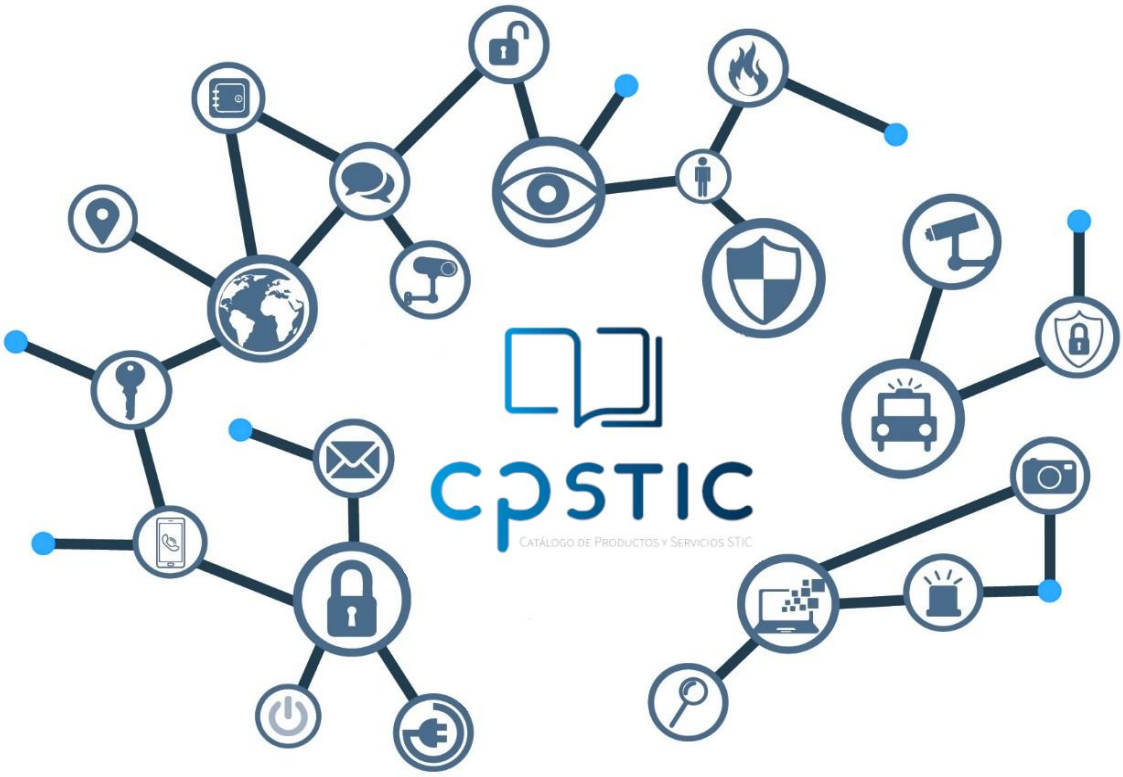
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 105

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



Octubre de 2026

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

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

Edita:

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2026
NIPO: 083-26-171-7

Fecha de Edición: Octubre de 2026

CCN
c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
2026.10.14 09:31:00 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

ÍNDICE

ÍNDICE **3**
1. INTRODUCCIÓN **7**
2. OBJETIVO **8**
3. ALCANCE **8**
4. INCLUSIÓN DE UN PRODUCTO DEL CPSTIC **9**
5. REVISIÓN DE VALIDEZ DE PRODUCTOS STIC **10**
6. EXCLUSIÓN DE UN PRODUCTO O SERVICIO DEL CPSTIC **11**
7. PRODUCTOS CUALIFICADOS **12**
7.1 HERRAMIENTAS PARA EL DESARROLLO DE PRODUCTOS DE SEGURIDAD 14
7.2 CONTROL DE ACCESOS 16
7.2.1 CONTROL DE ACCESO A RED (NAC) 16
7.2.2 SERVIDORES DE AUTENTICACIÓN 20
7.2.3 GESTIÓN DE ACCESO PRIVILEGIADO (PAM) 22
7.2.4 GESTIÓN DE IDENTIDADES (IM) 27
7.2.5 AUTENTICACIÓN MULTI-FACTOR (MFA) 36
7.2.6 HERRAMIENTAS DE VIDEOIDENTIFICACIÓN 37
7.3 PROTECCIÓN DE DISPOSITIVOS 46
7.3.1 ANTI-VIRUS / EPP (ENDPOINT PROTECTION PLATFORM) 46
7.3.2 EDR (ENDPOINT DETECTION AND RESPONSE) 57
7.3.3 HERRAMIENTAS DE GESTIÓN DE DISPOSITIVOS (UEM) 69
7.3.4 HERRAMIENTAS DE SANDBOX 71
7.4 PROTECCIÓN DE REDES Y SISTEMAS 72
7.4.1 SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM) 72
7.4.2 SISTEMAS DE ORQUESTACIÓN, AUTOMATIZACIÓN Y RESPUESTA DE SEGURIDAD (SOAR) 84
7.4.3 HERRAMIENTAS DE GESTIÓN DE RED 85
7.4.4 DETECCIÓN Y RESPUESTA DE AMENAZAS EN RED (NDR) 88
7.4.5 CASB 93
7.5 PROTECCIÓN DE PERÍMETRO 94
7.5.1 ENRUTADORES 94
7.5.2 SWITCHES 126
7.5.3 CORTAFUEGOS 169
7.5.4 PROXIES 206
7.5.5 DISPOSITIVOS DE RED INALÁMBRICOS 208
7.5.6 PASARELAS SEGURAS DE INTERCAMBIO DE DATOS 219
7.5.7 DIODOS DE DATOS 223
7.5.8 WEB APPLICATION FIREWALL (WAF) 224
7.5.9 REDES DEFINIDAS POR SOFTWARE (SDN) 225
7.5.10 DISPOSITIVOS DE PREVENCIÓN Y DETECCIÓN DE INTRUSIONES (IDS E IPS) 228
7.5.11 PROTECCIÓN DE CORREO ELECTRÓNICO 246

7.5.12 BALANCEADORES DE CARGA 250
7.6 PROTECCIÓN DE LAS COMUNICACIONES 253
7.6.1 HERRAMIENTAS VOZ IP 253
7.6.2 HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA (IM) 256
7.6.3 HERRAMIENTAS DE VIDEOCONFERENCIA 258
7.6.4 REDES PRIVADAS VIRTUALES: IPSEC 260
7.6.5 REDES PRIVADAS VIRTUALES: TLS 276
7.6.6 REDES PRIVADAS VIRTUALES: OTRAS 278
7.7 PROTECCIÓN DE LA INFORMACIÓN 279
7.7.1 ALMACENAMIENTO CIFRADO DE DATOS 279
7.7.2 CIFRADO Y COMPARTICIÓN SEGURA DE INFORMACIÓN 281
7.7.3 HERRAMIENTAS DE BORRADO SEGURO 283
7.7.4 SISTEMAS PARA PREVENCIÓN DE FUGAS DE DATOS 285
7.7.5 GESTIÓN DE METADATOS 286
7.8 PROTECCIÓN DE INSTALACIONES E INFRAESTRUCTURAS 296
7.8.1 CÁMARAS IP 296
7.8.2 CONTROL DE ACCESO FÍSICO 297
7.9 ESPACIO 298
7.9.1 PRODUCTOS CRIPTOGRÁFICOS PARA ACCESO A SERVICIOS GNSS 298
7.10 SOPORTE CRIPTOGRÁFICO 299
7.10.1 HERRAMIENTAS PARA FIRMA ELECTRÓNICA 299
7.10.2 MÓDULO DE SEGURIDAD HARDWARE (HSM) 303
7.10.3 INFRAESTRUCTURA PKI 311
7.10.4 DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS 312
7.11 PROTECCIÓN DE PLATAFORMAS 314
7.11.1 DISPOSITIVOS MÓVILES 314
7.11.2 SISTEMAS OPERATIVOS 324
7.11.3 HIPERCONVERGENCIA 326
7.11.4 INFRAESTRUCTURA DE ESCRITORIO VIRTUAL (VDI) 328
7.11.5 CONMUTADORES KVM 330
7.12 SEGURIDAD OT 335
7.12.1 SEGURIDAD OT 335
7.13 COMUNICACIONES TÁCTICAS SEGURAS 336
7.13.1 SOLUCIONES PARA PROTECCIÓN DE LAS COMUNICACIONES TÁCTICAS 336
7.14 OTRAS HERRAMIENTAS 338
7.14.1 OTRAS HERRAMIENTAS 338
8. PRODUCTOS APROBADOS 370
8.1 HERRAMIENTAS PARA EL DESARROLLO DE PRODUCTOS DE SEGURIDAD 371
8.2 CONTROL DE ACCESOS 372
8.2.1 CONTROL DE ACCESO A RED (NAC) 372
8.2.2 SERVIDORES DE AUTENTICACIÓN 373

8.2.3 GESTIÓN DE ACCESO PRIVILEGIADO (PAM) 375
8.2.4 GESTIÓN DE IDENTIDADES (IM) 378
8.3 PROTECCIÓN DE DISPOSITIVOS 381
8.3.1 ANTI-VIRUS / EPP (ENDPOINT PROTECTION PLATFORM) 381
8.3.2 EDR (ENDPOINT DETECTION AND RESPONSE) 383
8.4 PROTECCIÓN DE REDES Y SISTEMAS 385
8.4.1 SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM) 385
8.4.2 HERRAMIENTAS DE GESTIÓN DE RED 391
8.4.3 DETECCIÓN Y RESPUESTA DE AMENAZAS EN RED (NDR) 393
8.5 PROTECCIÓN DE PERÍMETRO 394
8.5.1 ENRUTADORES 394
8.5.2 SWITCHES 407
8.5.3 CORTAFUEGOS 429
8.5.4 DISPOSITIVOS DE RED INALÁMBRICOS 449
8.5.5 PASARELAS SEGURAS DE INTERCAMBIO DE DATOS 451
8.5.6 DIODOS DE DATOS 455
8.5.7 PROTECCIÓN DE CORREO ELECTRÓNICO 456
8.5.8 BALANCEADORES DE CARGA 457
8.6 PROTECCIÓN DE LAS COMUNICACIONES 459
8.6.1 HERRAMIENTAS VOZ IP 459
8.6.2 HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA (IM) 461
8.6.3 HERRAMIENTAS DE VIDEOCONFERENCIA 463
8.6.4 REDES PRIVADAS VIRTUALES: OTRAS 464
8.7 PROTECCIÓN DE LA INFORMACIÓN 468
8.7.1 ALMACENAMIENTO CIFRADO DE DATOS 468
8.7.2 CIFRADO Y COMPARTICIÓN SEGURA DE INFORMACIÓN 469
8.7.3 HERRAMIENTAS DE BORRADO SEGURO 471
8.7.4 GESTIÓN DE METADATOS 472
8.8 ESPACIO 480
8.8.1 PRODUCTOS CRIPTOGRÁFICOS PARA ACCESO A SERVICIOS GNSS 480
8.9 SOPORTE CRIPTOGRÁFICO 481
8.9.1 INFRAESTRUCTURA PKI 481
8.9.2 DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS 482
8.10 PROTECCIÓN DE PLATAFORMAS 484
8.10.1 DISPOSITIVOS MÓVILES 484
8.10.2 SISTEMAS OPERATIVOS 485
8.10.3 HIPERCONVERGENCIA 486
8.11 COMUNICACIONES TÁCTICAS SEGURAS 488
8.11.1 SOLUCIONES PARA PROTECCIÓN DE LAS COMUNICACIONES TÁCTICAS 488
8.11.2 PLATAFORMAS Y DISPOSITIVOS TÁCTICOS CONFIABLES 491

8.12 TEMPEST 494
8.12.1 ARMARIOS APANTALLADOS 494
8.12.2 MONITORES 498
8.12.3 PERIFÉRICOS 499
8.12.4 CPU 504
8.12.5 IMPRESORAS 506
8.12.6 SERVIDOR 507
8.12.7 PORTÁTIL 508
8.13 OTRAS HERRAMIENTAS 510
8.13.1 OTRAS HERRAMIENTAS 510
9. PRODUCTOS Y SERVICIOS DE CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD 512
9.1 GOBERNANZA Y PLANIFICACIÓN DE LA SEGURIDAD 513
9.2 NORMATIVA DE SEGURIDAD Y CONFORMIDAD 515
9.3 ANÁLISIS Y GESTIÓN DE RIESGOS 517
9.4 NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES 525
9.5 INTERCAMBIO DE CIBERINTELIGENCIA 526
9.6 FORMACIÓN Y CONCIENCIACIÓN 527
10. REFERENCIAS 535
11. ABREVIATURAS 536

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, BÁSICA[1]).

    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.

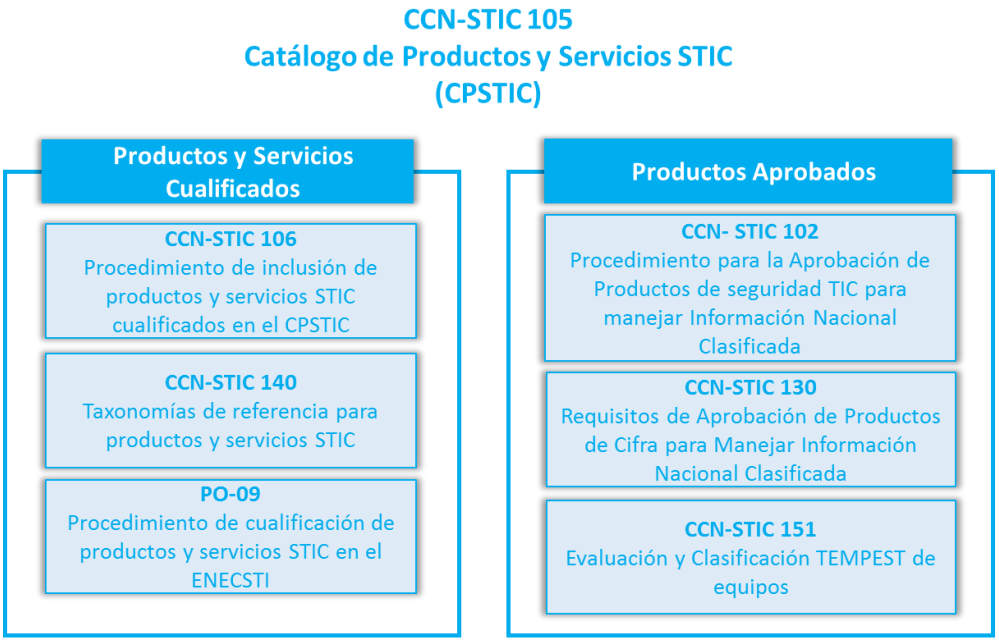


Figura 1. Inclusión de productos y servicios de seguridad en el CPSTIC

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 Y SERVICIOS STIC

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	1.3
Fabricante	Cryptographic and Security System (CS2)
Familia	-
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/12/2026

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	3.7.1-ccn
Fabricante	Centro Criptológico Nacional
Familia	-
Tipo	Producto
Categoría ENS	N/A
Fecha Inclusión	18/02/2025
Revisión de Validez	31/12/2027

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	31/10/2026

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 ACCESOS

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	31/12/2027

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, Forninet y mas) todo ello mediante la integración múltiples fuentes de autenticación (Directorios activos, LDAP, BBDD y provedores externos de identidad)

Observaciones

CCN-STIC 1103 Procedimiento de Empleo Seguro Aruba ClearPass 6.11

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	31/10/2026

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

CCN-STIC 1104 Procedimiento de Empleo Seguro pendiente de Actualización

INFORMACIÓN IMPORTANTE

iMC MagicBox	
Versión	7.3
Fabricante	New H3C Technologies
Familia	Control de acceso a red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/08/2025
Revisión de Validez	31/01/2028

Descripción

H3C iMC (Centro de Gestión Inteligente) es una plataforma flexible y escalable diseñada para las necesidades integrales de gestión de red de empresas globales. iMC y sus componentes, como EIA, ofrecen seguridad integrada, monitorización, control de acceso, análisis basado en IA, interfaces de enlace Norte – Sur. Su arquitectura se basa en jerarquías de acceso y control habituales en a gran escala. Soporta gestión de dispositivos de terceros que proteger las inversiones existentes. Estas capacidades ayudan a los clientes a reducir significativamente los gastos operativos basados en gestión y mantenimiento.

Observaciones

CCN-STIC 1119 Procedimiento de Empleo Seguro iMC MagicBox

INFORMACIÓN IMPORTANTE

iMaster NCE Campus

Versión	V300R023C00SPC010T
Fabricante	Huawei Technologies
Familia	Control de acceso a red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/10/2024
Revisión de Validez	31/03/2027

Descripción

iMaster NCE-Campus, es un sistema de gestión y control de redes autónomas de última generación de Huawei para redes de campus, integra funciones de gestión, control, análisis e inteligencia artificial (IA), lo que proporciona una automatización completa del ciclo de vida de las redes de campus. En cuanto a la capacidad NAC, introduce el nuevo protocolo de autenticación HTTP2.0 y puede autenticar un gran número de dispositivos de red y usuarios utilizando varios modos de autenticación de acceso. Esto incluye la autenticación 802.1X, la autenticación por portal, la autenticación por SMS y la autenticación por redes sociales. También proporciona múltiples políticas de control de acceso de usuarios, lo que mejora significativamente la seguridad de la red. Al mismo tiempo, ofrece la posibilidad de que los usuarios se desacoplen de las direcciones IP, lo que les permite acceder a la red en cualquier momento y lugar, con permisos consistentes. Esto garantiza la libre movilidad y una experiencia de usuario consistente, al tiempo que se cumplen los requisitos de control de permisos.

Observaciones

CCN-STIC 1474 PES Huawei iMaster NCE Campus

OpenNAC Enterprise by Cipherbit

Versión	1.2.5-1
Fabricante	Cipherbit – Grupo Oesia
Familia	Control de acceso a red (NAC)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/09/2021
Revisión de Validez	30/11/2026

Descripción

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

7.2.2 SERVIDORES DE AUTENTICACIÓN

Location-Based Identity Platform	
Versión	
Fabricante	Ironchip Telco
Familia	Servidores de Autenticación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/11/2026

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

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	31/12/2027

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, Forninet y mas) todo ello mediante la integración múltiples fuentes de autenticación (Directorios activos, LDAP, BBDD y provedores externos de identidad)

Observaciones

CCN-STIC 1103 Procedimiento de Empleo Seguro Aruba ClearPass 6.11

Microsoft Entra ID

Versión	
Fabricante	Microsoft
Familia	Servidores de Autenticación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	03/03/2025
Revisión de Validez	28/02/2027

Descripción

Microsoft Entra ID (antes conocido como Azure Active Directory) es un servicio cloud para la gestión de identidades y accesos en entornos digitales, actuando como un orquestador que integra múltiples funcionalidades incluyendo autenticación multifactor, inicio de sesión único (SSO), gestión para el acceso seguro a aplicaciones y servicios, soporte para la definición de políticas de acceso condicional basadas en factores de riesgo que se ajustan dinámicamente las medidas de seguridad según el contexto del usuario. Además, permite la integración híbrida que permite sincronizar identidades entre entornos locales y nube, así como la federación de identidades que facilita la colaboración con usuarios externos sin comprometer la protección. Microsoft EntraID abarca el ciclo completo de la identidad, gestionando de forma precisa la creación, actualización y eliminación de usuarios y grupos, e incorpora herramientas de gobernanza y auditoría para el cumplimiento normativo. También ofrece opciones de autenticación sin contraseña mediante tecnologías biométricas o llaves de seguridad, integra funciones de autoservicio como el restablecimiento de contraseñas, y proporciona APIs para conectar aplicaciones y servicios de forma personalizada. Incluye una suite de análisis y vigilancia que permite detectar comportamientos anómalos en tiempo real en la administración de accesos digitales.

Observaciones

CCN-STIC-1116 Procedimiento de Empleo Seguro Microsoft Entra ID

INFORMACIÓN IMPORTANTE

7.2.3 GESTIÓN DE ACCESO PRIVILEGIADO (PAM)

Safeguard for Privilege 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	31/10/2026

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

CyberArk Privileged Access Manager Self-Hosted

Versión	14.0
Fabricante	CYBERARK
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/03/2025
Revisión de Validez	31/10/2026

Descripción

CyberArk Privileged Access Manager es una solución de seguridad de la identidad que permite proteger, controlar y monitorizar el acceso privilegiado a infraestructuras locales, en la nube e híbridas. Permite a las organizaciones:
Administrar y proteger las credenciales de las cuentas privilegiadas y sus derechos de acceso.
• Asegurar y controlar, de forma centralizada, el acceso a las credenciales privilegiadas basadas en políticas de seguridad definidas administrativamente.
• Aislar y asegurar las sesiones de los usuarios privilegiados.
• Monitorizar y controlar la actividad de las cuentas privilegiadas, identificando actividades sospechosas y permitiendo responder a las amenazas.
• Ver sesiones privilegiadas en tiempo real, suspender automáticamente y terminar remotamente las sesiones sospechosas.
• Detectar, alertar y responder a actividades privilegiadas anómalas.
• Que los usuarios privilegiados ejecuten comandos administrativos autorizados desde sus sesiones nativas de Unix o Linux, eliminando los privilegios raíz innecesarios.
• Controlar el acceso de privilegios mínimos para multitud de objetivos, con una variedad de más de 350 conectores comprobados accesibles desde su Market Place sin cargo adicional.

Observaciones

CCN-STIC 1108 PES CyberArk Privileged Account Security Solution PAS (En proceso de actualización)

INFORMACIÓN IMPORTANTE

CyberArk Privilege Cloud

Versión	14.X
Fabricante	CYBERARK
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	19/03/2025
Revisión de Validez	28/02/2027

Descripción

CyberArk Privileged Access Manager es una solución de seguridad de la identidad que permite proteger, controlar y monitorizar el acceso privilegiado a infraestructuras locales, en la nube e híbridas. Permite a las organizaciones:
Administrar y proteger las credenciales de las cuentas privilegiadas y sus derechos de acceso.
• Asegurar y controlar, de forma centralizada, el acceso a las credenciales privilegiadas basadas en políticas de seguridad definidas administrativamente.
• Aislar y asegurar las sesiones de los usuarios privilegiados.
• Monitorizar y controlar la actividad de las cuentas privilegiadas, identificando actividades sospechosas y permitiendo responder a las amenazas.
• Ver sesiones privilegiadas en tiempo real, suspender automáticamente y terminar remotamente las sesiones sospechosas.
• Detectar, alertar y responder a actividades privilegiadas anómalas.
• Que los usuarios privilegiados ejecuten comandos administrativos autorizados desde sus sesiones nativas de Unix o Linux, eliminando los privilegios raíz innecesarios.
• Controlar el acceso de privilegios mínimos para multitud de objetivos, con una variedad de más de 350 conectores comprobados accesibles desde su Market Place sin cargo adicional.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

SOFFID IAM

Versión	3.5
Fabricante	SOFFID IAM
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/03/2025
Revisión de Validez	31/08/2027

Descripción

Soffid es la solución IAM que integra la gestión de acceso (AM), el gobierno de identidad (IGA), el riesgo y cumplimiento de identidad (IRC) y la gestión de cuentas privilegiadas (PAM) en una única plataforma integral. Su enfoque modular escalable y flexible, permite incorporar las anteriores soluciones en función de las necesidades particulares.

Con Soffid, las organizaciones gestionan las identidades de manera ágil y sin complicaciones porque la plataforma proporciona una visión centralizada y un control completo sobre identidades, accesos y cuentas privilegiadas.

- Gestión centralizada sin complejidad: Unifica el control de accesos, eliminando integraciones innecesarias y reduciendo el tiempo de implementación.
- Automatización eficiente: Para empleados y otros usuarios, permitiendo que accedan a las aplicaciones y a los datos estrictamente necesarios para desempeñar su trabajo, uso o colaboración.
- Protección de cuentas privilegiadas con controles avanzados, gestión de sesiones y monitorización de accesos críticos.
- Gobierno inteligente: Certificación de accesos, auditoría continua y cumplimiento normativo adaptado a cada organización.
- Facilidad operativa: Optimiza la gestión de identidades con procesos automatizados y ágiles, reduciendo la carga operativa de IT.

Observaciones

CCN-STIC 1118. Procedimiento de Empleo Seguro Soffid IAM

INFORMACIÓN IMPORTANTE

ENDURANCE

Versión	1.1.2
Fabricante	COSMIKAL
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	04/03/2025
Revisión de Validez	31/08/2027

Descripción

Endurance es un Espacio de Trabajo Remoto Blindado (RSW: Remote Shielded Workspace) que simplifica y aumenta la protección, control, uso y administración de los activos digitales de las organizaciones.
Gracias a la sencillez de su instalación, uso y mantenimiento, facilita la protección de activos tanto para gran corporación como para pyme. Endurance es un puente seguro entre los endpoints de los usuarios y los activos mediante un entorno de trabajo blindado que limita y customiza las funcionalidades de todas las aplicaciones. Cada usuario dispone de su propio escritorio remoto con los accesos autorizados accediendo mediante un bróker de conexión en aplicación nativa o mediante un navegador web desde cualquier tipo de dispositivo. Esta arquitectura, potenciada mediante funcionalidades de PAM (vault, permisos, roles, políticas, etc), deriva en tres ventajas fundamentales:

1. Simplifica la arquitectura de red de acceso a los activos.
2. Reduce los riesgos asociados a los endpoints.
3. Además de los accesos a activos IT/OT, protege archivos y transferencias.

Endurance es una combinación de tecnologías en una sola herramienta donde convergen seguridad, usabilidad y productividad.

Observaciones

CCN-STIC 1117. Procedimiento de Empleo Seguro Cosmikal Endurance

INFORMACIÓN IMPORTANTE

7.2.4 GESTIÓN DE IDENTIDADES (IM)

Falcon Identity Protection	
Versión	Falcon Console (N/A) y Falcon Sensor (v7.27)
Fabricante	CrowdStrike
Familia	Gestión de identidades (IM)
Tipo	Servicio
Categoría ENS	MEDIA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/10/2026
Descripción	

CrowdStrike Identity Threat Protection es una solución de seguridad de las identidades que combina una visibilidad completa del riesgo de las identidades para entornos on-premise o nube, detección avanzada de amenazas, análisis de comportamiento basado en ML e IA para identificar anomalías y patrones sospechosos, respuesta automatizada para remediación inmediata de incidentes y, lo más importante, protección ante amenazas relacionadas con la identidad mediante la prevención en tiempo real de ataques de robo de credenciales, escalado de privilegios, movimiento lateral o accesos no autorizados. Además, se integra nativamente con el ecosistema CrowdStrike Falcon® para correlacionar datos de endpoints, nube e identidades, proporcionando una visión unificada de la postura de seguridad de la organización y eliminando los puntos ciegos en los ataques multi-dominio.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Identity and Access Management (IAM)	
Versión	
Fabricante	Google
Familia	Gestión de identidades (IM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	16/07/2025
Revisión de Validez	31/10/2026
Descripción	

IAM proporciona a los administradores la capacidad de gestionar los recursos de la nube de forma centralizada controlando quién puede realizar qué acción en recursos específicos.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

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	31/12/2026

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

CCN-STIC 887A Guía de configuración segura AWS

WSO2 Identity Server

Versión	v7.0.0
Fabricante	WSO2 LLC
Familia	Gestión de identidades (IM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2026
Revisión de Validez	31/08/2028

Descripción

WSO2 Identity Server es una potente y moderna solución de gestión de identidades y accesos. Permite a las organizaciones ofrecer experiencias digitales excepcionales y fiables a todo tipo de usuarios. WSO2 Identity Server puede gestionar las solicitudes de autenticación de los proveedores de servicios integrados y redirigirlas a los servicios de autenticación adecuados, ya sea de forma remota o local. WSO2 Identity Server garantiza una fácil integración con diversas aplicaciones para facilitar el inicio de sesión único (SSO), el inicio de sesión social, la federación de identidades, la seguridad de las API, la autenticación fuerte, la gestión de cuentas y el cumplimiento de la normativa de privacidad.

Observaciones

CCN-STIC-1001 Procedimiento de empleo seguro WSO2 Identity Server

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	31/10/2026

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 desaprovisionamiento 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

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	31/10/2026

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

SailPoint IdentityIQ

Versión V8.3p5

Fabricante Sailpoint

Familia Gestión de identidades (IM)

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/06/2026

Revisión de Validez 30/11/2028

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 Procedimiento de Empleo Seguro SailPoint IdentityIQ

Azure Identity Access Management (IAM)

Versión

Fabricante Microsoft

Familia Gestión de identidades (IM)

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 03/01/2025

Revisión de Validez 31/12/2026

Descripción

Azure Access Control (IAM) es un conjunto integral de herramientas y servicios en la nube de Microsoft diseñados para gestionar de manera segura las identidades digitales y los accesos a recursos y aplicaciones. Este servicio permite a las organizaciones controlar quién puede acceder a qué recursos, garantizando que solo las personas autorizadas tengan los permisos adecuados. Azure Access Control (IAM) facilita la implementación de políticas de seguridad basadas en roles, la autenticación multi factor y el monitoreo continuo de actividades sospechosas, contribuyendo a proteger la información sensible y a cumplir con normativas de seguridad.

Observaciones

CCN-STIC 1115. Procedimiento de Empleo Seguro Microsoft IAM

INFORMACIÓN IMPORTANTE

Amazon Cognito

Versión

Fabricante AWS

Familia Gestión de identidades (IM)

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 17/09/2024

Revisión de Validez 31/10/2026

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

CCN-STIC-887A Guía de configuración segura AWS

INFORMACIÓN IMPORTANTE

SOFFID IAM

Versión	3.5
Fabricante	SOFFID IAM
Familia	Gestión de identidades (IM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/03/2025
Revisión de Validez	31/08/2027

Descripción

Soffid es la solución IAM que integra la gestión de acceso (AM), el gobierno de identidad (IGA), el riesgo y cumplimiento de identidad (IRC) y la gestión de cuentas privilegiadas (PAM) en una única plataforma integral. Su enfoque modular escalable y flexible, permite incorporar las anteriores soluciones en función de las necesidades particulares.

Con Soffid, las organizaciones gestionan las identidades de manera ágil y sin complicaciones porque la plataforma proporciona una visión centralizada y un control completo sobre identidades, accesos y cuentas privilegiadas.

- Gestión centralizada sin complejidad: Unifica el control de accesos, eliminando integraciones innecesarias y reduciendo el tiempo de implementación.
- Automatización eficiente: Para empleados y otros usuarios, permitiendo que accedan a las aplicaciones y a los datos estrictamente necesarios para desempeñar su trabajo, uso o colaboración.
- Protección de cuentas privilegiadas con controles avanzados, gestión de sesiones y monitorización de accesos críticos.
- Gobierno inteligente: Certificación de accesos, auditoría continua y cumplimiento normativo adaptado a cada organización.
- Facilidad operativa: Optimiza la gestión de identidades con procesos automatizados y ágiles, reduciendo la carga operativa de IT.

Observaciones

CCN-STIC 1118. Procedimiento de Empleo Seguro Soffid IAM

INFORMACIÓN IMPORTANTE

Microsoft Entra ID

Versión

Fabricante Microsoft

Familia Gestión de identidades (IM)

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 03/03/2025

Revisión de Validez 28/02/2027

Descripción

Microsoft Entra ID (antes conocido como Azure Active Directory) es un servicio cloud para la gestión de identidades y accesos en entornos digitales, actuando como un orquestador que integra múltiples funcionalidades incluyendo autenticación multifactor, inicio de sesión único (SSO), gestión para el acceso seguro a aplicaciones y servicios, soporte para la definición de políticas de acceso condicional basadas en factores de riesgo que se ajustan dinámicamente las medidas de seguridad según el contexto del usuario. Además, permite la integración híbrida que permite sincronizar identidades entre entornos locales y nube, así como la federación de identidades que facilita la colaboración con usuarios externos sin comprometer la protección. Microsoft EntraID abarca el ciclo completo de la identidad, gestionando de forma precisa la creación, actualización y eliminación de usuarios y grupos, e incorpora herramientas de gobernanza y auditoría para el cumplimiento normativo. También ofrece opciones de autenticación sin contraseña mediante tecnologías biométricas o llaves de seguridad, integra funciones de autoservicio como el restablecimiento de contraseñas, y proporciona APIs para conectar aplicaciones y servicios de forma personalizada. Incluye una suite de análisis y vigilancia que permite detectar comportamientos anómalos en tiempo real en la administración de accesos digitales.

Observaciones

CCN-STIC-1116 Procedimiento de Empleo Seguro Microsoft Entra ID

INFORMACIÓN IMPORTANTE

Module and Entity Management

Versión	4.0
Fabricante	NOLOGIN CONSULTING SLU
Familia	Gestión de identidades (IM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	30/06/2026
Revisión de Validez	30/11/2026

Descripción

MEM es la solución de gestión de identidades y accesos desarrollada por Nologin. En el escenario evaluado de proveedor de identidad, MEM actúa como punto central de autenticación de los usuarios de la organización frente a las aplicaciones y servicios integrados, proporcionando inicio de sesión único (SSO). El producto permite definir políticas de autenticación por usuario y por organización, con soporte de autenticación mediante contraseña, autenticación multifactor (MFA) y mecanismos sin contraseña basados en WebAuthn.

MEM gestiona el ciclo de vida completo de las identidades con una visión integrada de las aplicaciones y servicios de la organización, controlando en todo momento quién puede acceder a qué: automatiza el alta, modificación y baja de usuarios y la provisión y desprovisión de las aplicaciones, servicios y permisos asignados a cada identidad. Mediante organizaciones jerárquicas refleja la estructura de la entidad y aplica sobre ellas políticas de seguridad, incluyendo expiración de contraseñas y caducidad de identidades. Incorpora registro, trazabilidad y auditoría de las operaciones realizadas en la plataforma, y protege las comunicaciones con las aplicaciones integradas mediante canales seguros TLS. El producto puede desplegarse on-premise o en la nube, en un único nodo o en clúster.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.2.5 AUTENTICACIÓN MULTI-FACTOR (MFA)

AuthPoint	
Versión	
Fabricante	WatchGuard Technologies
Familia	Autenticación Multi-Factor (MFA)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/10/2026
Revisión de Validez	31/03/2027

Descripción

AuthPoint ofrece protección de identidad empresarial para organizaciones de cualquier tamaño mediante autenticación multifactor (MFA), políticas de confianza cero, SSO y autenticación sin contraseña resistente al phishing. Protege el acceso a VPN, aplicaciones cloud, equipos, servidores y escritorio remoto desde una única consola cloud. Los usuarios acceden a sus recursos desde un único portal web seguro, y los administradores, internos o MSP, configuran qué métodos y políticas aplican a cada recurso, grupo y caso de uso. Reduce la complejidad y carga operativa de aplicar autenticación sólida, con visibilidad y control para reducir riesgos y frenar las amenazas de identidad.

Observaciones

N/A

INFORMACIÓN IMPORTANTE

7.2.6 HERRAMIENTAS DE VIDEOIDENTIFICACIÓN

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	31/12/2026
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

VerificaID	
Versión	2.1
Fabricante	Bewor Tech
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	29/05/2025
Revisión de Validez	30/04/2027
Descripción	

Solución de verificación de identidad digital mediante video identificación, que combina tecnología biométrica y algoritmo propio de validación documental para un proceso seguro y ágil. El procedimiento incluye la validación automatizada del documento de identidad (análisis de ambas caras y elementos de seguridad, como hologramas), la comparación biométrica entre la imagen del documento y el rostro del usuario, y la ejecución de una prueba de vida pasiva. Adicionalmente, la solución incorpora una plataforma de supervisión para la revisión manual por parte de personal autorizado, reforzando la fiabilidad y permitiendo la auditoría de cada proceso.

Observaciones

CCN-STIC 1657. Procedimiento de Empleo Seguro Bewor VerificaID

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	31/05/2027

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

Signicat VideoID High

Versión	v.2024
Fabricante	SIGNICAT
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/01/2026
Revisión de Validez	31/12/2027

Descripción

Signicat VideoID High es una solución de videoidentificación y verificación de identidad diseñada con altos estándares de seguridad para garantizar una identificación remota fiable y resistente a intentos de fraude. Su módulo biométrico emplea inteligencia artificial (IA) y algoritmos de aprendizaje automático (ML) avanzados para detectar y mitigar ataques de suplantación de identidad. Entre sus capacidades, incluye detección de ataques de presentación (PAD), protegiendo contra intentos de fraude mediante imágenes en pantalla, máscaras de distintos materiales y niveles de sofisticación. Además, incorpora mecanismos de detección de ataques de inyección (IAD) que previenen la manipulación mediante vídeos pregrabados o técnicas de deepfake.

La solución combina transmisión de vídeo en tiempo real con IA para autenticar la identidad del solicitante mediante la extracción y comparación de rasgos biométricos con los datos del documento de identidad. El proceso refuerza la seguridad mediante la validación de elementos visuales del documento (hologramas), la ejecución de una prueba de vida y la posibilidad de integrar una OTP como capa adicional de protección.

Además, Signicat VideoID High permite la verificación manual por parte de agentes especializados, quienes analizan las evidencias recogidas y evalúan indicadores adicionales de seguridad. El proceso de identificación es desasistido y asíncrono, garantizando un equilibrio óptimo entre usabilidad, precisión y resistencia a intentos de fraude sofisticados.

La versión v.2024-GCP de Signicat VideoID High se distingue por estar desplegada en la infraestructura de nube pública de Google Cloud Platform (GCP). Esta configuración permite aprovechar las capacidades de escalabilidad, disponibilidad y seguridad propias del entorno GCP, manteniendo los mismos estándares funcionales y de protección frente al fraude que la versión v.2024.

Observaciones

CCN-STIC-1004 Procedimiento de empleo seguro Signicat VideoID High

INFORMACIÓN IMPORTANTE

TrustCloud VideoID

Versión	4.0
Fabricante	TrustCloud Tech
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	18/12/2024
Revisión de Validez	30/11/2026

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 (video selfie) o asistidas. La tecnología ofrece múltiples capas de autenticación, garantizando seguridad, fluidez y una experiencia de usuario óptima, tanto para el alta de empresa como el de usuario final, poniendo especial atención a aquellos usuarios menos habituados a los procesos digitales.

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

CCN-STIC 1649. Procedimiento de Empleo Seguro TrustCloud VideoID

LOQR Platform

Versión	Backoffice 3.1, SDK 3.0
Fabricante	LOQR
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/05/2024
Revisión de Validez	31/10/2026

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 ypara 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

Veridas Identity verification Platform

Versión	2024-01
Fabricante	Veridas Digital Authentication Solutions
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	30/08/2024
Revisión de Validez	31/10/2026

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

INFORMACIÓN IMPORTANTE

MobbScan

Versión	2.35
Fabricante	Mobbeel
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/03/2026
Revisión de Validez	31/07/2027

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

CCN-STIC 1646 Procedimiento de Empleo Seguro MobbScan

IQP VideoID and SelfID_BO

Versión	14.0
Fabricante	InfoCert
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	22/01/2026
Revisión de Validez	31/10/2026

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) y 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.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Inetum Digital Onboarding

Versión	1.1
Fabricante	INETUM
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/09/2023
Revisión de Validez	30/11/2026

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

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	30/11/2026

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

Signaturit VideoID by IVNOSYS	
Versión	1.15
Fabricante	Ivnosys Soluciones
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	03/11/2025
Revisión de Validez	31/10/2027

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

Mi eID eSIGN

Versión	1.3
Fabricante	ANF Certification Authority
Familia	Herramientas de videoidentificación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2026
Revisión de Validez	30/09/2028

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

CCN-STIC 1641 Procedimiento de Empleo Seguro Mi eID eSIGN

INFORMACIÓN IMPORTANTE

7.3 PROTECCIÓN DE DISPOSITIVOS

7.3.1 ANTI-VIRUS / EPP (ENDPOINT PROTECTION PLATFORM)

SentinelOne Singularity Complete	
Versión	Agent 24.2.3.471
Fabricante	SentinelOne
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	22/07/2025
Revisión de Validez	30/06/2027

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 PES SentinelOne Singularity Complete

INFORMACIÓN IMPORTANTE

Microsoft Defender for Endpoint

Versión	
Fabricante	Microsoft
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	16/06/2025
Revisión de Validez	31/05/2027

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.

Falcon Sensor con Falcon Console Cloud

Versión	7.21.19205
Fabricante	CrowdStrike
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/06/2025
Revisión de Validez	30/11/2027

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 Procedimiento de Empleo Seguro Falcon Sensor

INFORMACIÓN IMPORTANTE

Watchguard Endpoint Security Prime

Versión	EPDR 4.70 Manag. Agent. 1.25, Protect. Agent 8.00
Fabricante	WatchGuard Technologies
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	30/06/2026
Revisión de Validez	31/05/2027

Descripción

Endpoint Security Prime ofrece protección de nivel empresarial gracias a sus completas capacidades de EDR, visibilidad a nivel de incidente, contexto de los ataques y análisis de las causas fundamentales. Al consolidar las señales relacionadas en una vista unificada de los incidentes, las organizaciones pueden comprender rápidamente los eventos de seguridad, identificar los activos afectados y priorizar las medidas de respuesta. Diseñado para equipos que no cuentan con analistas de seguridad especializados, reduce el ruido de las alertas y la sobrecarga operativa, al tiempo que proporciona la visibilidad y el contexto necesarios para mejorar la postura de seguridad, reducir la exposición al riesgo y responder a las amenazas actuales.

Observaciones

CCN-STIC-1213 Procedimiento de Empleo Seguro en Proceso de Actualización

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

INFORMACIÓN IMPORTANTE

ESET Endpoint Security

Versión	11.0.2044.0
Fabricante	ESET
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	08/10/2024
Revisión de Validez	31/03/2027

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

CCN-STIC 1204 Procedimiento de Empleo Seguro ESET Endpoint Security

INFORMACIÓN IMPORTANTE

GravityZone	
Versión	
Fabricante	Bitdefender
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/06/2024
Revisión de Validez	30/11/2026

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

CCN-STIC-1230 Procedimiento de Empleo Seguro Bitdefender GravityZone

INFORMACIÓN IMPORTANTE

Symantec EndPoint Security Complete (SESC)

Versión	Cyber Defense Manager v2.0.9.122.7, Agent v14.3
Fabricante	Symantec a division of Broadcom
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	12/11/2025
Revisión de Validez	30/04/2028

Descripción

Symantec Endpoint Security Complete (SES Complete) es una solución integral para la protección avanzada de endpoints en entornos empresariales y gubernamentales. Ofrece defensas multicapa que combinan antivirus, antimalware, seguridad web y control de aplicaciones en un solo agente unificado ESA (Endpoint Security Agent), gestionado desde una consola unificada. Incluye capacidades de prevención, detección y respuesta ante amenazas avanzadas (EDR), mitigación de vulnerabilidades en memoria, protección contra malware sin archivos y directiva de acceso a la red de confianza cero. SES Complete añade funciones como protección y seguridad del directorio activo, analíticas de ataques en la nube, análisis forense automatizado y caza de amenazas basada en inteligencia artificial. Además, integra políticas contextuales adaptativas y autenticación multifactor, lo que facilita la defensa proactiva y la visibilidad total sobre los dispositivos de usuario final de las organizaciones.

Symantec Endpoint Security (SES) Complete incluye CBX, la plataforma unificada de Extended Detection and Response (XDR) de Broadcom/Symantec. La arquitectura de Symantec CBX consolida en un único ecosistema la protección, detección y respuesta en el endpoint (EPP/EDR), la seguridad en la navegación y tráfico web (Web Protection) y la prevención avanzada de pérdida de datos (Symantec DLP). A través del agente unificado ESA, la solución ejecuta políticas de prevención multicapa, análisis estático y dinámico mediante aprendizaje automático, sandboxing, aislamiento de superficie de ataque y contención adaptativa en tiempo real.

Observaciones

CCN-STIC-1247 Procedimiento de Empleo Seguro Symantec Endpoint Security Complete

INFORMACIÓN IMPORTANTE

Cytomic EPDR	
Versión	v4.6
Fabricante	WatchGuard Technologies
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	07/08/2025
Revisión de Validez	31/07/2027

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 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 1244 Panda Adaptive Defense 360 y Cytomic Advanced EPDR

WatchGuard Endpoint Security 360 (WatchGuard EPDR) / Elite (WatchGuard Advanced EPDR)	
Versión	EPDR 4.70, Manag. Agent. 1.25, Protect. Agent 8.00
Fabricante	WatchGuard Technologies
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	27/06/2025
Revisión de Validez	31/05/2027

Descripción

Endpoint Security 360 y Elite ofrecen una solución EDR escalable, autónoma y basada en el modelo Zero Trust. Amplían las capacidades de prevención, detección y respuesta con un completo conjunto de funciones de protección de endpoints diseñadas para impedir que las amenazas lleguen a los dispositivos y servidores, y para reducir la superficie de ataque. Para organizaciones maduras con equipos de seguridad dedicados que realizan investigaciones en profundidad, Endpoint Security Elite también proporciona visibilidad telemétrica completa, contexto de investigación enriquecido, búsqueda de amenazas basada en STIX/YARA, mapeo de TTP de MITRE, un asistente de IA generativa para el análisis del lenguaje natural y políticas de seguridad avanzadas. Ofrece protección de alto nivel y sólidas capacidades de respuesta automatizada con una carga operativa mínima.

Observaciones

CCN-STIC-1213 Procedimiento de Empleo Seguro en Proceso de Actualización

INFORMACIÓN IMPORTANTE

Panda Adaptive Defense 360

Versión	v4.6
Fabricante	WatchGuard Technologies
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	07/08/2025
Revisión de Validez	31/07/2027

Descripción

Panda Adaptive Defense 360 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 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 1244 Panda Adaptive Defense 360 y Cytomic Advanced EPDR

Trend Vision One Endpoint Security

Versión	20.0.1.4540
Fabricante	Trend Micro
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2028

Descripción

Vision One - Endpoint Security, es la propuesta EPP y EDR de Trend Micro para proteger Endpoints, Servidores como cargas de trabajo en nube.

Forma parte de la plataforma Trend Vision One, en conjunto con otras capacidades de protección: E-mail, NDR, CTEM, CNAPP, MDM, etc alimentando con la telemetría recogida la arquitectura XDR que facilita una detección temprana y protección frente a los retos que presenta el cibercrimen moderno.

El producto se ofrece tanto en formato SaaS (Trend Vision One Console) como On-Premise (Trend Vision One On-Prem Management Server).
El Trend Vision One On-Prem Management Server NO ESTÁ CUALIFICADO

Observaciones

CCN-STIC 1216 Procedimiento de Empleo Seguro Trend Vision One Endpoint Security

INFORMACIÓN IMPORTANTE

Sophos XDR

Versión

Fabricante Sophos

Familia Anti-virus / EPP (Endpoint Protection Platform)

Tipo Servicio

Categoría ENS MEDIA

Fecha Inclusión 01/03/2026

Revisión de Validez 29/02/2028

Descripción

La versión cualificada de este producto/servicio es: Sophos XDR (Core Agent: 2025.1.3.2.0, Sophos Intercept X: 2024.1.2.1.0), Sophos Central Admin: N/A

La plataforma de protección de endpoints de Sophos unifica prevención, detección y respuesta avanzadas en un único agente y consola cloud. Combina múltiples capas de seguridad para frenar ransomware, ataques fileless, zero-day y técnicas de explotación. Reduce la superficie de ataque mediante controles de USB, aplicaciones, navegación y DLP, y detecta malware con IA local, análisis de comportamiento y firmas de SophosLabs. Supervisa la integridad de los archivos para identificar ransomware local o remoto e incorpora protección adaptativa que eleva automáticamente la defensa ante indicios de actividad maliciosa.

Incluye capacidades de XDR para investigar incidentes, realizar threat hunting y analizar el alcance de amenazas mediante el Lago de Datos y asistentes de IA que explican hallazgos y resumen casos. Además, amplía la visibilidad integrando telemetría de firewalls, correo, identidad, backup, red y productividad, mientras sus asistentes de IA actúan como analistas y threat hunters virtuales, acelerando la detección, correlación y respuesta

Observaciones

CCN-STIC-1003 Procedimiento de empleo seguro Sophos XDR

INFORMACIÓN IMPORTANTE

Cynet 360

Versión	4.29.999.19020; Cynet XDR Console N/A
Fabricante	Cynet Security
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	MEDIA
Fecha Inclusión	11/03/2026
Revisión de Validez	31/10/2026

Descripción

Cynet ofrece una plataforma XDR unificada impulsada por IA que integra NGAV, EPP, EDR multi-OS (Windows (entorno cualificado), Linux, Mac), NDR y analítica centralizada de logs tipo SIEM con detecciones alineadas a MITRE ATT&CK, además de investigación y respuesta automatizadas de nivel SOAR en una sola consola. Extiende la protección a SaaS y Cloud mediante SSPM, CSPM y Cloud Detection & Response, junto con External Attack Surface Management, Seguridad del Email y Protección de Dispositivos Móviles. Incorpora Endpoint Security Posture Management para CVEs y configuraciones erróneas, evaluación de vulnerabilidades e inventario, visibilidad IoT, monitoreo de actividad de archivos, filtrado y protección web, analítica de comportamiento de usuarios, honeypots de engaño, protección de identidad e ITDR, inteligencia y caza de amenazas, además de amplias integraciones vía API. Ofrece detección y enriquecimiento basados en IA, remediaciones predefinidas y personalizadas, Playbooks y CyOps MDR 24/7 para monitoreo, caza proactiva, investigación, respuesta a incidentes, informes de amenazas y monitoreo de robo de credenciales. Se cuenta con equipos de soporte que guían la implementación, best-practices y el mantenimiento continuo 24/7

Observaciones

Procedimiento de Empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cortex XDR

Versión	Console v3.16 & Agent v9.0.0.16757
Fabricante	Palo Alto Networks
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/07/2025
Revisión de Validez	31/12/2027

Descripción

La plataforma Cortex de Palo Alto Networks integra tecnologías esenciales para las operaciones de ciberseguridad destacando EPP (protección de endpoints) y EDR (detección y respuesta en endpoints). Ofrece otras funcionalidades como ASM (gestión de superficie de ataque), SIEM (gestión de eventos), SOAR (orquestación y respuesta), ITDR (detección y respuesta de identidades), UEBA (análisis de comportamiento) y CDR (detección y respuesta en la nube). Todo se gestiona desde una consola unificada en la nube, que facilita visibilidad, coordinación y respuesta eficaz.

En ese contexto, Cortex XDR ofrece prevención, detección y respuesta extendida mediante la correlación nativa de telemetría desde red, endpoint, identidad, nube y correo electrónico. Se basa en inteligencia artificial, análisis de comportamiento y aprendizaje continuo para detectar malware, exploits y amenazas día cero con alta precisión, reducir falsos positivos y acelerar las investigaciones.

Se integran además novedades de la plataforma: Cortex Cloud, que amplía la cobertura a arquitecturas híbridas y multicloud; Exposure Management, que prioriza activos expuestos y vulnerabilidades según riesgo; y Advanced Email Security, que analiza correos mediante heurística, reglas y modelos LLM para detectar phishing, BEC y amenazas generadas por IA.

Observaciones

CCN-STIC-1222 Procedimiento de Empleo Seguro Cortex XDR Agent

INFORMACIÓN IMPORTANTE

7.3.2 EDR (ENDPOINT DETECTION AND RESPONSE)

SentinelOne Singularity Complete	
Versión	Agent 24.2.3.471
Fabricante	SentinelOne
Familia	EDR (Endpoint Detection and Response)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	22/07/2025
Revisión de Validez	30/06/2027
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 PES SentinelOne Singularity Complete

Microsoft Defender for Endpoint	
Versión	
Fabricante	Microsoft
Familia	EDR (Endpoint Detection and Response)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	16/06/2025
Revisión de Validez	31/05/2027
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

Falcon Sensor con Falcon Console Cloud	
Versión	7.21.19205
Fabricante	CrowdStrike
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/06/2025
Revisión de Validez	30/11/2027

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 Procedimiento de Empleo Seguro Falcon Sensor

Watchguard Endpoint Security Prime	
Versión	EPDR 4.70 Manag. Agent. 1.25, Protect. Agent 8.00
Fabricante	WatchGuard Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	30/06/2026
Revisión de Validez	31/05/2027

Descripción

Endpoint Security Prime ofrece protección de nivel empresarial gracias a sus completas capacidades de EDR, visibilidad a nivel de incidente, contexto de los ataques y análisis de las causas fundamentales. Al consolidar las señales relacionadas en una vista unificada de los incidentes, las organizaciones pueden comprender rápidamente los eventos de seguridad, identificar los activos afectados y priorizar las medidas de respuesta. Diseñado para equipos que no cuentan con analistas de seguridad especializados, reduce el ruido de las alertas y la sobrecarga operativa, al tiempo que proporciona la visibilidad y el contexto necesarios para mejorar la postura de seguridad, reducir la exposición al riesgo y responder a las amenazas actuales.

Observaciones

CCN-STIC-1213 Procedimiento de Empleo Seguro en Proceso de Actualización

INFORMACIÓN IMPORTANTE

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

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

TEHTRIS Endpoint Detection and Response	
Versión	1.8.1
Fabricante	TEHTRI-SECURITY SPAIN
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/06/2024
Revisión de Validez	30/11/2026

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 analisis completo de los endpoints con capacidades de investigación avanzada (Threat Hunting, compliance, analisis 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

CCN-STIC 1233 Procedimiento de Empleo Seguro Tehtris EDR

INFORMACIÓN IMPORTANTE

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

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

CCN-STIC-1230 Procedimiento de Empleo Seguro Bitdefender GravityZone

INFORMACIÓN IMPORTANTE

Symantec EndPoint Security Complete (SESC)

Versión	Cyber Defense Manager v2.0.9.122.7, Agent v14.3
Fabricante	Symantec a division of Broadcom
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	12/11/2025
Revisión de Validez	30/04/2028

Descripción

Symantec Endpoint Security Complete (SES Complete) es una solución integral para la protección avanzada de endpoints en entornos empresariales y gubernamentales. Ofrece defensas multicapa que combinan antivirus, antimalware, seguridad web y control de aplicaciones en un solo agente unificado ESA (Endpoint Security Agent), gestionado desde una consola unificada. Incluye capacidades de prevención, detección y respuesta ante amenazas avanzadas (EDR), mitigación de vulnerabilidades en memoria, protección contra malware sin archivos y directiva de acceso a la red de confianza cero. SES Complete añade funciones como protección y seguridad del directorio activo, analíticas de ataques en la nube, análisis forense automatizado y caza de amenazas basada en inteligencia artificial. Además, integra políticas contextuales adaptativas y autenticación multifactor, lo que facilita la defensa proactiva y la visibilidad total sobre los dispositivos de usuario final de las organizaciones.

Symantec Endpoint Security (SES) Complete incluye CBX, la plataforma unificada de Extended Detection and Response (XDR) de Broadcom/Symantec. La arquitectura de Symantec CBX consolida en un único ecosistema la protección, detección y respuesta en el endpoint (EPP/EDR), la seguridad en la navegación y tráfico web (Web Protection) y la prevención avanzada de pérdida de datos (Symantec DLP). A través del agente unificado ESA, la solución ejecuta políticas de prevención multicapa, análisis estático y dinámico mediante aprendizaje automático, sandboxing, aislamiento de superficie de ataque y contención adaptativa en tiempo real.

Observaciones

CCN-STIC-1247 Procedimiento de Empleo Seguro Symantec Endpoint Security Complete

INFORMACIÓN IMPORTANTE

Cytomic EPDR

Versión	v4.6
Fabricante	WatchGuard Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	07/08/2025
Revisión de Validez	31/07/2027

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 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 1244 Panda Adaptive Defense 360 y Cytomic Advanced EPDR

FortiEDR

Versión	6.0
Fabricante	Fortinet
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	24/04/2025
Revisión de Validez	30/09/2027

Descripción

FortiEDR es una solución integral de seguridad para Endpoints que ofrece protección en tiempo real, automatizada y con respuesta a incidentes orquestada. Protege diversos sistemas operativos y plataformas, incluyendo la nube, mediante la prevención, detección y respuesta a amenazas avanzadas, incluso en dispositivos ya comprometidos. FortiEDR emplea aprendizaje automático a nivel de kernel (en Windows y Linux) para bloquear las brechas y proteger los datos de la exfiltración y el cifrado de ransomware.
Integra varias herramientas de Fortinet y de terceros, facilitando la gestión y automatización de la seguridad. Su arquitectura permite una implementación flexible y escalable, reduciendo los tiempos de detección y respuesta a incidentes. Finalmente, ofrece servicios gestionados opcionales para una mayor seguridad.

Observaciones

CCN-STIC 1010 Procedimiento de Empleo Seguro FortiEDR

INFORMACIÓN IMPORTANTE

WatchGuard Endpoint Security 360 (WatchGuard EPDR) / Elite (WatchGuard Advanced EPDR)	
Versión	EPDR 4.70, Manag. Agent. 1.25, Protect. Agent 8.00
Fabricante	WatchGuard Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	27/06/2025
Revisión de Validez	31/05/2027
Descripción	

Endpoint Security 360 y Elite ofrecen una solución EDR escalable, autónoma y basada en el modelo Zero Trust. Amplían las capacidades de prevención, detección y respuesta con un completo conjunto de funciones de protección de endpoints diseñadas para impedir que las amenazas lleguen a los dispositivos y servidores, y para reducir la superficie de ataque. Para organizaciones maduras con equipos de seguridad dedicados que realizan investigaciones en profundidad, Endpoint Security Elite también proporciona visibilidad telemétrica completa, contexto de investigación enriquecido, búsqueda de amenazas basada en STIX/YARA, mapeo de TTP de MITRE, un asistente de IA generativa para el análisis del lenguaje natural y políticas de seguridad avanzadas. Ofrece protección de alto nivel y sólidas capacidades de respuesta automatizada con una carga operativa mínima.

Observaciones

CCN-STIC-1213 Procedimiento de Empleo Seguro en Proceso de Actualización

Panda Adaptive Defense 360	
Versión	v4.6
Fabricante	WatchGuard Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	07/08/2025
Revisión de Validez	31/07/2027
Descripción	

Panda Adaptive Defense 360 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 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 1244 Panda Adaptive Defense 360 y Cytomic Advanced EPDR

INFORMACIÓN IMPORTANTE

Trend Vision One Endpoint Security

Versión	20.0.1.4540
Fabricante	Trend Micro
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2028

Descripción

Vision One - Endpoint Security, es la propuesta EPP y EDR de Trend Micro para proteger Endpoints, Servidores como cargas de trabajo en nube.

Forma parte de la plataforma Trend Vision One, en conjunto con otras capacidades de protección: E-mail, NDR, CTEM, CNAPP, MDM, etc alimentando con la telemetría recogida la arquitectura XDR que facilita una detección temprana y protección frente a los retos que presenta el cibercrimen moderno.

El producto se ofrece tanto en formato SaaS (Trend Vision One Console) como On-Premise (Trend Vision One On-Prem Management Server).
El Trend Vision One On-Prem Management Server NO ESTÁ CUALIFICADO

Observaciones

CCN-STIC 1216 Procedimiento de Empleo Seguro Trend Vision One Endpoint Security

Harmony Mobile - Android

Versión	5.0.3.10688
Fabricante	Check Point Software Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2026
Revisión de Validez	31/12/2026

Descripción

Harmony Mobile es una solución de seguridad móvil (MTD - Mobile Threat Defense) diseñada para proteger dispositivos corporativos y BYOD frente a vectores de ataque avanzados. La solución garantiza la integridad de los terminales mediante un análisis multinivel que abarca:

Protección de Red: Prevención de ataques Man-in-the-Middle y filtrado de contenido malicioso mediante inspección en tiempo real.
Seguridad de Aplicaciones: Análisis estático y dinámico de apps para detectar malware, vulnerabilidades y comportamientos de riesgo.
Defensa del Sistema: Detección de alteraciones en el sistema operativo (rooting/jailbreak) y configuraciones vulnerables.
Privacidad por Diseño: Despliegue no intrusivo que protege los datos corporativos sin comprometer la privacidad personal ni el rendimiento del dispositivo.

Observaciones

Procedimiento de Empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

Sophos XDR

Versión

Fabricante Sophos

Familia EDR (Endpoint Detection and Response)

Tipo Servicio

Categoría ENS MEDIA

Fecha Inclusión 01/03/2026

Revisión de Validez 29/02/2028

Descripción

La versión cualificada de este producto/servicio es: Sophos XDR (Core Agent: 2025.1.3.2.0, Sophos Intercept X: 2024.1.2.1.0), Sophos Central Admin: N/A

La plataforma de protección de endpoints de Sophos unifica prevención, detección y respuesta avanzadas en un único agente y consola cloud. Combina múltiples capas de seguridad para frenar ransomware, ataques fileless, zero-day y técnicas de explotación. Reduce la superficie de ataque mediante controles de USB, aplicaciones, navegación y DLP, y detecta malware con IA local, análisis de comportamiento y firmas de SophosLabs. Supervisa la integridad de los archivos para identificar ransomware local o remoto e incorpora protección adaptativa que eleva automáticamente la defensa ante indicios de actividad maliciosa.

Incluye capacidades de XDR para investigar incidentes, realizar threat hunting y analizar el alcance de amenazas mediante el Lago de Datos y asistentes de IA que explican hallazgos y resumen casos. Además, amplía la visibilidad integrando telemetría de firewalls, correo, identidad, backup, red y productividad, mientras sus asistentes de IA actúan como analistas y threat hunters virtuales, acelerando la detección, correlación y respuesta

Observaciones

CCN-STIC-1003 Procedimiento de empleo seguro Sophos XDR

INFORMACIÓN IMPORTANTE

Cynet 360

Versión	4.29.999.19020; Cynet XDR Console N/A
Fabricante	Cynet Security
Familia	EDR (Endpoint Detection and Response)
Tipo	Servicio
Categoría ENS	MEDIA
Fecha Inclusión	11/03/2026
Revisión de Validez	31/10/2026

Descripción

Cynet ofrece una plataforma XDR unificada impulsada por IA que integra NGAV, EPP, EDR multi-OS (Windows (entorno cualificado), Linux, Mac), NDR y analítica centralizada de logs tipo SIEM con detecciones alineadas a MITRE ATT&CK, además de investigación y respuesta automatizadas de nivel SOAR en una sola consola. Extiende la protección a SaaS y Cloud mediante SSPM, CSPM y Cloud Detection & Response, junto con External Attack Surface Management, Seguridad del Email y Protección de Dispositivos Móviles. Incorpora Endpoint Security Posture Management para CVEs y configuraciones erróneas, evaluación de vulnerabilidades e inventario, visibilidad IoT, monitoreo de actividad de archivos, filtrado y protección web, analítica de comportamiento de usuarios, honeypots de engaño, protección de identidad e ITDR, inteligencia y caza de amenazas, además de amplias integraciones vía API. Ofrece detección y enriquecimiento basados en IA, remediaciones predefinidas y personalizadas, Playbooks y CyOps MDR 24/7 para monitoreo, caza proactiva, investigación, respuesta a incidentes, informes de amenazas y monitoreo de robo de credenciales. Se cuenta con equipos de soporte que guían la implementación, best-practices y el mantenimiento continuo 24/7

Observaciones

Procedimiento de Empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

Harmony Mobile - iOS

Versión	5.2.0.16232 con OPN VPN v4.15.292
Fabricante	Check Point Software Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2026
Revisión de Validez	31/12/2026

Descripción

Harmony Mobile es una solución de seguridad móvil (MTD - Mobile Threat Defense) diseñada para proteger dispositivos corporativos y BYOD frente a vectores de ataque avanzados. La solución garantiza la integridad de los terminales mediante un análisis multinivel que abarca:

Protección de Red: Prevención de ataques Man-in-the-Middle y filtrado de contenido malicioso mediante inspección en tiempo real.

Seguridad de Aplicaciones: Análisis estático y dinámico de apps para detectar malware, vulnerabilidades y comportamientos de riesgo.

Defensa del Sistema: Detección de alteraciones en el sistema operativo (rooting/jailbreak) y configuraciones vulnerables.

Privacidad por Diseño: Despliegue no intrusivo que protege los datos corporativos sin comprometer la privacidad personal ni el rendimiento del dispositivo.

Observaciones

Procedimiento de Empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cortex XDR

Versión	Console v3.16 & Agent v9.0.0.16757
Fabricante	Palo Alto Networks
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/07/2025
Revisión de Validez	31/12/2027

Descripción

La plataforma Cortex de Palo Alto Networks integra tecnologías esenciales para las operaciones de ciberseguridad destacando EPP (protección de endpoints) y EDR (detección y respuesta en endpoints). Ofrece otras funcionalidades como ASM (gestión de superficie de ataque), SIEM (gestión de eventos), SOAR (orquestación y respuesta), ITDR (detección y respuesta de identidades), UEBA (análisis de comportamiento) y CDR (detección y respuesta en la nube). Todo se gestiona desde una consola unificada en la nube, que facilita visibilidad, coordinación y respuesta eficaz.
En ese contexto, Cortex XDR ofrece prevención, detección y respuesta extendida mediante la correlación nativa de telemetría desde red, endpoint, identidad, nube y correo electrónico. Se basa en inteligencia artificial, análisis de comportamiento y aprendizaje continuo para detectar malware, exploits y amenazas día cero con alta precisión, reducir falsos positivos y acelerar las investigaciones.
Se integran además novedades de la plataforma: Cortex Cloud, que amplía la cobertura a arquitecturas híbridas y multicloud; Exposure Management, que prioriza activos expuestos y vulnerabilidades según riesgo; y Advanced Email Security, que analiza correos mediante heurística, reglas y modelos LLM para detectar phishing, BEC y amenazas generadas por IA.

Observaciones

CCN-STIC-1222 Procedimiento de Empleo Seguro Cortex XDR Agent

INFORMACIÓN IMPORTANTE

7.3.3 HERRAMIENTAS DE GESTIÓN DE DISPOSITIVOS (UEM)

EndPoint Mobile Manager	
Versión	Server v12.7.1.0-36, Agente v12.9.0.0.1R
Fabricante	Ivanti
Familia	Herramientas de Gestión de dispositivos (UEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2026
Revisión de Validez	28/02/2027

Descripción

English
Ivanti Endpoint Manager Mobile (EPMM) is an Enterprise Mobility Management (EMM) and Unified Endpoint Management (UEM) solution that provides centralized administration, security, and control for enterprise mobile and endpoint devices. The system enables organizations to enforce security policies, protect corporate data, and ensure compliant access to business resources.

Ivanti EPMM enables administrators to manage the device lifecycle from provisioning through retirement.

Core functions include device enrollment, user and device inventory, policy and configuration deployment, certificate management, compliance evaluation, device actions, and audit and reporting capabilities.

Ivanti EPMM also supports application distribution and update management, while enabling identity, connectivity, and security functions through profiles, restrictions, and certificate deployment. Administrators can monitor device status, control software deployment, and take remediation actions when devices fall out of compliance.

Spanish
Ivanti Endpoint Manager Mobile (EPMM) es una solución de gestión de movilidad empresarial (EMM) y de gestión unificada de terminales (UEM) que ofrece administración, seguridad y control centralizados para los dispositivos móviles y terminales de la empresa. El sistema permite a las organizaciones aplicar políticas de seguridad, proteger los datos corporativos y garantizar un acceso conforme a la normativa a los recursos empresariales.

Ivanti EPMM permite a los administradores gestionar el ciclo de vida de los dispositivos, desde su aprovisionamiento hasta su retirada.

Entre sus funciones principales se incluyen el registro de dispositivos, el inventario de usuarios y dispositivos, la implementación de políticas y configuraciones, la gestión de certificados, la evaluación del cumplimiento normativo, las acciones sobre los dispositivos y las capacidades de auditoría y generación de informes.

Ivanti EPMM también admite la distribución de aplicaciones y la gestión de actualizaciones, al tiempo que habilita funciones de identidad, conectividad y seguridad mediante perfiles, restricciones y la implementación de certificados. Los administradores pueden supervisar el estado de los dispositivos, controlar la implementación de software y tomar medidas correctivas cuando los dispositivos incumplan los requisitos de cumplimiento normativo.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Essentials Mobile Threat Defense	
Versión	5.38
Fabricante	Techstep
Familia	Herramientas de Gestión de dispositivos (UEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/07/2025
Revisión de Validez	30/01/2028

Descripción

(ES) Essentials Mobile Threat Defense es una solución avanzada de Gestión Unificada de Dispositivos de Trabajo (UEM) diseñada para proteger, configurar y administrar smartphones, tablets, MacBooks y dispositivos rugerizados en toda la organización. Disponible en modalidad on-premise, garantiza la soberanía total de los datos y el cumplimiento de los más estrictos requisitos de seguridad.

Compatible con entornos multiOS (Android, iOS, macOS, tvOS), Essentials Mobile Threat Defense permite a los equipos de TI mantener el control, optimizar la productividad y proteger la información confidencial, cumpliendo con las normativas regulatorias.

https://www.techstep.io/es/essentials-mobile-threat-defense

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.3.4 HERRAMIENTAS DE SANDBOX

Deep Discovery Inspector	
Versión	6.5.1129
Fabricante	Trend Micro
Familia	Herramientas de Sandbox
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/11/2026

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

7.4 PROTECCIÓN DE REDES Y SISTEMAS

7.4.1 SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM)

BigSIEM	
Versión	NA
Fabricante	Secure&IT
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	24/02/2025
Revisión de Validez	30/09/2029
Descripción	

BigSIEM es un motor de correlación de eventos de seguridad diseñado para detectar y responder rápidamente ante amenazas informáticas. Se trata de un concepto integrado SIEM+XDR+SOAR. BigSIEM integra un BigDATA para la ingesta y custodia segura de logs, la integración con proveedores de inteligencia, el motor de análisis basado en Threat Analyzer y el módulo de Intelligence Engine, que realiza correlaciones avanzadas de eventos, detección heurística, monitorización y alertas, aprendiendo del comportamiento de los sistemas protegidos en base a una IA.
BigSIEM permite análisis en tiempo real, inteligencia de seguridad, alertas y notificaciones, herramientas de visualización y control, priorización de eventos, respuesta inmediata ante incidentes (BigSOAR), generación de informes y cumplimiento normativo.

Observaciones

CCN-STIC 1241 Procedimiento de Empleo Seguro BigSIEM

INFORMACIÓN IMPORTANTE

Chronicle SIEM

Versión	
Fabricante	Google
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	16/02/2024
Revisión de Validez	30/11/2026

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

CCN-STIC 1234 Procedimiento de Empleo Seguro Chronicle SIEM & SOAR

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

INFORMACIÓN IMPORTANTE

LogPoint SIEM

Versión	7.4.0.4
Fabricante	LogPoint
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/03/2025
Revisión de Validez	31/08/2027

Descripción

Logpoint SIEM es una herramienta de Analálisis y Gestión de eventos de seguridad. Logpoint ofrece un análisis rápido e informes enriquecidos.Por otro lado, es capaz de ofrecer una gran variedad de informes de cumplimiento gracias a la base de plantillas built-in de las que dispone.
Como parte de la infraestructura de Logpoint, el SIEM tiene la posibilidad de integracion con Logpoint SOAR y con Logpoint NDR.

Observaciones

CCN-STIC 1242 Procedimiento de Empleo Seguro LogPoint SIEM

Amazon GuardDuty

Versión	
Fabricante	AWS
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	14/03/2025
Revisión de Validez	28/02/2027

Descripción

Amazon GuardDuty es un servicio de detección de amenazas que monitoriza continuamente la actividad maliciosa y el comportamiento anómalo para proteger sus cuentas de AWS, cargas de trabajo, clústeres de Kubernetes y datos almacenados en Amazon Simple Storage Service (Amazon S3). El servicio GuardDuty monitoriza actividades como llamadas API inusuales, despliegues no autorizados y credenciales filtradas que indican un posible reconocimiento o compromiso de la cuenta. GuardDuty identifica a los atacantes sospechosos a través de fuentes integradas de inteligencia sobre amenazas y detección de anomalías mediante aprendizaje automático para detectar anomalías en la actividad de las cuentas y las cargas de trabajo. Cuando se detecta un posible uso no autorizado, el servicio envía un informe detallado a la consola de GuardDuty, Amazon CloudWatch Events y AWS Security Hub. Esto hace que los hallazgos sean procesables y fáciles de integrar en los sistemas existentes de gestión de eventos y flujos de trabajo. La investigación adicional para determinar la causa raíz de un hallazgo se realiza fácilmente utilizando Amazon Detective directamente desde la consola de GuardDuty.

Observaciones

CCN-STIC-887A Guía de configuración segura AWS

INFORMACIÓN IMPORTANTE

MONSE	
Versión	Probe 1.0, Agente 8.18.2
Fabricante	GRUPO CIES
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	31/12/2026

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

INFORMACIÓN IMPORTANTE

Splunk Cloud

Versión	9.3
Fabricante	Splunk
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	15/06/2025
Revisión de Validez	31/05/2027

Descripción

Splunk Cloud Platform es la versión como servicio en la nube de Splunk Enterprise, que ofrece las mismas capacidades de recopilación, búsqueda, monitorización, generación de informes y análisis de datos de máquina, tanto en tiempo real como históricos. Es una solución nativa en la nube, gestionada y actualizada de forma centralizada por Splunk, lo que garantiza un acceso uniforme y continuo a las funcionalidades más recientes, bajo altos estándares de seguridad y disponibilidad.
La plataforma incorpora capacidades avanzadas de Detección, Investigación y Respuesta ante Amenazas (TDIR) mediante la aplicación Splunk Enterprise Security (ES), y permite la orquestación y automatización de respuestas a incidentes a través de Splunk SOAR. Proporciona correlación de eventos en tiempo real, análisis contextual, priorización basada en riesgos e integración con fuentes externas de inteligencia de amenazas.
Splunk Cloud es compatible con marcos de referencia como MITRE ATT&CK y facilita la implementación de casos de uso esenciales alineados con los controles del Esquema Nacional de Seguridad (ENS), todo ello en un entorno SaaS gestionado, con actualizaciones automáticas, alta disponibilidad y soporte para entornos híbridos y multinube.

Observaciones

CCN-STIC 1243 Procedimiento de Empleo Seguro Splunk Cloud

Devo SIEM

Versión	
Fabricante	Devo Technology
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	08/04/2025
Revisión de Validez	31/03/2027

Descripción

Devo es una plataforma nativa en la nube de registro y análisis de seguridad. Devo ingiere registros a escala de la nube, almacena todos los registros en su formato nativo y permite al cliente consultar los datos inmediatamente después de la ingesta inicial. Devo proporciona múltiples aplicaciones en la plataforma, entre ellas Devo Intelligent SIEM, Security Operations, MITRE ATT&CK Advisor, Relay y Collectors, lo que permite a los equipos SOC y de operaciones de TI del cliente aprovechar los mismos datos y colaborar en ellos.

Observaciones

CCN-STIC 1245 Procedimiento de Empleo Seguro DEVO SIEM

INFORMACIÓN IMPORTANTE

Microsoft Sentinel

Versión	
Fabricante	Microsoft
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/01/2027

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

NetWitness Platform	
Versión	12.5
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	29/06/2027

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 Analitics) 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

Elastic Platform	
Versión	8.15.2
Fabricante	ELASTIC
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/12/2025
Revisión de Validez	31/05/2028

Descripción

Elastic, The Search AI Company, integra su experiencia en tecnología de búsqueda con inteligencia artificial para ayudar a transformar el crecimiento exponencial de datos no estructurados y que no se aprovechan para accionar respuestas y obtener resultados.
Elastic Search AI Platform es la base de las dos soluciones listas para usar de Elastic (Seguridad y Observabilidad), que cuenta con 3 características clave:

1) Abierta por diseño: La apertura impulsa el ingenio y la creatividad.

2) Orientada al rendimiento: la velocidad, la escala y la relevancia no son negociables.

3) Acelera la innovación ante un panorama de datos en continua evolución.

Elastic Security, con su SIEM en el core de la solución XDR, proporciona la visibilidad completa en toda la superficie de ataque que los analistas del SOC necesitan para modernizar su enfoque de detección, investigación y respuesta. Los cientos de integraciones, reglas de correlación e inteligencia sobre amenazas alimentada por el laboratorio de Elastic, reducen los tiempos de resolución. Además, con sus módulos Observability y Elasticsearch se proporciona una visibilidad unificada con capacidades de automatización que necesarias para minimizar el tiempo de inactividad, optimizar el rendimiento y resolver incidentes más rápido.

Observaciones

CCN-STIC-1246 Procedimiento de Empleo Seguro Elastic Platform

INFORMACIÓN IMPORTANTE

Splunk Enterprise

Versión	9.4
Fabricante	Splunk
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2024
Revisión de Validez	16/12/2026

Descripción

Splunk Enterprise es una plataforma de gestión de eventos e información de seguridad (SIEM) que proporciona una visibilidad completa de la postura de seguridad de una organización. Permite gestionar el ciclo completo de seguridad, incluyendo capacidades de Detección, Monitorización, Investigación y Respuesta ante incidentes de seguridad (TDIR).

La plataforma incorpora capacidades avanzadas de búsqueda, generación de informes y análisis en tiempo real e histórico, 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 aquellos que afectan a activos o identidades críticas, así como generar alertas basadas en riesgo e identificar anomalías y amenazas tanto externas como internas.

Además, Splunk Enterprise permite la orquestación y automatización de respuestas a incidentes mediante Splunk SOAR, proporcionando correlación de eventos en tiempo real, análisis contextual, priorización basada en riesgos e integración con fuentes externas de inteligencia de amenazas. Las más de 2.500 reglas de detección abarcan todos los ámbitos de seguridad: IT, OT, IoT, IoMT y nubes públicas en cualquiera de sus formatos.

Observaciones

CCN-STIC-1225 Procedimiento de Empleo Seguro Splunk Enterprise 9.4

INFORMACIÓN IMPORTANTE

FortiAnalyzer	
Versión	7.2
Fabricante	Fortinet
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2024
Revisión de Validez	31/12/2027

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 predefinidias (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.
Modelos:
Familia E: FAZ-400E, FAZ-2000E, FAZ-3500E.
Familia F: FAZ-200F, FAZ-300F, FAZ-800F, FAZ-1000F, FAZ-3000F, FAZ-3500F, FAZ-3700F.
Familia G: FAZ-150G, FAZ-300G, FAZ-800G, FAZ-810G, FAZ-1000G, FAZ-3000G, FAZ-3100G, FAZ-3500G, FAZ-3510G, FAZ-3700G.
Modelos VM: FAZ-VM, FAZ-VM64, FAZ-VM64-ALI, FAZ-VM64-AWS, FAZ-VM64-AWSOnDemand, FAZ-VM64-AZURE, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-IBM, FAZ-VM64-KVC, FAZ-VM64-OPC, FAZ-VM64-XEN.

Observaciones

CCN-STIC-1444 Procedimiento de empleo seguro FortiAnalyzer

INFORMACIÓN IMPORTANTE

NGSIEM Logica - Monica

Versión	8.0
Fabricante	ICA Sistemas y Seguridad
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2026
Revisión de Validez	31/12/2026

Descripción

LogICA
La plataforma española LogICA Next Generation SIEM permite a los equipos de ciberseguridad recopilar y analizar información de seguridad a gran escala, detectar amenazas avanzadas mediante analítica de comportamiento, anomalías e inteligencia de amenazas, y automatizar procesos de investigación y respuesta ante incidentes en entornos IT, OT, IoT y cloud. LogICA integra información de cualquier fuente corporativa, tecnológica o de negocio, correlando y enriqueciendo datos en tiempo real para proporcionar visibilidad del riesgo y facilitar la priorización de incidentes. Su arquitectura abierta combina capacidades SIEM, análisis avanzado, threat hunting, detección basada en comportamiento e integración con fuentes de inteligencia externas, permitiendo identificar amenazas conocidas y emergentes con mayor precisión. Asimismo, se integra con herramientas y asistentes basados en Inteligencia Artificial que facilitan la investigación, contextualización y gestión de incidentes de seguridad, mejorando la productividad de los equipos SOC. Además, incorpora capacidades de monitorización operativa, cuadros de mando y automatización de procesos de seguridad, adaptándose a despliegues on-premise, virtualizados, híbridos o cloud.

MONICA
La plataforma española MONICA NG SIEM permite a los analistas de ciberseguridad recopilar, correlacionar y analizar información de seguridad de cualquier fuente tecnológica o de negocio, ofreciendo capacidades avanzadas de detección, investigación y respuesta ante amenazas en entornos IT, OT, IoT y cloud. MONICA procesa eventos y telemetría en tiempo real mediante correlación avanzada, analítica de comportamiento, detección de anomalías e inteligencia de amenazas para identificar actividades maliciosas, vulnerabilidades y riesgos emergentes. Facilita la contextualización y priorización de incidentes mediante el enriquecimiento de la información y casos de uso especializados. Asimismo, se integra con herramientas y asistentes basados en Inteligencia Artificial para apoyar la investigación y gestión de incidentes, reduciendo los tiempos de detección y respuesta. MONICA dispone además de capacidades nativas de integración con herramientas y servicios del ecosistema del Centro Criptológico Nacional, favoreciendo la interoperabilidad y el intercambio seguro de información. Su arquitectura abierta y escalable permite automatizar operaciones e integrarse en despliegues on-premise, virtualizados, híbridos o cloud.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

GLORIA

Versión	6.26.0
Fabricante	S2 Grupo Soluciones de Seguridad S.L
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2026
Revisión de Validez	28/02/2027

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

7.4.2 SISTEMAS DE ORQUESTACIÓN, AUTOMATIZACIÓN Y RESPUESTA DE SEGURIDAD (SOAR)

Chronicle SOAR	
Versión	
Fabricante	Google
Familia	Sistemas de orquestación, automatización y respuesta de seguridad (SOAR)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	24/02/2025
Revisión de Validez	31/01/2027
Descripción	

Google SecOps - SOAR, una solución de seguridad, orquestación, automatización y respuesta (SOAR) nativa de la nube, permite a los equipos de seguridad responder a las ciberamenazas en cuestión de minutos. Google SecOps - SOAR fusiona un enfoque único centrado en las amenazas, una automatización de playbooks potente pero sencilla y una investigación rica en contexto para liberar tiempo valioso y permitir que los miembros del equipo de seguridad estén informados y sean productivos y eficaces.

Observaciones

CCN-STIC 1234 Procedimiento de Empleo Seguro Chronicle SIEM & SOAR

INFORMACIÓN IMPORTANTE

7.4.3 HERRAMIENTAS DE GESTIÓN DE RED

BMC	
Versión	3.8.6.11
Fabricante	xFusion Digital Technologies Co., Ltd.
Familia	Herramientas de gestión de red
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2026
Revisión de Validez	31/03/2027

Descripción

The iBMC (intelligent Baseboard Management Controller) is the management and control unit for servers. The BMC provides interfaces such as IPMI, SNMP, Redfish, web, and CLI to meet various system integration needs. It can realize remote control and maintenance of servers, provide comprehensive monitoring of servers, and provide rich and detailed logs, effectively improving server management efficiency and reducing operating costs.

El iBMC (controlador inteligente de gestión de placa base) es la unidad de gestión y control de los servidores. El BMC proporciona interfaces como IPMI, SNMP, Redfish, web y CLI para satisfacer diversas necesidades de integración de sistemas. Permite controlar y mantener los servidores de forma remota, supervisarlos de manera integral y generar registros completos y detallados, lo que mejora eficazmente la eficiencia de su gestión y reduce los costes operativos.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

iMC MagicBox

Versión	7.3
Fabricante	New H3C Technologies
Familia	Herramientas de gestión de red
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/08/2025
Revisión de Validez	31/01/2028

Descripción

H3C iMC (Centro de Gestión Inteligente) es una plataforma flexible y escalable diseñada para las necesidades integrales de gestión de red de empresas globales. iMC y sus componentes, como EIA, ofrecen seguridad integrada, monitorización, control de acceso, análisis basado en IA, interfaces de enlace Norte – Sur. Su arquitectura se basa en jerarquías de acceso y control habituales en a gran escala. Soporta gestión de dispositivos de terceros que proteger las inversiones existentes. Estas capacidades ayudan a los clientes a reducir significativamente los gastos operativos basados en gestión y mantenimiento.

Observaciones

CCN-STIC 1119 Procedimiento de Empleo Seguro iMC MagicBox

NetinDS

Versión	2.0.2
Fabricante	Mytra Control
Familia	Herramientas de gestión de red
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	20/11/2024
Revisión de Validez	30/04/2027

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

CCN-STIC 1235. Procedimiento de Empleo Seguro NetinDS

INFORMACIÓN IMPORTANTE

FortiManager

Versión	7.2
Fabricante	Fortinet
Familia	Herramientas de gestión de red
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2024
Revisión de Validez	30/11/2027

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".
Modelos:

- Familia E: FMG-300E, FMG-400E y FMG-2000E.
- Familia F: FMG-200F, FMG-300F, FMG-1000F, FMG-3000F y FMG-3700F.
- Familia G: FMG-200G, FMG-400G, FMG-410G, FMG-1000G, FMG-3000G, FMG-3100G y FMG-3700G.
- Familia VM: FMG-VM.

Observaciones

CCN-STIC-1443 Procedimiento de empleo seguro FortiManager

INFORMACIÓN IMPORTANTE

7.4.4 DETECCIÓN Y RESPUESTA DE AMENAZAS EN RED (NDR)

AWS CloudWatch	
Versión	
Fabricante	AWS
Familia	Detección y respuesta de amenazas en red (NDR)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	31/12/2026

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

CARMEN	
Versión	Versión 7.24.3
Fabricante	S2 GRUPO / CCN
Familia	Detección y respuesta de amenazas en red (NDR)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/10/2026

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

GigaVUE(HC3, HC1, HC1Plus, HCT), GigaVUE(TA25, TA25E, TA200, TA200E, TA400), GTAP	
Versión	6.5
Fabricante	Gigamon
Familia	Detección y respuesta de amenazas en red (NDR)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	09/07/2025
Revisión de Validez	31/12/2027

Descripción

Gigamon ofrece una plataforma de visibilidad y análisis del tráfico de red que potencia la seguridad y el rendimiento de las infraestructuras TI. Sus capacidades no son de seguridad directa como un firewall o un antivirus, sino que complementan las herramientas de ciberseguridad proporcionando datos más precisos, completos y procesables. Entre sus principales capacidades de seguridad destacan la visibilidad profunda del tráfico de red (Deep Observability)y optimización del tráfico para herramientas de seguridad. También, posee detección y respuesta mejoradas (XDR, SIEM, NDR) y descifrado de tráfico cifrado (SSL/TLS Decryption). Otras caracteristicas que ofrece GigaVUE son la segmentación y control del acceso a tráfico, la seguridad en entornos híbridos y multicloud y la posibilidad de integración con ecosistema de seguridad.

Observaciones

CCN-STIC 1301 Procedimiento de Empleo Seguro GigaVUE 6.5

INFORMACIÓN IMPORTANTE

Azure Activity Log

Versión

Fabricante Microsoft

Familia Detección y respuesta de amenazas en red (NDR)

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 04/03/2025

Revisión de Validez 28/02/2027

Descripción

Microsoft Azure Activity Log es un servicio que registra de forma automática y continua las actividades a nivel de suscripción en la plataforma Azure. Funciona capturando eventos del plano de control, lo que abarca operaciones como la creación, modificación y eliminación de recursos, proporcionando detalles precisos sobre quién ejecutó cada acción, cuándo se realizó y sobre qué elemento incidió. Además, permite filtrar la información por recursos, tipo de operación y rango de tiempo, facilitando así la consulta y el seguimiento de las actividades registradas. Su integración con otros servicios de monitorización y análisis posibilita la exportación de los registros a sistemas externos para una evaluación más profunda, la generación de alertas y el diagnóstico de anomalías. Azure Activity Log ofrece una visión centralizada y detallada de la administración y evolución de la infraestructura en la nube con una operativa sencilla con la capacidad de soportar procesos de auditoría y control.

Observaciones

CCN-STIC-1308 Procedimiento de Empleo Seguro Azure Activity Log

Azure Monitor Log Analytics

Versión

Fabricante Microsoft

Familia Detección y respuesta de amenazas en red (NDR)

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 03/03/2025

Revisión de Validez 28/02/2027

Descripción

Microsoft Azure Monitor Log Analytics es una herramienta que centraliza la recopilación, el almacenamiento y el análisis de datos generados por recursos de Azure, aplicaciones y sistemas operativos, permitiendo explorar grandes volúmenes de información a través de un lenguaje de consultas avanzado basado en Kusto Query Language. Su arquitectura escalable posibilita el procesamiento de datos en tiempo real, facilitando la correlación de registros, la identificación de patrones y la detección de anomalías, mientras que sus capacidades para configurar alertas y paneles personalizados ofrecen una visión integral del rendimiento y la seguridad de las infraestructuras digitales. Asimismo, integra datos provenientes de diversas fuentes, lo que permite un diagnóstico detallado de incidencias y la optimización de operaciones mediante informes configurables y acciones automatizadas, todo bajo una plataforma analítica adaptable a distintos escenarios operativos.

Observaciones

CCN-STIC-1307 Procedimiento de Empleo Seguro Azure Monitor Log Analytics

INFORMACIÓN IMPORTANTE

Claroty IoMT, XIoT, OT and IT Visibility and Cybersecurity

Versión	
Fabricante	Claroty Ltd
Familia	Detección y respuesta de amenazas en red (NDR)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	30/06/2026
Revisión de Validez	30/11/2026

Descripción

Claroty xDome es una plataforma modular de ciberseguridad para entornos CPS (Cyber Physical Systems) que se adapta para proteger su entorno y cumplir sus objetivos a medida que estos evolucionan. Claroty xDome extiende los controles esenciales de ciberseguridad a múltiples casos de uso en su trayectoria de ciberseguridad CPS (OT, XIoT, IoMT, IT, BMS, etc) y está diseñada para ofrecer flexibilidad y facilidad de uso, integrándose a la perfección con su infraestructura tecnológica existente. Con la base fundamental de un descubrimiento preciso, exhaustivo y completo del entorno, xDome ofrece funciones esenciales para una amplia gama de casos de uso, incluyendo la gestión de activos, gestión de vulnerabilidades y riesgos, gestión de la superficie de ataque, protección de la red, detección de amenazas y gestión de cambios. Además del valor fundamental de inventariado y monitorización que proporciona xDome, las capacidades de la plataforma cubren también casos de uso relacionados con la Gestión de Exposición, Detección de Amenazas, Gestión de Seguridad de Red y Eficiencia Operacional para cualquier dispositivo conectado en el entorno del cliente.

Observaciones

Procedimiento de Empleo Seguro pendiente de Publicación.

INFORMACIÓN IMPORTANTE

Vision Series Network Packet Broker

Versión	5.7.1
Fabricante	Keysight
Familia	Detección y respuesta de amenazas en red (NDR)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	24/11/2025
Revisión de Validez	30/04/2028

Descripción

Keysight proporciona una plataforma de Network Packet Broker orientada a proporcionar visibilidad, tratamiento y distribución del tráfico de red para su uso por herramientas de monitorización, análisis y ciberseguridad, permitiendo una visibilidad precisa y un comportamiento predecible, mediante la entrega de tráfico relevante, depurado y procesable. La solución puede integrarse en entornos físicos, virtualizados, híbridos y multicloud.

La plataforma ofrece visibilidad sobre flujos L2–L7, optimización del tráfico para herramientas conectadas, segmentación y control del acceso a los flujos, así como funciones de deduplicación, truncado, eliminación de cabeceras, generación de metadatos/NetFlow o desencriptado SSL/TLS. Asimismo, incorpora una compilación automática de reglas de filtrado, facilitando la gestión coherente de políticas en escenarios complejos. La plataforma se apoya en una arquitectura con recursos hardware especializados para mantener un procesamiento determinista del tráfico, incluso en situaciones de alta carga.

Observaciones

CCN-STIC 1248 PES Keysight Vision Packet Brokers

INFORMACIÓN IMPORTANTE

7.4.5 CASB

Microsoft Defender for Cloud Apps	
Versión	
Fabricante	Microsoft
Familia	CASB
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	10/12/2024
Revisión de Validez	30/11/2026

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

CCN-STIC 1239. Procedimiento de Empleo Seguro Microsoft Defender for Cloud Apps

INFORMACIÓN IMPORTANTE

7.5 PROTECCIÓN DE PERÍMETRO

7.5.1 ENRUTADORES

Ekinops One 2501	
Versión	OneOS6.12.x5patch01
Fabricante	Ekinops
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	11/07/2024
Revisión de Validez	31/12/2026
Descripción	

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

Observaciones

CCN-STIC 1470 Procedimiento de Empleo Seguro Ekinops One 2501

RUCKUS FastIron series ICX8100, ICX8100-X, ICX8200, ICX7550 e ICX7850 Switch/Router	
Versión	10.0.10h
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.
Series ICX8100 incluye: ICX8100-24, ICX8100-48, ICX8100-24P, ICX8100-48P, ICX8100-48PF, ICX8100-C08PF, ICX8100-C16P.
Series ICX8100-X incluye: ICX8100-24-X, ICX8100-48-X, ICX8100-24P-X, ICX8100-48P-X, ICX8100-48PF-X, ICX8100-C08PF-X, ICX8100-C16P-X.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Ekinops One 2520

Versión	OneOS6.12.x5patch01
Fabricante	Ekinops
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	11/07/2024
Revisión de Validez	31/12/2026

Descripción

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

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

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	31/03/2027



Descripción

Equipos diseñados para utilizarse en labores de acceso y agregación, o nucleo 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 exiten 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 son gestionables, tanto localmente (gestión on-premise) como pueden llegar a administrarse en modalidad Software-as-a-Service

Observaciones

CCN-STIC 1480 PES ArubaOS-Switch 16

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
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	16/06/2028
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

QFX Series (QFX5700)	
Versión	Junos OS 23.4R2-S2-EVO
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/06/2025
Revisión de Validez	30/11/2027
Descripción	

La línea QFX5700 que incluye el QFX5700 y QFX5700E admite funciones avanzadas de Capa 2, Capa 3 y EVPN-VXLAN. La plataforma está diseñada para su uso en centros de datos, campus, interconexión de centros de datos (DCI) y conexión de clústeres de firewall. La elección de velocidad de interfaz para la conectividad de servidores o dentro de un solución de fabric permite versatilidad en el despliegue y protección de la inversión.
Los proveedores de nube pública y de servicios que buscan satisfacer el crecimiento explosivo obtienen soporte de puertos 400GbE a escala de Internet. Para los clientes empresariales que están haciendo la transición de sus granjas de servidores de 10GbE a 25GbE, el QFX5700 proporciona la opción de ser usado como spine para arquitectura EVPN-VXLAN de 100GbE/400GbE con bajo consumo de energía en un espacio reducido. Con hasta 25.6 Tbps de rendimiento bidireccional, el switch está optimizado para despliegues de leaf & spine en centros de datos empresariales, computación de alto rendimiento, proveedores de servicios o en la nube.

Observaciones

CCN-STIC-1440 Procedimiento de Empleo Seguro Juniper QFX Series

INFORMACIÓN IMPORTANTE

MX Series (204, 304, 10003)	
Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027
Descripción	

Las plataformas de enrutamiento universal MX204, MX304 y 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 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. 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.

Observaciones

CCN-STIC-1456 Procedimiento de Empleo Seguro Juniper Routers MX Series

Huawei AR6000&AR600 Series Routers (NetEngine AR6120, NetEngine AR6121,NetEngine AR6140-9G-2AC, NetEngine AR6140-16G-4XG. NetEngine AR6280, NetEngine AR6300, NetEngine AR651, NetEngine AR651C, NetEngine AR651W, NetEngine AR657W, NetEngine AR611W y NetEngine AR617VW-LTE4EA)	
Versión	V300R019C11SPC200 + Patch V300R019C11HP0095T
Fabricante	Huawei Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	09/08/2027
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-1437 Procedimiento de empleo seguro Enrutadores Huawei AR6000&AR600

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	30/11/2026
Descripción	

Los Catalyst Industrial Ethernet 9300 Rugged Series Switches son equipos diseñado 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

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
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	16/07/2027
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

INFORMACIÓN IMPORTANTE

EX 4400 Series (4400-24T|24P|24MP|48T|48P|48F|48MP)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

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, asi 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

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

INFORMACIÓN IMPORTANTE

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	TELDAT
Familia	Enrutadores
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	20/08/2024
Revisión de Validez	31/01/2027

Descripción

Familia de routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones

Observaciones

CCN-STIC 1471 Procedimiento de Empleo Seguro Teldat Routers

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.

INFORMACIÓN IMPORTANTE

MX Series (240, 480, 960) con tarjetas MPC10E y MX-SPC3

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

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

CCN-STIC-1456 Procedimiento de Empleo Seguro Juniper Routers MX Series

EX 9200 Series (9204, 9208, 9214) con tarjetas EX9200-15C

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las 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 de las funcionalidades de seguridad. Como switch de nivel 2 en la capa OSI, realiza un análisis de los 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 trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

INFORMACIÓN IMPORTANTE

EX3400 Series (3400-24T|24P|48T|48P)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las 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 de las funcionalidades de seguridad. Como switch de nivel 2 en la capa OSI, realiza un análisis de los 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 trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

INFORMACIÓN IMPORTANTE

QFX Series (5120-48YM|48T|48Y|32C, 5200-48Y|32C, 5210-64C) y EX4650-48Y

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

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 Procedimiento de Empleo Seguro Juniper QFX Series

INFORMACIÓN IMPORTANTE

QFX Series (QFX5700)

Versión	Junos OS 24.4R1-EVO
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

Descripción

La línea QFX5700 que incluye el QFX5700 y QFX5700E admite funciones avanzadas de Capa 2, Capa 3 y EVPN-VXLAN. La plataforma está diseñada para su uso en centros de datos, campus, interconexión de centros de datos (DCI) y conexión de clústeres de firewall. La elección de velocidad de interfaz para la conectividad de servidores o dentro de un solución de fabric permite versatilidad en el despliegue y protección de la inversión.
Los proveedores de nube pública y de servicios que buscan satisfacer el crecimiento explosivo obtienen soporte de puertos 400GbE a escala de Internet. Para los clientes empresariales que están haciendo la transición de sus granjas de servidores de 10GbE a 25GbE, el QFX5700 proporciona la opción de ser usado como spine para arquitectura EVPN-VXLAN de 100GbE/400GbE con bajo consumo de energía en un espacio reducido. Con hasta 25.6 Tbps de rendimiento bidireccional, el switch está optimizado para despliegues de leaf & spine en centros de datos empresariales, computación de alto rendimiento, proveedores de servicios o en la nube.

Observaciones

CCN-STIC-1440 Procedimiento de Empleo Seguro Juniper QFX Series

Adtran FSP3000R7 Network Element (SH1HU, SH7HU, SH9HU)

Versión	22.5.2
Fabricante	Adtran
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2025
Revisión de Validez	30/06/2027

Descripción

Adtran FSP 3000 es una plataforma de transporte óptico abierta, flexible y escalable, basada en tecnología de multiplexación por división de longitud de onda (WDM).
La plataforma proporciona soluciones para distintos tipos de servicios y aplicaciones, abarcando desde la interconexión de centros de datos (DCI) hasta infraestructuras de operadores en distintos segmentos de red, incluyendo redes metropolitanas y de larga distancia.
El FSP 3000 dispone de diversas variantes de chasis modulares que se adaptan a diferentes requisitos de espacio y capacidad. Sus tarjetas insertables soportan una amplia gama de módulos ópticos enchufables, con capacidades desde 1 Gbit/s hasta 800 Gbit/s con múltiples protocolos de cliente.

Observaciones

CCN-STIC 1013 Procedimiento de Empleo Seguro Adtran FSP3000R7 Network Element

INFORMACIÓN IMPORTANTE

EX4100 Series (4100-24P|24T|24MP|48P|48T|48MP|F-12P|F-24P|F-48P|F-12T|F-24T|F-48T)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

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, reenvia 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

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

INFORMACIÓN IMPORTANTE

EX2300 Series (EX2300-C-12T|12P|24T|24P|48T|48P|24MP|48MP)	
Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las 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 de las funcionalidades de seguridad. Como switch de nivel 2 en la capa OSI, realiza un análisis de los 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 trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

INFORMACIÓN IMPORTANTE

Huawei NetEngine AR AR5000, AR6000 and AR8000 Series

Versión	V600R023C00SPC100
Fabricante	Huawei Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2024
Revisión de Validez	26/04/2028

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.

AR5000 Series(
NetEngine AR5710-H8T2TS1
NetEngine AR5710-S10T1X2
NetEngine AR5710-S8P2X
NetEngine AR5710-S8T2X
NetEngine AR5710-S8T2XE
NetEngine AR5710-S8T2X-LTE4EA
NetEngine AR5710-H8T2TS1-T
NetEngine AR5710-S8T2XE-LTE4EA-T)

AR6000 Series(
NetEngine AR6710-L8T3TS1X2
NetEngine AR6710-L26T2X4
NetEngine AR6710-L50T2X4
NetEngine AR6710-L26T2X4-T
NetEngine AR6710-L50T2X4-T
NetEngine AR6710-L8T3TS1X2-T
NetEngine AR6710-H4T4X2Y7
NetEngine AR6710-L14T2X4)

AR8000 Series(
NetEngine AR8140-12G10XG
NetEngine AR8140-T-12G10XG
NetEngine AR8700-8)

Observaciones

CCN-STIC 1452 Huawei NetEngine AR6700&AR8000

INFORMACIÓN IMPORTANTE

SDE-1X Series

Versión	OSDx v4.2.1.3
Fabricante	TELDAT
Familia	Enrutadores
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2028

Descripción

Familia de edge-routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones.

Observaciones

CCN-STIC 1484 Procedimiento de Empleo Seguro Teldat SDE-1x Series y SDE-2x Series

HPE Aruba Networking CX 4100i, 6000, 6100, 6200, 6300, 6400, 8100, 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	30/11/2027



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

CCN-STIC 1432 Procedimiento de Empleo Seguro Aruba CX Series

INFORMACIÓN IMPORTANTE

ACX Series (5448, 5448-M, 5448-D)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

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 Procedimiento de Empleo Seguro ACX Routers

INFORMACIÓN IMPORTANTE

RS SEries, M2 Series, M10 Series, Atlas-840 Series, Ares-C640 Series	
Versión	OSDx v4.2.1.3
Fabricante	TELDAT
Familia	Enrutadores
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	30/06/2026
Revisión de Validez	30/11/2026

Descripción

Familia de routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones.

Observaciones

Procedimiento de Empleo pendiente de publicación.

Atlas-840, M10-Smart Series, M2 Series, 4GePlus Series, Teldat-5Ge Series, 5Ge-Rail Series, Connect-4GePlus Series, Connect-5Ge Series, Connect-FW Series, Regesta SmartV2 Series, H5 Rail Series	
Versión	11.02.04.85.02
Fabricante	TELDAT
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	23/09/2025
Revisión de Validez	29/02/2028

Descripción

Familia de routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones

Observaciones

CCN-STIC 1471 Procedimiento de Empleo Seguro Teldat Router

INFORMACIÓN IMPORTANTE

SDE-2X Series	
Versión	OSDx v4.2.1.3
Fabricante	TELDAT
Familia	Enrutadores
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2028

Descripción

Familia de edge-routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones.

Observaciones

CCN-STIC 1484 Procedimiento de Empleo Seguro Teldat SDE-1x Series y SDE-2x Series

Huawei S Series Ethernet Switches S5732 (H24S6Q, H24UM2CC, H48S6Q, H48UM2CC, H48XUM2CC, H24S6Q-K, H24UM2C-K, H48S6Q-K, H48UM2C-K)	
Versión	V200R022C00SPC500
Fabricante	Huawei Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	16/06/2028

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

HPE Aruba Networking Orchestrator and EdgeConnect Release

Versión	9.4.2
Fabricante	HPE Aruba Networking
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/04/2025
Revisión de Validez	31/10/2026

Descripción

Los productos incluidos en esta cualificación son los pertenecientes a las familias EC-101XX, EC-S-P y EC-M-H.
La solución EdgeConnect SD-WAN de HPE Aruba Networking permite desplegar redes SD-WAN seguras de cualquier tamaño, tanto locales como internacionales mediante el uso de diversas topologías como hub&spoke, mesh o regionales. La solución SD-WAN permite construir múltiples overlays con políticas diferenciadas de gestión de los enlaces y topologías específicas dependiendo del tipo de tráfico. EdgeConnect permite una gestión de enlaces muy avanzada que incluye balanceo por paquete y dynamic path control lo que permite ofrecer al usuario conexiones agregadas de alta capacidad y calidad incluso utilizando enlaces degradados. La solución EdgeConnect introduce múltiples funcionalidades de seguridad como VRFs, statefull firewall con zonas e IDS/IPS. La solución SD-WAN de Aruba ofrece funcionalidades de optimización WAN mediante aceleración de protocolo TCP y reducción de datos mediante compresión y deduplicación. EdgeConnect SD-WAN permite la integración con múltiples proveedores de seguridad SSE lo que permite, mediante el uso de políticas específicas, derivar el tráfico a los diferentes proveedores de seguridad

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

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
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	16/06/2028

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
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	16/06/2028

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 S5736 (S24UM4XC, S48S4X-A, S24S4XC, S24T4XC, S24U4XC, S48S4XC, S48S4X-D, S48T4XC, S48U4XC)	
Versión	V200R022C00SPC500
Fabricante	Huawei Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	16/06/2028
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 S6735 (S6735-S24X6C y S6735-S48X6C) y S12700 (S12700E-4, S12700E-8 y S12700E-12)	
Versión	V200R022C00SPC500
Fabricante	Huawei Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	16/06/2028
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 S6730 (H24X6C, H48X6C, S24X6Q, H24X4Y4C, H24X6C-K, H28Y4C, H28Y4C-K, H48X6C-K) y S6730S (H24X6C-A, S24X6C-A)	
Versión	V200R022C00SPC500
Fabricante	Huawei Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	16/06/2028
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

Cisco Routers IOS-XE 17.12

Versión	IOS-XE 17.12
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/09/2024
Revisión de Validez	30/09/2027

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.

Modelos:
Cisco Embedded Services Router Series 6300: ESR-6300-NCP-K9, ESR-6300-CON-K9
Catalyst 8200 series: C8200-1N-4T, C8200L-1N-4T;
Catalyst 8500 series: C8500L-8S4X;
Cisco Catalyst 8000V Edge: C8000V Edge;
Cisco 1000 Series
Integrated Services Routers (ISR1000): C1161(X)-8P, C1161(X)-8PLTEP, C1131(X)-8PW, C1131(X)-8PLTEPW, C1121-4P, C1121-4PLTEP, C1121(X)-8P, C1121(X)-8PLTEP, C1121(X)-8PLTEPW, C1126(X)-8PLTEP, C1127(X)-8P(M)LTEP, C1128-8PLTEP, C1111-4P, C1111-4PLTEEA/LA, C1111-4PW, C1116-4P, C1116- 4PWE, C1116-4PLTEEA, C1116-4PLTEEAWE, C1117-4P(M), C1117-4P(M)W, C1117-4P(M)LTEEA/LA, C1117-4P(M)LTEEA/LAW, C1101-4P, C1101-4PLTEP, C1101-4PLTEPW;
Cisco Catalyst 1800 Rugged Series (IR1800): IR1821-K9, IR1831-K9, IR1833-K9, IR1835-K9;
Cisco Catalyst 8300 Rugged Series (IR8300): IR8340-K9;
Cisco ASR 1000 Series: ASR1001-X, ASR1001-HX, ASR1002-HX, ASR1006-X, ASR1009-X, ASR1013, ASR1000-MIP100, Ethernet Port Adapters: EPA-18X1GE, EPA10X10GE, EPA-QSFP-1X100GE, EPA-CPAK-2X40GE, EPA-2X40GE, EPA-1X40GE
Cisco ISR 4000 Series: ISR4321, ISR4331, ISR4351, ISR4431, ISR4451-X, ISR4461.
Network Interface Modules (NIM): NIM-1GE-CU-SFP, NIM-2GE-CU-SFP.

Observaciones

CCN-STIC 1465 Procedimiento de Empleo Seguro Cisco Routers IOS-XE

INFORMACIÓN IMPORTANTE

NE40E 8000 Series Routers running VRP software	
Versión	V800R012C00SPC300
Fabricante	Huawei Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	30/12/2027

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

VoyagerVM 4.0	
Versión	KlasOS Keel 5.4.3
Fabricante	Klas
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	23/09/2025
Revisión de Validez	29/02/2028

Descripción

VoyagerVM 4.0 es un servidor rugerizado y diseñado para operar en las condiciones más extremas. Integra un procesador Intel Xeon D de 10ª Generación con TPM2.0 y arranque seguro. Todos los discos del sistema son NVMe y además son discos con capacidades de auto-cifrado (TCG Opal 2.0). Además, el servidor incluye múltiples tarjetas de red de Intel: 4x 25Gbps (SFP28), 2x 2.5Gbps (RJ45) y tarjeta de red dedicada para gestión fuera de banda del servidor a 1Gbps (RJ45). El servidor cuenta también con un puerto de expansión para conectar otros periféricos como una GPU o almacenamiento adicional. Su sistema operativo Keel incluye funcionalidades de enrutamiento, cortafuegos, SD-WAN y virtualización. Esto permite securizar el acceso a todo tipo de redes usando el cortafuegos integrado o virtualizando otra solución de terceros.

Observaciones

CCN-STIC 1479 Procedimiento de Empleo Seguro VoyagerVM 4.0

INFORMACIÓN IMPORTANTE

Klas TRX R2

Versión	KlasOS Keel 5.4.0
Fabricante	Klas
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	23/07/2025
Revisión de Validez	31/12/2027

Descripción

TRX R2 es un enrutador rugerizado y diseñado para operar en las condiciones más extremas. Tiene capacidad de conexión a múltiples redes WAN incluyendo: redes móviles, WiFi y redes fijas a 1G/10G. Su sistema operativo KlasOS Keel incluye funcionalidades de enrutamiento, cortafuegos, SD-WAN, GPS y virtualización. Esto permite securizar el acceso a todo tipo de redes usando el cortafuegos integrado o virtualizando otra solución de terceros.

Observaciones

CCN-STIC 1478 Procedimiento de Empleo Seguro Klas TRX R2

INFORMACIÓN IMPORTANTE

Nokia 7750 Series (7750 SR-1 (FP4), 7750 SR-1s, 7750 SR-2s, 7750 SR-7s/14s (CPM & CPM-s v2), 7750 SR-7/12/12e/ESS (CPM5), 7750 SR-1x, 7750 SR-1 (FP5), 7750 SR-1se, 7750 SR-2se))	
Versión	SR OS v24.10
Fabricante	NOKIA
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	03/11/2025
Revisión de Validez	30/04/2028

Descripción

La familia de enrutadores de servicio 7750 SR de Nokia proporciona soluciones IP/MPLS de alto rendimiento diseñadas para proveedores de servicios y grandes empresas. Esta familia se beneficia de las ventajas que aporta la tecnología de última generación de microchips de silicio FP5/FP4 de Nokia, permitiendo la creación de una amplia gama de servicios IP con requisitos excepcionales de rendimiento, escalabilidad e inteligencia en el 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. Ofrece un conjunto completo de capacidades de seguridad en las múltiples capas de la red incluyendo:
Seguridad a nivel de red: listas de control de acceso (ACL), filtrado granular del tráfico basado en direcciones IP, puertos, protocolos y más parámetros.
Protección del plano de control (CoPP): protege el plano de control del enrutador de ataques DDoS y tráfico excesivo.
MACsec (IEEE 802.1AE): proporciona cifrado de capa 2 para enlaces Ethernet, lo que garantiza la confidencialidad y la integridad de estos.
Seguridad de nivel de servicio; VPN IPsec: admite VPN seguras con cifrado y autenticación.
Filtros de servicio: se aplican por servicio para controlar la entrada y salida del tráfico, lo que mejora el aislamiento de los abonados al servicio.
Seguridad del protocolo de enrutamiento: autenticación para este tipo de protocolos OSPF, BGP, IS-IS y otros que admiten la autenticación MD5/SHA para evitar la suplantación de identidad.
Monitoreo y detección de amenazas: detección y mitigación de DDoS integrada apoyándose en FlowSpec.
NetFlow/IPFIX: proporciona visibilidad detallada del tráfico para su análisis y la detección de anomalías.
Syslog y SNMPv3: registro y monitoreo seguros con cifrado y autenticación.
Seguridad de la plataforma y el sistema operativo: arranque seguro y firma de imágenes, garantizando que solo se ejecute software confiable en la plataforma.
SSH y HTTPS: interfaces de administración seguras para evitar el acceso no autorizado.

Observaciones

CCN-STIC 1457 PES Enrutadores NOKIA SR y IXR 2026

INFORMACIÓN IMPORTANTE

RouterTeldat-M1 Series

Versión	11.01.09
Fabricante	TELDAT
Familia	Enrutadores
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2023
Revisión de Validez	03/05/2028

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

SRX Series (300, 320, 340, 345, 345-DUAL-AC, 380, 1500, 1600, 2300, 4100, 4200, 4300, 4600, 5400, 5600, 5800)	
Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

Descripción

La familia de firewall mid-range de Juniper Networks® 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 Procedimiento de Empleo Seguro Juniper SRX Series

INFORMACIÓN IMPORTANTE

Juniper PTX10000 Series (PTX10004, PTX10016, PTX10001-36MR, PTX10002-36QDD)

Versión	JunOs 23.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2025
Revisión de Validez	29/02/2028

Descripción

La familia de routers PTX10k de HPE Juniper Networking está diseñada para ofrecer un rendimiento extremo en redes IP/MPLS de alto rendimiento, combinando capacidades avanzadas de routing y switching con sólidas funciones de seguridad integradas. Basados en la arquitectura de ASIC Express, proporcionan alta capacidad de conmutación, baja latencia y alta eficiencia energética, ideales para operadores y grandes proveedores de servicios. La familia PTX incorporan protección a nivel de infraestructura, mitigación de ataques DDoS y telemetría en tiempo real para detectar anomalías. Sus funcionalidades de segmentación de red en capa L2 y L3 basadas en estándares de la industria, el control del plano de routing y la compatibilidad con protocolos como MP-BGP, IS-IS, MPLS y SRv6 garantizan un enrutamiento basado en estándares, fiable, seguro y escalable en entornos redes WAN y centros de datos de misión crítica.

Observaciones

Pendiente PES

INFORMACIÓN IMPORTANTE

Juniper MX Series (10004, 10008, 10016)

Versión	JunOS 23.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2025
Revisión de Validez	29/02/2028

Descripción

Las plataformas de enrutamiento universal MX10000, compuestas por el MX10003, MX10004, MX10008, MX10016, 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 MX es altamente escalable desde desde los 2.4Tbps en 3U, pasando por 38,4 Tbps en 7 slots hasta un rendimiento de 76,8 Tbps en 13 slots.

Observaciones

INFORMACIÓN IMPORTANTE

Cisco Aggregation Services Router 9000(ASR9K)

Versión	IOS-XR 7.11
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	28/02/2025
Revisión de Validez	31/07/2027

Descripción

Los routers Cisco Aggregation Services Router 9000 (ASR9K) ejecutando IOS-XR 7.11 están diseñados para ofrece rendimiento y escalabilidad en redes de proveedores de servicios y grandes empresas.
Soportan configuraciones modulares con opciones de alta densidad de puertos, incluyendo 1/10/40/100 Gigabit Ethernet, y están equipados con procesadores de alto rendimiento para garantizar un procesamiento eficiente del tráfico.
IOS-XR 7.11 proporciona una plataforma de software robusta y escalable, con soporte para múltiples protocolos de enrutamiento y conmutación. Incluye capacidades avanzadas de automatización y programabilidad, como modelado de datos YANG, NETCONF y APIs REST, facilitando la integración con herramientas de gestión y orquestación de redes.
En términos de seguridad, estos routers ofrecen características avanzadas como autenticación multifactor, control de acceso basado en roles (RBAC) y cifrado de datos en tránsito. Soportan telemetría en tiempo real, permitiendo la monitorización continua del rendimiento y la detección proactiva de problemas.
Diseñados para entornos críticos, los routers ASR9K soportan características de alta disponibilidad como ISSU (In-Service Software Upgrade), redundancia de hardware y conmutación por error rápida.
Compatibles con tecnologías de redes definidas por software (SDN), proporcionan una solución completa que simplifica la gestión de la red y mejora la agilidad operativa.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Nokia 7250 IXR Series (7250 IXR-R4, 7250 IXR-R6, 7250 IXR-R6d/dl, 7250 IXR-e (Small)

Versión	SR OS v24.10
Fabricante	NOKIA
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	03/11/2025
Revisión de Validez	30/04/2028

Descripción

La familia 7250 IXR de Nokia incluye enrutadores de servicio de alto rendimiento disponibles para proveedores de servicio y empresas de todo tipo. Esta dispone tanto de enrutadores con chasis compacto y modular como con monoprocesador, compartiendo ambos la robustez del sistema operativo “Service Router (SR OS)” de Nokia .

Algunos de los escenarios típicos de su implementación son: agregación de borde metropolitano, consolidación de múltiples enlaces de capa de acceso (por ejemplo, 10/40 Gb) en redes troncales de alta capacidad (100/400 Gb), conectividad de baja latencia y alto rendimiento para “Fronthaul y Backhaul”, interconexión de centros de datos (DCI) dispersos geográficamente con interfaces ópticas de alta capacidad , Enterprise WAN y transporte 5G,

Esta familia de enrutadores combina el cifrado acelerado por hardware (MACsec) con sólidos mecanismos de control de acceso como la autenticación usuarios vía SSH para la administración de los enrutadores, asegurando el acceso restringido a estos. Además proporciona una protección integrada del plano de control frente a ataques DDoS, ayudando a mantener la disponibilidad del servicio incluso bajo este tipo de ataques. Entre sus funcionalidades se encuentran el registro integral, el arranque seguro , la firma de firmware , las listas de control de acceso (ACL) y el filtrado granular del tráfico basado en direcciones IP, puertos y protocolos , todo esto proporciona una base sólida para los requisitos des seguridad y auditoría.

Observaciones

CCN-STIC 1457 PES Enrutadores NOKIA SR y IXR 2026

INFORMACIÓN IMPORTANTE

7.5.2 SWITCHES

RUCKUS FastIron series ICX8100, ICX8100-X, ICX8200, ICX7550 e ICX7850 Switch/Router	
Versión	10.0.10h
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.
Series ICX8100 incluye: ICX8100-24, ICX8100-48, ICX8100-24P, ICX8100-48P, ICX8100-48PF, ICX8100-C08PF, ICX8100-C16P.
Series ICX8100-X incluye: ICX8100-24-X, ICX8100-48-X, ICX8100-24P-X, ICX8100-48P-X, ICX8100-48PF-X, ICX8100-C08PF-X, ICX8100-C16P-X.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Switches IOS-XE 17.12 - 9400 Series

Versión	IOS-XE 17.12.02
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/11/2024
Revisión de Validez	30/04/2027

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.
Modelos:
Chassis:
C9404R, C9407R, C9410R.
Supervisors:
C9400X-SUP-2, C9400X-SUP-2XL, C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y.
Line cards:
C9400-LC-48HX,C9400-LC-48XS, C9400X-LC-48HN, C9400-LC-24XY, C9400-LC-12QC, C9400-LC-24S, C9400-LC-48S, C9400-LC-24XS, C9400-LC-48P, C9400-LC-48T, C9400-LC-48U, C9400-LC-48UX, C9400-LC-48H.

Observaciones

CCN-STIC 1012 Procedimiento de Empleo Seguro Cisco Switches IOS-XE

INFORMACIÓN IMPORTANTE

Cisco Switches IOS-XE 17.12 - 9500 Series

Versión	IOS-XE 17.12.02
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/11/2024
Revisión de Validez	30/04/2027

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.
Modelos:
C9500X-28C8D, C9500X-60L4D, C9500-16X, C9500-32C, C9500-32QC, C9500-24Y4C, C9500-48Y4C.
Network modules:
C9500-NM-8X, C9500-NM-2Q.

Observaciones

CCN-STIC 1012 Procedimiento de Empleo Seguro Cisco Switches IOS-XE

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

Versión	IOS-XE 17.12
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	03/12/2024
Revisión de Validez	31/05/2027

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

CCN-STIC 1012 Procedimiento de Empleo Seguro Cisco Switches IOS-XE

INFORMACIÓN IMPORTANTE

Cisco Switches IOS-XE 17.12 - 9600 Series

Versión	IOS-XE 17.12.02
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/11/2024
Revisión de Validez	30/04/2027

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.
Modelos:
Chassis:
C9606R.
Supervisors:
C9600-SUP-1, C9600X-SUP2.
Line cards;
C9600-LC-40YL4CD, C9600X-LC-32CD, C9600-LC-24C, C9600-LC-48YL, C9600-LC-48TX.

Observaciones

CCN-STIC 1012 Procedimiento de Empleo Seguro Cisco Switches IOS-XE

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	31/03/2027

Descripción

Equipos diseñados para utilizarse en labores de acceso y agregación, o nucleo 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 exiten 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 son gestionables, tanto localmente (gestión on-premise) como pueden llegar a administrarse en modalidad Software-as-a-Service

Observaciones

CCN-STIC 1480 PES ArubaOS-Switch 16

Alcatel-Lucent Enterprise OS series: 6360, 6465, 6560, 6570, 6860, 6870, 6900, 9900.

Versión	AOS 8.10R04
Fabricante	ALE International
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	30/06/2026
Revisión de Validez	30/11/2026

Descripción

Familia de conmutadores L3+ compactos apilables, con alta densidad de puertos 1GE, Multigigabit ethernet 1/2.5/5/10 GigE y enlaces 10GE, 25GE, 100GE y 200GE, diseñada para redes convergentes, de alto rendimiento y seguridad reforzada. Maximiza el rendimiento de la red, garantiza la escalabilidad y mejora la conectividad de IoT con conmutadores de red de alta velocidad y baja latencia que están optimizados para WiFi 6/6E/7.

Gracias a su gran flexibilidad, se adaptan a cualquier tamaño de red, y cualquier entorno, incluidos los que demandan aspectos de seguridad más exigentes.

https://www.al-enterprise.com/es-es/productos/conmutadores

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

QFX Series (QFX5700)

Versión	Junos OS 23.4R2-S2-EVO
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/06/2025
Revisión de Validez	30/11/2027

Descripción

La línea QFX5700 que incluye el QFX5700 y QFX5700E admite funciones avanzadas de Capa 2, Capa 3 y EVPN-VXLAN. La plataforma está diseñada para su uso en centros de datos, campus, interconexión de centros de datos (DCI) y conexión de clústeres de firewall. La elección de velocidad de interfaz para la conectividad de servidores o dentro de un solución de fabric permite versatilidad en el despliegue y protección de la inversión.
Los proveedores de nube pública y de servicios que buscan satisfacer el crecimiento explosivo obtienen soporte de puertos 400GbE a escala de Internet. Para los clientes empresariales que están haciendo la transición de sus granjas de servidores de 10GbE a 25GbE, el QFX5700 proporciona la opción de ser usado como spine para arquitectura EVPN-VXLAN de 100GbE/400GbE con bajo consumo de energía en un espacio reducido. Con hasta 25.6 Tbps de rendimiento bidireccional, el switch está optimizado para despliegues de leaf & spine en centros de datos empresariales, computación de alto rendimiento, proveedores de servicios o en la nube.

Observaciones

CCN-STIC-1440 Procedimiento de Empleo Seguro Juniper QFX Series

INFORMACIÓN IMPORTANTE

MX Series (204, 304, 10003)	
Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

Descripción

Las plataformas de enrutamiento universal MX204, MX304 y 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 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. 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.

Observaciones

CCN-STIC-1456 Procedimiento de Empleo Seguro Juniper Routers MX Series

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	30/11/2026

Descripción

Los Catalyst Industrial Ethernet 9300 Rugged Series Switches son equipos diseñado 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

Fortiswitch

Versión	7.6
Fabricante	Fortinet
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/02/2026
Revisión de Validez	28/02/2029

Descripción

La gama de switches FortiSwitch ofrece conmutación segura de capa 2 y capa 3 integrada con FortiGate mediante FortiLink, permitiendo convertir la red Ethernet en una extensión directa del Security Fabric. Esto permite aplicar políticas de segmentación dinámica, control de acceso basado en 802.1X y visibilidad de dispositivos sin necesidad de licencias adicionales. Con soporte para PoE, redundancia y calidad de servicio (QoS) entre otras características, FortiSwitch está diseñado para entornos críticos como campus, SD-Branch y centros de datos. Su gestión centralizada a través de FortiGate o FortiManager simplifica la operación y mejora la visibilidad global del acceso a la red.

Observaciones

CCN-STIC 1482 Procedimiento de Empleo Seguro FortiSwitch v7.6

EX 4400 Series (4400-24T|24P|24MP|48T|48P|48F|48MP)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

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, asi 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

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

INFORMACIÓN IMPORTANTE

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	TELDAT
Familia	Switches
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	20/08/2024
Revisión de Validez	31/01/2027

Descripción

Familia de routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones

Observaciones

CCN-STIC 1471 Procedimiento de Empleo Seguro Teldat Routers

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

H3C IE4320 Series, IE4320-EI Series, IE4500-G Series and IE4520 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/08/2025
Revisión de Validez	30/11/2029

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.

Modelos:

IE4320 Series, H3C Comware Software Version 7.1.070 Release 6369

IE4320-28S-HPWR model

IE4320-EI Series, H3C Comware Software Version 7.1.070 Release 6815P03

IE4320-8T2P2X-PWR-EI model, IE4320-8T2P2X-EI model, IE4320-16T4X-EI model, IE4320-8T8P4X-EI model, IE4320-16T8TP4P model, IE4320-24T4X-EI model, IE4320-16T8TP4X-EI model, IE4320-16T8TP4X-HPWR-EI model, IE4320-12P4TP4X-C-EI model, IE4320-24T16P4X-EI model.

IE4500-G Series, H3C Comware Software Version 7.1.070 Release 8307P15

IE4500-14S-UPWR-G model, IE4500-14S-G model, IE4500-36S-C-UPWR-G model, IE4500-28S-G model, IE4500-28F-G model, IE4520-56S-C-G model.

IE4520 Series, H3C Comware Software Version 7.1.070 Release 6816

IE4520-30S-C model

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

INFORMACIÓN IMPORTANTE

MX Series (240, 480, 960) con tarjetas MPC10E y MX-SPC3

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

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

CCN-STIC-1456 Procedimiento de Empleo Seguro Juniper Routers MX Series

EX 9200 Series (9204, 9208, 9214) con tarjetas EX9200-15C

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las 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 de las funcionalidades de seguridad. Como switch de nivel 2 en la capa OSI, realiza un análisis de los 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 trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

INFORMACIÓN IMPORTANTE

EX3400 Series (3400-24T|24P|48T|48P)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las 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 de las funcionalidades de seguridad. Como switch de nivel 2 en la capa OSI, realiza un análisis de los 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 trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

INFORMACIÓN IMPORTANTE

QFX Series (5120-48YM|48T|48Y|32C, 5200-48Y|32C, 5210-64C) y EX4650-48Y

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

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 Procedimiento de Empleo Seguro Juniper QFX Series

INFORMACIÓN IMPORTANTE

QFX Series (QFX5700)

Versión	Junos OS 24.4R1-EVO
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

Descripción

La línea QFX5700 que incluye el QFX5700 y QFX5700E admite funciones avanzadas de Capa 2, Capa 3 y EVPN-VXLAN. La plataforma está diseñada para su uso en centros de datos, campus, interconexión de centros de datos (DCI) y conexión de clústeres de firewall. La elección de velocidad de interfaz para la conectividad de servidores o dentro de un solución de fabric permite versatilidad en el despliegue y protección de la inversión.
Los proveedores de nube pública y de servicios que buscan satisfacer el crecimiento explosivo obtienen soporte de puertos 400GbE a escala de Internet. Para los clientes empresariales que están haciendo la transición de sus granjas de servidores de 10GbE a 25GbE, el QFX5700 proporciona la opción de ser usado como spine para arquitectura EVPN-VXLAN de 100GbE/400GbE con bajo consumo de energía en un espacio reducido. Con hasta 25.6 Tbps de rendimiento bidireccional, el switch está optimizado para despliegues de leaf & spine en centros de datos empresariales, computación de alto rendimiento, proveedores de servicios o en la nube.

Observaciones

CCN-STIC-1440 Procedimiento de Empleo Seguro Juniper QFX Series

Adtran FSP3000R7 Network Element (SH1HU, SH7HU, SH9HU)

Versión	22.5.2
Fabricante	Adtran
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2025
Revisión de Validez	30/06/2027

Descripción

Adtran FSP 3000 es una plataforma de transporte óptico abierta, flexible y escalable, basada en tecnología de multiplexación por división de longitud de onda (WDM).
La plataforma proporciona soluciones para distintos tipos de servicios y aplicaciones, abarcando desde la interconexión de centros de datos (DCI) hasta infraestructuras de operadores en distintos segmentos de red, incluyendo redes metropolitanas y de larga distancia.
El FSP 3000 dispone de diversas variantes de chasis modulares que se adaptan a diferentes requisitos de espacio y capacidad. Sus tarjetas insertables soportan una amplia gama de módulos ópticos enchufables, con capacidades desde 1 Gbit/s hasta 800 Gbit/s con múltiples protocolos de cliente.

Observaciones

CCN-STIC 1013 Procedimiento de Empleo Seguro Adtran FSP3000R7 Network Element

INFORMACIÓN IMPORTANTE

EX4100 Series (4100-24P|24T|24MP|48P|48T|48MP|F-12P|F-24P|F-48P|F-12T|F-24T|F-48T)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

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, reenvia 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

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

INFORMACIÓN IMPORTANTE

EX2300 Series (EX2300-C-12T|12P|24T|24P|48T|48P|24MP|48MP)	
Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las 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 de las funcionalidades de seguridad. Como switch de nivel 2 en la capa OSI, realiza un análisis de los 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 trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

INFORMACIÓN IMPORTANTE

Cisco MDS 9000 Series Switches

Versión	NX-OS 9.4
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	13/05/2025
Revisión de Validez	30/11/2026

Descripción

Los switches Cisco MDS 9000 Series ejecutando NX-OS 9.4 ofrecen rendimiento y escalabilidad en entornos de almacenamiento en red (SAN). Estos switches
soportan configuraciones modulares y fijas, proporcionando opciones de alta densidad de puertos que incluyen 16/32/64-Gbps Fibre Channel, lo que garantiza
un rendimiento de línea en todos los puertos. NX-OS 9.4 proporciona una plataforma de software robusta y escalable con soporte para múltiples protocolos de almacenamiento y conmutación. Incluye capacidades avanzadas de automatización y programabilidad, como NX-API, Python, y soporte para Ansible
y Puppet, facilitando la integración con herramientas de gestión y orquestación de redes.
En términos de seguridad, estos switches ofrecen características avanzadas como autenticación multifactor, control de acceso basado en roles (RBAC) y cifrado de datos en tránsito. Además, soportan telemetría en tiempo real, permitiendo la monitorización continua del rendimiento y la detección proactiva de problemas. Diseñados para entornos críticos, soportan características de alta disponibilidad como ISSU (In-Service Software Upgrade), redundancia de hardware y conmutación por error rápida. Son compatibles con tecnologías de redes definidas por software (SDN) y proporcionan una solución completa que simplifica la gestión de la red y mejora en la agilidad operativa. Ideales para centros de datos que requieren alta densidad de puertos, rendimiento de línea, seguridad avanzada y capacidades de automatización y
telemetría.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

SDE-1X Series

Versión	OSDx v4.2.1.3
Fabricante	TELDAT
Familia	Switches
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2028

Descripción

Familia de edge-routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones.

Observaciones

CCN-STIC 1484 Procedimiento de Empleo Seguro Teldat SDE-1x Series y SDE-2x Series

HPE Aruba Networking CX 4100i, 6000, 6100, 6200, 6300, 6400, 8100, 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	30/11/2027



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

CCN-STIC 1432 Procedimiento de Empleo Seguro Aruba CX Series

INFORMACIÓN IMPORTANTE

H3C S5500 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/11/2029

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.
Modelos:

S5500 Series

- S5570S-28S-EI, S5570S-54S-EI, S5570S-54F-EI, S5570S-36F-EI ,S5570S-54S-PWR-EI-A, S5570S-28S-HPWR-EI-A, S5560X-30C-EI, S5560X-54C-EI, S5560X-30C-PWR-EI, S5560X-54C-PWR-EI, S5560X-30F-EI, S5560X-54F-EI, S5560X-34S-EI, S5560X-54S-EI, S5560X-30F-EIF, S5590-28T8XC-EI ,S5590-48T4XC-EI, S5590-28S8XC-EI, S5590-48S4XC-EI, S5590-28P8XC-EI, S5590-48P6XC-EI, S5590-48TS4X2QC-EI, S5590-24X4YC-EI, S5590-24UXM4YC-EI, S5590-48UXM4YC-EI, S5590-24UXMC-EI, S5590-32UN4X4Y2CC-EI, S5590-48UN4Y2CC-EI,, S5590-48UM4YC-EI.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

INFORMACIÓN IMPORTANTE

ACX Series (5448, 5448-M, 5448-D)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

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 Procedimiento de Empleo Seguro ACX Routers

INFORMACIÓN IMPORTANTE

RS SEries, M2 Series, M10 Series, Atlas-840 Series, Ares-C640 Series	
Versión	OSDx v4.2.1.3
Fabricante	TELDAT
Familia	Switches
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	30/06/2026
Revisión de Validez	30/11/2026

Descripción

Familia de routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones.

Observaciones

Procedimiento de Empleo pendiente de publicación.

Atlas-840, M10-Smart Series, M2 Series, 4GePlus Series, Teldat-5Ge Series, 5Ge-Rail Series, Connect-4GePlus Series, Connect-5Ge Series, Connect-FW Series, Regesta SmartV2 Series, H5 Rail Series	
Versión	11.02.04.85.02
Fabricante	TELDAT
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	23/09/2025
Revisión de Validez	29/02/2028

Descripción

Familia de routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones

Observaciones

CCN-STIC 1471 Procedimiento de Empleo Seguro Teldat Router

INFORMACIÓN IMPORTANTE

SDE-2X Series

Versión	OSDx v4.2.1.3
Fabricante	TELDAT
Familia	Switches
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2028

Descripción

Familia de edge-routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones.

Observaciones

CCN-STIC 1484 Procedimiento de Empleo Seguro Teldat SDE-1x Series y SDE-2x Series

INFORMACIÓN IMPORTANTE

H3C 7500 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/11/2029

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.
Modelos:

S7500 Series

- S7503X, S7503E-M, S7506X-POE, S7506X-S, S7510X-POE, S7503X-M-G, S7503X-G, S7506X-G-POE, S7510X-G-POE, S7506X-G, S7510X-G, S7506X-G-MF.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

INFORMACIÓN IMPORTANTE

H3C S5000 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2029

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.
Modelos:

S5000 Series

- S5000NV6-12T4N4NS-EI, S5000NV6-12P4UN4NS-EI, S5000NV6-20T4N4NS-EI, S5000NV6-20P4UN4NS-EI, S5000NV6-48T4NS-EI, S5000NV6-48P4NS-EI, S5000NV6-4T4N2NS-EI, S5000NV6-4P4UN2NS-EI.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

INFORMACIÓN IMPORTANTE

x930-52GPX, AT-SBx908Gen2, AT-x950, AT-x550, AT-x530, AT-530L, AT-x230, AT-x220, AT-x230-52, AT-IE340, AT-IE220 Switches and AlliedWare Plus	
Versión	5.5.4-1.8
Fabricante	Allied Telesis
Familia	Switches
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	09/06/2025
Revisión de Validez	30/11/2027

Descripción

Switches apilables Layer 3 con puertos Gigabit. Ofrecen flexibilidad, fiabilidad y alto rendimiento al estar orientados a soluciones de core y distribución de redes. Vienen con opciones de 24 y 48 puertos con uplinks de 10G y 40G. Son apilables hasta 8 unidades gracias a la tecnología Virtual Chassis Stacking (VCStack™) que permite crear pilas con equipos separados hasta 40 km. Están equipados con el sistema operativo AlliedWare Plus. Entre sus características más reseñables, destacan: • Soporte de AMF para gestión avanzada de redes convergentes • Protocolos para redes flexibles como EPSR, G.8032 o UDLD • Monitorización activa de fibra (AFM) • Análisis de tráfico sFlow • POE continuo • Layer 3: RIP, OSPF, BGP, VRF • Controlador wireless

Observaciones

CCN-STIC-1422 Procedimiento de empleo Seguro AlliedWare Plus (AW+) (PENDIENTE DE ACTUALIZACIÓN)

AT-XS916, AT-GS980MX, AT-GS980M, AT-GS970M, AT-x320, GS980EM, AT-x240, SE240, AT-x250, SE250, AT-x540L, SE540L Switches and AlliedWare Plus	
Versión	5.5.4-1.8
Fabricante	Allied Telesis
Familia	Switches
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	08/06/2025
Revisión de Validez	30/11/2027

Descripción

Switches apilables Layer 3 con puertos Gigabit. Ofrecen flexibilidad, fiabilidad y alto rendimiento al estar orientados a soluciones de core y distribución de redes. Vienen con opciones de 24 y 48 puertos con uplinks de 10G y 40G. Son apilables hasta 8 unidades gracias a la tecnología Virtual Chassis Stacking (VCStack™) que permite crear pilas con equipos separados hasta 40 km. Están equipados con el sistema operativo AlliedWare Plus. Entre sus características más reseñables, destacan: • Soporte de AMF para gestión avanzada de redes convergentes • Protocolos para redes flexibles como EPSR, G.8032 o UDLD • Monitorización activa de fibra (AFM) • Análisis de tráfico sFlow • POE continuo • Layer 3: RIP, OSPF, BGP, VRF • Controlador wireless

Observaciones

CCN-STIC-1422 Procedimiento de empleo Seguro AlliedWare Plus (AW+) (PENDIENTE DE ACTUALIZACIÓN)

INFORMACIÓN IMPORTANTE

RouterTeldat-M1 Series

Versión	11.01.09
Fabricante	TELDAT
Familia	Switches
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2023
Revisión de Validez	03/05/2028

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

Huawei CE Series Switches

Versión	V300R023C10SPC100
Fabricante	Huawei Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/08/2025
Revisión de Validez	31/01/2028

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.
Los modelos incluidos en esta Serie de productos son los siguientes: CE6866-48S8CQ-P, CE8851-32CQ8DQ-P, CE6860-HAM, CE8850-HAM, CE6860-SAN, CE8850-SAN, CE6881H-48S6CQ, CE6881H-48T6CQ, CE6820H-48S6CQ, CE6863H-48S6CQ, CE16804, CE16808, CE16816, CE6885-48YS8CQ, CE6885-48YS8CQ-T, CE5855-48T4XS, CE5855SL-48T4XS, CE5855SH-48T4XS, CE6855-48XS8CQ, CE6863E-48S8CQ, CE6885-LL-56F, CE6885-SAN-56F, CE8851-32CQ4BQ, CE8855-32CQ4BQ, CE16800-X4, CE16800-X8, CE16800-X16, CE8865-4C, CE8865-SAN-4C, CE8875-24BQ8DQ

Observaciones

CCN-STIC 1481 PES Huawei CE Series Switches

INFORMACIÓN IMPORTANTE

H3C 12500 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/11/2029

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.
Modelos:

S12500 Series

- S12504X-AF, S12508X-AF, S12516X-AF, S12504G-AF, S12508G-AF, S12516G-AF, S12504G-AF (Type S), S12508G-AF (Type S), S12516G-AF (Type S), S12504CR (Type S), S12508CR (Type S), S12516CR (Type S).

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

INFORMACIÓN IMPORTANTE

Juniper PTX10000 Series (PTX10004, PTX10016, PTX10001-36MR, PTX10002-36QDD)

Versión	JunOs 23.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2025
Revisión de Validez	29/02/2028

Descripción

La familia de routers PTX10k de HPE Juniper Networking está diseñada para ofrecer un rendimiento extremo en redes IP/MPLS de alto rendimiento, combinando capacidades avanzadas de routing y switching con sólidas funciones de seguridad integradas. Basados en la arquitectura de ASIC Express, proporcionan alta capacidad de conmutación, baja latencia y alta eficiencia energética, ideales para operadores y grandes proveedores de servicios. La familia PTX incorporan protección a nivel de infraestructura, mitigación de ataques DDoS y telemetría en tiempo real para detectar anomalías. Sus funcionalidades de segmentación de red en capa L2 y L3 basadas en estándares de la industria, el control del plano de routing y la compatibilidad con protocolos como MP-BGP, IS-IS, MPLS y SRv6 garantizan un enrutamiento basado en estándares, fiable, seguro y escalable en entornos redes WAN y centros de datos de misión crítica.

Observaciones

Pendiente PES

INFORMACIÓN IMPORTANTE

Juniper MX Series (10004, 10008, 10016)

Versión	JunOS 23.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2025
Revisión de Validez	29/02/2028

Descripción

Las plataformas de enrutamiento universal MX10000, compuestas por el MX10003, MX10004, MX10008, MX10016, 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 MX es altamente escalable desde desde los 2.4Tbps en 3U, pasando por 38,4 Tbps en 7 slots hasta un rendimiento de 76,8 Tbps en 13 slots.

Observaciones

INFORMACIÓN IMPORTANTE

Extreme Networks Fabric Engine Switches: U5320, U5420, U5520, U5720, U7520 y U7720

Versión	9.1.100
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2026
Revisión de Validez	28/02/2027

Descripción

Los switches Extreme Networks 5000 y 7000 con Fabric Engine 9.1.100 implementan una arquitectura de seguridad “Zero Trust” nativa centrada en el aislamiento estricto del plano de datos y la protección del plano de control. Como propiedades de seguridad más notables, indicamos las siguientes:
- Red Invisible: El núcleo de las red opera mediante encapsulamiento MAC-in-MAC (IEEE 802.1ah). Oculta todas las direcciones IP y los nodos intermedios no responden ni a comandos “traceroute” ni de escaneo de puertos.
- Hipersegmentación: Despliegue de Segmentos Virtuales aislados de extremo a extremo. Mitiga el movimiento lateral de amenazas entre dispositivos, sin la complejidad de VRFs tradicionales o túneles VXLAN.
- Cifrado Hardware (MACsec 802.1AE): Cifrado de alto rendimiento en los enlaces para preservar la confidencialidad e integridad del tráfico.
- Microsegmentación y Control de Acceso: Integración con NAC (802.1X/EAP-TLS). Asigna dinámicamente accesos a segmentos específicos según la identidad del dispositivo o aplicación, confinando el tráfico de IoT y cargas de trabajo.
- Protección del Plano de Control: Plano de control unificado mediante IS-IS, complementado con Control Plane Policing (CoPP) por hardware contra ataques DoS/DDoS.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Switches IOS-XE 17.12 - 9300 Series

Versión	IOS-XE 17.12.02
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/11/2024
Revisión de Validez	30/04/2027

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.
Modelos:
9300X series:
C9300X-48HX (con los módulos de red C9300X-NM-4C, C9300X-NM-8M, C9300X-NM-2C y C9300X-NM-8Y)
C9300X-48TX (con los módulos de red C9300X-NM-4C, C9300X-NM-8M, C9300X-NM-2C y C9300X-NM-8Y)
C9300X-12Y (con los módulos de red C9300X-NM-8M, C9300X-NM-2C y C9300X-NM-8Y)
C9300X-24Y (con los módulos de red C9300X-NM-4C, C9300X-NM-8M, C9300X-NM-2C y C9300X-NM-8Y)
C9300X-48HXN (con los módulos de red C9300X-NM-8M, C9300X-NM-2C y C9300X-NM-8Y)
C9300X-24HX (con los módulos de red C9300X-NM-8M, C9300X-NM-2C y C9300X-NM-8Y)
9300LM series:
C9300LM-24U, C9300LM-48UX, C9300LM-48T, C9300LM-48U.
Catalyst 9300 Series
C9300-48UXM, C9300-24T, C9300-24P, C9300-24U, C9300-24UX, C9300-24S, C9300-24UB, C9300-24UXB, C9300-24H, C9300-48T, C9300-48P, C9300-48U, C9300-48UN, C9300-48S, C9300-48UB, C9300-48H.
Network modules:
C9300-NM-4G, C9300-NM-8X, C9300-NM-2Q, C9300-NM-4M, C9300-NM-2Y, C9300LM-48U.
Catalyst 9300L Series
C9300L-24T-4X, C9300L-24P-4G, C9300L-48T-4X, C9300L-48P-4G, C9300L-24T-4G, C9300L-24P-4X, C9300L-48T-4G, C9300L-48P-4X, C9300L-48PF-4G, C9300L-48PF-4X, C9300L-24UXG-4X, C9300L-24UXG-2Q, C9300L-48UXG-4X, C9300L-48UXG-2Q.

Observaciones

CCN-STIC 1012 Procedimiento de Empleo Seguro Cisco Switches IOS-XE

INFORMACIÓN IMPORTANTE

H3C 10500 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/11/2029

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.
Modelos:

S10500 Series

-,S10506X, S10508X, S10510X, S10506X-G, S10508X-G, S10512X-G, S10506X-G-PoE, S10512X-G-PoE.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

INFORMACIÓN IMPORTANTE

H3C 6500 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/11/2029

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.
Modelos:

S6500 Series

- S6520X-18C-SI, S6520X-26C-SI, S6520X-26MC-UPWR-SI, S6520X-26MC-SI, S6520X-16ST-SI, S6520X-24ST-SI, S6520X-10XT-SI, S6520X-16XT-SI, S6520X-26XC-UPWR-SI, S6520X-54XC-UPWR-SI, S6520X-30HC-EI, S6520X-30QC-EI, S6520X-54HC-EI, S6520X-54QC-EI, S6520X-54HC-HI, S6520X-54QC-HI, S6520X-30HC-HI, S6520X-30QC-HI, S6520X-54HF-EI, S6520X-54HF-HI, S6520X-30HF-EI, S6520X-30HF-HI, S6520X-54HC-UPWR-EI, S6526XE-48X4CC-EI, S6526XE-32X4CC-EI, S6526XE-32X6CC-HI, S6526XE-48X6CC-HI.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

INFORMACIÓN IMPORTANTE

Cisco Switches IOS-XE 17.12 - Industrial Series Switches

Versión	IOS-XE 17.12.02
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/11/2024
Revisión de Validez	30/04/2027

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.
Modelos:
IE-3200-8T2S-E, IE-3200-8P2S-E, IE-3300-8T2S, IE-3300-8P2S, IE-3300-8T2X, IE-3300-8U2X, IE-3400-8T2S-E, IE-3400-8T2S-A, IE-3400-8P2S-E, IE-3400-8P2S-A, IE-3400H-8FT-E, IE-3400H-16FT-E, IE-3400H-24FT-E, IE-3400H-8T-E, IE-3400H-16T-E, IE-3400H-24T-E.

Observaciones

CCN-STIC 1012 Procedimiento de Empleo Seguro Cisco Switches IOS-XE

INFORMACIÓN IMPORTANTE

H3C 6800 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/11/2029

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.
Modelos:

S6800 Series

- S6890-54HF, S6890-30HF, S6890-44HF, S6825-54HF, S6805-54HF, S6805-54HT, S6850-56HF ,S6850-2C ,S6800-54HT, S6800-54HF, S6800-32Q-H1, S6800-2C-H1, S6800-4C-H1, S6800-54QF-H3, S6800-54QT-H3, S6800-54QF-H5, S6812-24X6C, S6812-48X6C, S6813-24X6C, S6813-48X6C, S6805-54HF-H1 , S6805-54HT-H1, S6850-56HF-H1, S6850-56HF-SAN.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

INFORMACIÓN IMPORTANTE

H3C 9800 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/11/2029

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.
Modelos:

S9800 Series

- S9820-8C, S9820-8C-SAN, S9850-32H, S9850-4C, S9850-32H-H1, S9850-4C-H1, S9820-64H, S9820-64H-H1, S9820-8M, S9850-32H-G.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

INFORMACIÓN IMPORTANTE

H3C S5100 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/11/2029

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.
Modelos:

S5100 Series

- S5130S-28T8X-EI-G-V2, ,S5130S-48T6X-EI-G-V2, S5130S-24UN8X-EI-G-V2, S5130S-48UN6X-EI-G-V2, S5136S-48P4S-EI, S5136S-8FP4XS-EI-Q, S5136S-24FP4T4S-EI, S5136S-48T4S-EI-Q, S5136S-24T4X-EI-Q, S5136S-48S2T4X-EI, S5136S-10T4X-EI-Q, S5136S-16FP4X-EI, S5136S-24P4X-EI, S5136S-48FP4X-EI, S5136S-48P4X-EI, S5136S-24T4S-EI-Q, S5136S-16T4X-EI-Q, S5136S-24S8T4X-EI, S5136S-48ST4X-EI, S5136S-48FP4S-EI, S5136S-24FP4S4X-EI, S5136S-8T4XS-EI-Q, S5136S-10FPT4X-EI-Q, S5136S-48T4X-EI-Q, S5130S-28S-HI, S5130S-52S-HI, S5130S-28S-PWR-HI, S5130S-52S-PWR-HI, S5130S-28C-HI, S5130S-52C-HI, S5130S-28C-PWR-HI, S5130S-52C-PWR-HI, S5130S-10P-EI, S5130S-12TP-EI, S5130S-20P-EI, S5130S-28P-EI, S5130S-52P-EI, S5130S-10P-HPWR-EI, S5130S-12TP-HPWR-EI, S5130S-20P-PWR-EI, S5130S-28P-PWR-EI, S5130S-28P-HPWR-EI, S5130S-52P-PWR-EI, S5130S-28S-EI, S5130S-52S-EI, S5130S-28F-EI, S5130S-52F-EI, S5130S-28TP-EI, S5130S-52TP-EI, S5130S-28S-PWR-EI, S5130S-28S-HPWR-EI, S5130S-52S-PWR-EI, S5170-28S-EI, S5170-54S-EI, S5170-54S-PWR-EI, S5170-28S-HPWR-EI.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

INFORMACIÓN IMPORTANTE

Cisco Nexus 9000 Series Switches

Versión	NX-OS 10.4
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	20/02/2025
Revisión de Validez	30/11/2026

Descripción

Los switches Cisco Nexus 9000 Series con NX-OS 10.4 ofrecen rendimiento y escalabilidad en centros de datos modernos. Soportan configuraciones modulares y fijas, con opciones de puertos de alta densidad que incluyen 1/10/25/40/100/400 Gigabit Ethernet. La arquitectura de backplane sin bloqueo garantiza un rendimiento de línea en todos los puertos.

NX-OS 10.4 proporciona una plataforma de software robusta y escalable con soporte para múltiples protocolos de enrutamiento y conmutación. Incluye capacidades avanzadas de automatización y programabilidad, como NX-API, Python, y soporte para Ansible y Puppet, facilitando la integración con herramientas de gestión y orquestación de redes.

En términos de seguridad, estos switches ofrecen autenticación multifactor, control de acceso basado en roles (RBAC) y cifrado de datos en tránsito. Además, soportan telemetría en tiempo real, permitiendo la monitorización continua del rendimiento y la detección proactiva de problemas.

Diseñados para entornos críticos, soportan características de alta disponibilidad como ISSU (In-Service Software Upgrade), redundancia de hardware y conmutación por error rápida. También son compatibles con Cisco ACI (Application Centric Infrastructure), proporcionando una solución SDN completa que simplifica la gestión de la red y mejora la agilidad operativa.

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	V600R024C10SPC500
Fabricante	Huawei Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2024
Revisión de Validez	31/12/2026
Descripción	





INFORMACIÓN IMPORTANTE

Los switches para campus de Huawei son ideales para crear redes de campus preparadas para el futuro con una gestión simplificada, alta fiabilidad e inteligencia de servicio, en sectores como el empresarial, gubernamental, educativo, financiero y manufacturero.
Los modelos cualificados son:
S3700 Series (S3710-H24P4S-A, S3710-H24T4S-A, S3710-H48LP4S-A, S3710-H48T4S-A), S5700 Series (S5731I-L8T2SN, S5731I-L8T2S2XN, S5731I-L8P2S2XN, S5731I-L16T2S2XN, S5732-H24S4X6QZ-TV2, S5732-H24S4X6QZ-V2, S5732-H24UM4Y2CZ-TV2, S5732-H24UM4Y2CZ-V2, S5732-H44S4X6QZ-TV2, S5732-H44S4X6QZ-V2, S5732-H48UM4Y2CZ-TV2, S5732-H48UM4Y2CZ-V2, S5732-H48XUM2CC, S5755E-H24HB2Y2CZ, S5735E-L8T4X-QA-V2, S5735E-L8P4X-QA-V2, S5735E-L16LP2X-QA-V2, S5735E-L16LP2UM2X-QA-V2, S5735E-L24P4S-A-V2, S5735E-L48LP4S-A-V2, S5735E-L24T4XE-A-V2, S5735E-L24P4XE-A-V2, S5735E-L48T4XE-A-V2, S5735E-L48LP4XE-A-V2, S5735E-L24ST4XE-A-V2, S5735E-L48S4XE-A-V2, S5735E-S24HS4XE-V2, S5735E-S48HS4XE-V2, S5735I-H24U8S4XE-QA-V2, S5735I-H8T4S2XN-V2, S5735I-L10T4X-A-V2, S5735I-L8P4X-A-V2, S5735I-S16T8S4XE-QD-V2, S5735I-S24T4XE-V2, S5735I-S24T8S4XE-QA-V2, S5735I-S24U4XE-V2, S5735I-S8T4SN-V2, S5735I-S8T4XN-V2, S5735I-S8U4XN-V2, S5735I-S8T4XN-T-V2, S5735I-S8T8P2S4XN-V2, S5735I-S8U2XN-V2, S5735I-S16T2S4XN-V2, S5735I-S24T4XE-T-V2, S5735I-S24U4XE-T-V2, S5735I-S48T4XE-V2, S5735I-H8T2XN-V2, S5735I-H8U2XN-V2, S5735-L10T4X-A-V2, S5735-L14P2S-QA-V2, S5735-L14P2S-TQA-V2, S5735-L16LP2UM2X-QA-V2, S5735-L16LP2X-QA-V2, S5735-L16P2UM2X-QA-V2, S5735-L16T4S-A-V2, S5735-L16T4X-QA-V2, S5735-L24LU8S4XE-QA-V2, S5735-L24P4S-A-V2, S5735-L24P4S-A-V2, S5735-L24P4XE-A-V2, S5735-L24PN4XE-A-V2, S5735-L24ST4XE-A-V2, S5735-L24T4S-A-V2, S5735-L24T4XE-A-V2, S5735-L24T4XE-D-V2, S5735-L24T4X-QA-V2, S5735-L24T8J4XE-A-V2, S5735-L48LP4S-A-V2, S5735-L48LP4XE-A-V2, S5735-L48LPN4XE-A-V2, S5735-L48P4XE-A-V2, S5735-L48PN4XE-A-V2, S5735-L48S4X-A-V2, S5735-L48S4XE-A-V2, S5735-L48T4S-A-V2, S5735-L48T4XE-A-V2, S5735-L48T4XE-D-V2, S5735-L8P2T4X-A-V2, S5735-L8P4S-A-V2, S5735-L8P4X-QA-V2, S5735-L8T4S-A-V2, S5735-L8T4X-QA-V2, S5735R-L16LP2S-QA-V2, S5735R-L16LP2UM2X-QA-V2, S5735R-L16LP2X-QA-V2, S5735R-L16T4S-A-V2, S5735R-L16T4X-QA-V2, S5735R-L24P4S-A-V2, S5735R-L24P4X-A-V2, S5735R-L24T4S-A-V2, S5735R-L24T4X-QA-V2, S5735R-L48LP4S-A-V2, S5735R-L48LP4X-A-V2, S5735R-L48P4X-A-V2, S5735R-L48T4S-A-V2, S5735R-L48T4X-A-V2, S5735R-L8P4S-A-V2, S5735R-L8P4X-QA-V2, S5735R-L8T4S-A-V2, S5735R-L8T4X-QA-V2, S5735R-S24P4X-V2, S5735R-S24T8J4X-XA-V2, S5735R-S48P4X-V2, S5735R-S48T4X-XA-V2, S5735-L8P2T4X-TA-V2, S5735-L10T4X-TA-V2, S5735-L24P4XE-TA-V2, S5735-L48T4XE-TA-V2, S5735-S24HS4XE-V2, S5735-S24P4XE-V2, S5735-S24P4XEZ-V2, S5735-S24P8J4XEZ-V2, S5735-S24PN4XE-V2, S5735-S24ST4XE-V2, S5735-S24T4XE-C-V2, S5735-S24T4XE-V2, S5735-S24T4XEZ-V2, S5735-S24T8J4XE-XA-V2, S5735-S24T8J4XEZ-V2, S5735-S24U4XE-V2, S5735-S48HS4XE-V2, S5735-S48P4XE-V2, S5735-S48P4XEZ-V2, S5735-S48PN4XE-V2, S5735-S48S4XE-V2, S5735-S48T4XE-C-V2, S5735-S48T4XE-V2, S5735-S48T4XE-XA-V2, S5735-S48T4XEZ-V2, S5735-S48U4XE-V2, S5751R-L24P2J2X-A, S5751R-L24P2PN2J2X-A, S5751R-L24P4J-A, S5751R-L24T2J2X-QA, S5751R-L24T4J-QA, S5751R-L8P2J-QA, S5751R-L8P2PN2X-QA, S5751R-L8P2X-QA, S5751R-L8T2J-QA, S5751R-L8T2X-QA, S5755-H24HB2Y2CZ, S5755-H24N4Y-A, S5755-H24P4Y2CZ, S5755-H24T4Y2CZ, S5755-H24U4Y2CZ, S5755-H24UM4Y2CZ, S5755-H24UM4Y2CZ-T, S5755-H24UN4Y2CZ, S5755-H24UTM4X4Y2C, S5755-H24UTM4X4Y2C-T, S5755-H48N4Y-A, S5755-H48P4Y2CZ, S5755-H48T4Y2CZ, S5755-H48T4Y2CZ-B, S5755-H48U4Y2CZ, S5755-H48UM4Y2CZ, S5755-H48UM4Y2CZ-T, S5755-H48UN4Y2CZ, S5755-H48UTM4X4Y2C, S5755-H48UTM4X4Y2C-T, S5755-S24P8J8YZ, S5755-S24P8Y, S5755-S24T8J8YZ, S5755-S24T8Y, S5755-S24U8J8YZ, S5755-S24U8Y, S5755-S48P8Y, S5755-S48P8YZ, S5755-S48T8Y, S5755-S48T8YZ, S5755-S48U8Y, S5755-S48U8YZ).
S6700 Series (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, S6730-H6FX4Y2CZ-V2, S6730-S48X6Q, S6750-H36C, S6750-H48Y8C, S6750-S16X10Y2CZ, S6750-S16X8YZ, S6750-S24T16X8Y2CZ, S6750E-S16X10Y2CZ, S6750E-S24T16X8Y2CZ, S6750-H36C-B, S6780-H4Z).
S8700 Series (S8700-10, S8700-4, S8700-6).
S16700 Series (S16700-4, S16700-8)

Observaciones

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

INFORMACIÓN IMPORTANTE

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	31/10/2026

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

CCN-STIC 1464 Procedimiento de Empleo Seguro CISCO 9300 y 3300 series switches IOS-XE 17.9

INFORMACIÓN IMPORTANTE

Cisco Switches IOS-XE 17.12 - 9200 Series

Versión	IOS-XE 17.12.02
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/11/2024
Revisión de Validez	30/04/2027

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.
Modelos:
Catalyst 9200CX Series:
C9200CX-12T-2X2G, C9200CX-12P-2X2G, C9200CX-8P-2X2G, C9200CX-8UXG-2X.
Catalyst 9200 Series:
C9200-24T, C9200-48T, C9200-24P, C9200-48P, C9200-24PB, C9200-48PB, C9200-48PL, C9200-24PXG, C9200-48PXG.
Network modules:
C9200-NM-4G, C9200-NM-4X, C9200-NM-2Y, C9200-NM-2Q.
Catalyst 9200 L Series:
C9200L-24P-4G, C9200L-24P-4X, C9200L-24T-4G, C9200L-24T-4X, C9200L-48P-4G, C9200L-48P-4X, C9200L-48T-4G, C9200L-48T-4X, C9200L-48PL-4G, C9200L-48PL-4X, C9200L-24PXG-2Y, C9200L-48PXG-2Y, C9200L-24PXG-4X, C9200L-48PXG-4X.

Observaciones

CCN-STIC 1012 Procedimiento de Empleo Seguro Cisco Switches IOS-XE

INFORMACIÓN IMPORTANTE

7.5.3 CORTAFUEGOS

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	31/05/2027
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 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	31/05/2027
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

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	31/05/2027
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 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	31/05/2027
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-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	31/05/2027
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 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	31/05/2027
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 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	31/05/2027
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	31/05/2027
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 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	31/05/2027

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

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	31/05/2027

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-1 600 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	31/05/2027
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 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	31/05/2027
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

Palo Alto Networks 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

Versión	PanOs 11.2
Fabricante	Palo Alto Networks
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	17/02/2025
Revisión de Validez	31/07/2027

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

CCN-STIC-1413 Procedimiento de Empleo Seguro Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

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	18/11/2026

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

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	31/05/2027

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

CCN-STIC 653 Seguridad en Check Point

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	18/11/2026

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	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/09/2024
Revisión de Validez	28/02/2027

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.
Modelos:
Familia F: FWF-81F-2R-3G4G-PoE, FWF-81F-2R-PoE, FG-101F, FG-201F, FG-401F, FG-601F, FG-1801F, FG-1801F-DC, FG-2601F, FG-3001F.
Familia E: FG-91E, FG-101E, FG-201E, FG-301E, FG-401E, FG-401E-DC, FG-501E, FG-601E, FG-1101E, FG-2000E, FG-2201E, FG-2500E, FG-3301E, FG-3401E, FG-3401E-DC, FG-3601E, FG-5001E1.
Familia VM: FortiGate-VM (FG-VM).

Observaciones

CCN-STIC-1406 Procedimiento de Empleo Seguro FortiGate 7.0

INFORMACIÓN IMPORTANTE

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	18/11/2026

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

Firewall NSa Series (2700, 3700, 4700, 5700, 6700)

Versión	SonicOS 7.0.1
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/02/2025
Revisión de Validez	31/07/2027

Descripción

La familia de firewalls de SonicWall están diseñados para adaptarse a una amplia gama de empresas, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones, centros de datos, carriers y proveedores de servicios.
Los firewalls de SonicWall son soluciones de seguridad de capa 7 que incorporan una amplia gama de servicios avanzados para la protección de redes. Entre sus funciones destacan la prevención de intrusiones, Gateway Antivirus, Antimalware, DNS Security, Botnet Filter, GeoIP Filter, filtrado de contenido/URL y control de aplicaciones.
Además, cuentan con inspección profunda de paquetes (DPI), descifrado e inspección de tráfico TLS/SSL (incluyendo TLS 1.3), inteligencia y control de aplicaciones, SD-WAN, y tecnologías avanzadas de prevención y detección de amenazas, como la inspección profunda de memoria en tiempo real (RTDMI).
Gracias a su integración con la nube, estos firewalls permiten un análisis proactivo de amenazas y una administración centralizada, garantizando una protección integral sin afectar el rendimiento de la red.
La serie NSa de generación 7 está orientada a medianas y grandes empresas, así como a organizaciones con múltiples sucursales y centros de datos. Con hardware de alto rendimiento y conectividad de hasta 40-GbE, proporciona una capacidad ampliada para manejar entornos con mayor volumen de tráfico y necesidades avanzadas de inspección y control.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

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	29/09/2027

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

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	18/11/2026

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 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	18/11/2026

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

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	
Versión	7.0
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	18/11/2026

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).

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	18/11/2026

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 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	18/11/2026

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

Stormshield Network Security UTM/NG-Firewall (Appliances desde SN210 a SN6200 en 4 compilaciones distintas: i, xr, XS, S, M, L y XL) y modelos virtuales (SNEVA1 a SNEVA4 y SNEVAU)	
Versión	4.3
Fabricante	Stormshield
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2024
Revisión de Validez	31/03/2027

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

CCN-STIC 1415 Procedimiento de Empleo Seguro UTM/NG-Firewall de Stormshield

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	18/11/2026
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

Sophos Firewall	
Versión	SFOS v20.0
Fabricante	Sophos
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/08/2024
Revisión de Validez	31/01/2027
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

CCN-STIC 1469 Procedimiento de Empleo Seguro Sophos Firewall

INFORMACIÓN IMPORTANTE

Aruba Mobility Controller (9004, 9012, 9240, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) y puntos de acceso (serie 200, 300, 500 y 600)	
Versión	ArubaOS 8.10
Fabricante	HPE Aruba Networking
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	13/04/2027

Descripción

Los HPE Aruba Mobility Controllers, junto con los APs de las series 200, 300, 500 y 600, permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan características de seguridad avanzadas en el control de acceso a la red, en la asignación de políticas de seguridad por usuario mediante el uso de roles, así como la posibilidad de despliegues multizona y terminación de túneles VPN. También se soportan mecanismos de monitorización de espectro y wireless IDS/IPS.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS Controladoras y Puntos de Acceso

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	22/08/2024
Revisión de Validez	31/05/2027

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 rugerizado 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

INFORMACIÓN IMPORTANTE

Firewall NSsp Series (10700, 11700, 13700, 15700, 12800, 12400)

Versión	SonicOS 7.0.1
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/02/2025
Revisión de Validez	31/07/2027

Descripción

La familia de firewalls de SonicWall están diseñados para adaptarse a una amplia gama de empresas, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones, centros de datos, carriers y proveedores de servicios.
Los firewalls de SonicWall son soluciones de seguridad de capa 7 que incorporan una amplia gama de servicios avanzados para la protección de redes. Entre sus funciones destacan la prevención de intrusiones, Gateway Antivirus, Antimalware, DNS Security, Botnet Filter, GeoIP Filter, filtrado de contenido/URL y control de aplicaciones.
Además, cuentan con inspección profunda de paquetes (DPI), descifrado e inspección de tráfico TLS/SSL (incluyendo TLS 1.3), inteligencia y control de aplicaciones, SD-WAN, y tecnologías avanzadas de prevención y detección de amenazas, como la inspección profunda de memoria en tiempo real (RTDMI).
Gracias a su integración con la nube, estos firewalls permiten un análisis proactivo de amenazas y una administración centralizada, garantizando una protección integral sin afectar el rendimiento de la red.
La serie NSSp de generación 7 responde a los requerimientos de grandes corporaciones, centros de datos, carriers y proveedores de servicios con conectividad de hasta 100-GbE,. Su plataforma de alto rendimiento permite gestionar millones de conexiones simultáneas con baja latencia, asegurando protección sin comprometer la velocidad ni la escalabilidad.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Atlas-840, M10-Smart Series, M2 Series, 4GePlus Series, Teldat-5Ge Series, 5Ge-Rail Series, Connect-4GePlus Series, Connect-5Ge Series, Connect-FW Series, Regesta SmartV2 Series, H5 Rail Series	
Versión	11.02.04.85.02
Fabricante	TELDAT
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	23/09/2025
Revisión de Validez	29/02/2028

Descripción

Familia de routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones

Observaciones

CCN-STIC 1471 Procedimiento de Empleo Seguro Teldat Router

SDE-1X Series	
Versión	OSDx v4.2.1.3
Fabricante	TELDAT
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2028

Descripción

Familia de edge-routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones.

Observaciones

CCN-STIC 1484 Procedimiento de Empleo Seguro Teldat SDE-1x Series y SDE-2x Series

INFORMACIÓN IMPORTANTE

RS SEries, M2 Series, M10 Series, Atlas-840 Series, Ares-C640 Series	
Versión	OSDx v4.2.1.3
Fabricante	TELDAT
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	30/06/2026
Revisión de Validez	30/11/2026

Descripción

Familia de routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones.

Observaciones

Procedimiento de Empleo pendiente de publicación.

Cisco FTD 7.4 on Cisco Secure Firewall 4200 Series with FMC-FMCv	
Versión	7.4
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	22/04/2025
Revisión de Validez	30/11/2026

Descripción

Los Cisco FTD 7.4 en la serie Cisco Secure Firewall 4200 con FMC/FMCv están diseñados para proporcionar una defensa avanzada contra amenazas y una gestión centralizada de la seguridad.
Estos firewalls combinan capacidades de inspección profunda de paquetes (DPI) con la inteligencia de amenazas de Cisco Talos, ofreciendo una protección robusta contra ataques conocidos y desconocidos.
La serie 4200 está optimizada para un rendimiento alto y una baja latencia, soportando hasta 100 Gbps de rendimiento de firewall. Con la versión 7.4, se introducen mejoras en la gestión de políticas y la visibilidad de la red, facilitando la administración de grandes entornos de seguridad. Además, la integración con Cisco SecureX permite una respuesta rápida y coordinada a incidentes de seguridad.
El Cisco Firepower Management Center (FMC) y su versión virtual (FMCv) proporcionan una plataforma centralizada para la gestión de políticas, la monitorización de eventos y la generación de informes detallados. Estas herramientas permiten una administración eficiente y una visibilidad completa de la postura de seguridad de la red.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco FTD 7.4 on Firepower 1000 Series with FMC-FMCv

Versión	7.4
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	22/04/2025
Revisión de Validez	30/11/2026

Descripción

Los Cisco FTD 7.4 en la serie Firepower 1000 con FMC/FMCv están diseñados para ofrecer una protección avanzada contra amenazas y una gestión centralizada de la seguridad.
Estos firewalls combinan capacidades de inspección profunda de paquetes (DPI) con la inteligencia de amenazas de Cisco Talos, proporcionando una defensa robusta contra ataques conocidos y desconocidos. La serie Firepower 1000 está optimizada para un rendimiento eficiente en entornos de pequeñas y medianas empresas, soportando hasta 8 Gbps de rendimiento de firewall2. Con la versión 7.4, se mejoran las capacidades de gestión de políticas y visibilidad de la red, facilitando la administración de la seguridad en entornos complejos. Además, la integración con Cisco SecureX permite una respuesta rápida y coordinada a incidentes de seguridad.
El Cisco Firepower Management Center (FMC) y su versión virtual (FMCv) proporcionan una plataforma centralizada para la gestión de políticas, la monitorización de eventos y la generación de informes detallados. Estas herramientas permiten una administración eficiente y una visibilidad completa de la postura de seguridad de la red.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

SDE-2X Series

Versión	OSDx v4.2.1.3
Fabricante	TELDAT
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2028

Descripción

Familia de edge-routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones.

Observaciones

CCN-STIC 1484 Procedimiento de Empleo Seguro Teldat SDE-1x Series y SDE-2x Series

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	31/05/2027

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

CCN-STIC 653 Seguridad en Check Point

HPE Aruba Networking Orchestrator and EdgeConnect Release	
Versión	9.4.2
Fabricante	HPE Aruba Networking
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/04/2025
Revisión de Validez	31/10/2026

Descripción

Los productos incluidos en esta cualificación son los pertenecientes a las familias EC-101XX, EC-S-P y EC-M-H.
La solución EdgeConnect SD-WAN de HPE Aruba Networking permite desplegar redes SD-WAN seguras de cualquier tamaño, tanto locales como internacionales mediante el uso de diversas topologías como hub&spoke, mesh o regionales. La solución SD-WAN permite construir múltiples overlays con políticas diferenciadas de gestión de los enlaces y topologías específicas dependiendo del tipo de tráfico. EdgeConnect permite una gestión de enlaces muy avanzada que incluye balanceo por paquete y dynamic path control lo que permite ofrecer al usuario conexiones agregadas de alta capacidad y calidad incluso utilizando enlaces degradados. La solución EdgeConnect introduce múltiples funcionalidades de seguridad como VRFs, statefull firewall con zonas e IDS/IPS. La solución SD-WAN de Aruba ofrece funcionalidades de optimización WAN mediante aceleración de protocolo TCP y reducción de datos mediante compresión y deduplicación. EdgeConnect SD-WAN permite la integración con múltiples proveedores de seguridad SSE lo que permite, mediante el uso de políticas específicas, derivar el tráfico a los diferentes proveedores de seguridad

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

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	31/05/2027

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

CCN-STIC 653 Seguridad en Check Point

CIBER ARMOUR CLAVISTER COS CORE	
Versión	15.00 VE
Fabricante	CLAVISTER
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2026
Revisión de Validez	28/02/2027

Descripción

Clavister cOS Core es el software Next Generation Firewall (NGFW) que se despliega tanto en el hardware Clavister NetWall como en el hardware de grado militar Clavister CyberArmour RSG, o en entornos virtualizados. Funcionalidades clave que permite gestionar y protecciones que ofrece: IP Routing: Estático, Dinámico, Virtual, Multicast. Políticas Firewall: Stateful para TCP, UDP e ICMP. Traducción de direcciones: Basada en políticas, Traducción Dinámica (NAT) y Estática (SAT). Detección de Anomalías por IA: Análisis de series temporales mediante machine learning para detecciones en tiempo real. ALG’s. VPN: IPsec, L2TP, L2TPv3, PPTP, y SSL VPN. Terminación TLS/SSL. Control de Aplicación. Escáner Anti-Virus. Capacidades IDP (Intrusion Detection and Prevention). Filtrado por contenido Web. Gestión del tráfico: Traffic Shaping, Threshold Rules y Server Load Balancing. Autenticación de usuarios. Interfaz de usuario basada en web, CLI, REST API, logging, SNMP, Cloud-Init. Alta Disponibilidad (HA) Activa y pasiva. Routers Virtuales. Soporte IPv6. ZoneDefense. Virtualización: VMware, KVM (x86 y ARM) e Hyper-V. Adicionalmente: RADIUS, Accounting, DHCP, protección DoS, PPPoE, GRE, DNS dinámico.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Firepower Threat Defense (FTD) on Cisco Secure Firewall 3100 Series with FMC/FMCv

Versión	7.4
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	27/02/2025
Revisión de Validez	31/07/2027

Descripción

Cisco FTD 7.4 (Firepower Threat Defense) es una solución de seguridad que combina capacidades de firewall de próxima generación (NGFW) y sistema de prevención de intrusiones (IPS).
En esta versión se incluyen mejoras en la detección de amenazas, bloqueo de malware en sesiones TLS cifradas y acceso a aplicaciones sin cliente para una postura de seguridad Zero Trust1.
Puede desplegarse como un dispositivo único o en modo multi-instancia, lo que permite ejecutar múltiples instancias independientes de FTD en el mismo hardware.
FMC (Firepower Management Center): Es la plataforma de gestión centralizada para soluciones de seguridad de Cisco. Permite la administración, monitoreo y análisis de las políticas de seguridad y eventos de red en tiempo real.
FMCv (Firepower Management Center Virtual): Es la versión virtualizada del FMC, que ofrece las mismas capacidades de gestión y análisis, pero está diseñada para entornos virtuales y de nube..

Observaciones

CCN-STIC 651B Procedimiento de Empleo Seguro Cortafuegos Cisco Secure Firewall

Forcepoint Virtual Appliance (ESXi)

Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2022
Revisión de Validez	29/09/2027

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

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	29/09/2027

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 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	29/09/2027

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

Klas TRX R2	
Versión	KlasOS Keel 5.4.0
Fabricante	Klas
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	23/07/2025
Revisión de Validez	31/12/2027
Descripción	

TRX R2 es un enrutador rugerizado y diseñado para operar en las condiciones más extremas. Tiene capacidad de conexión a múltiples redes WAN incluyendo: redes móviles, WiFi y redes fijas a 1G/10G. Su sistema operativo KlasOS Keel incluye funcionalidades de enrutamiento, cortafuegos, SD-WAN, GPS y virtualización. Esto permite securizar el acceso a todo tipo de redes usando el cortafuegos integrado o virtualizando otra solución de terceros.

Observaciones

CCN-STIC 1478 Procedimiento de Empleo Seguro Klas TRX R2

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	31/05/2027
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 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	31/05/2027

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

SRX Series (300, 320, 340, 345, 345-DUAL-AC, 380, 1500, 1600, 2300, 4100, 4200, 4300, 4600, 5400, 5600, 5800)_	
Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/04/2025
Revisión de Validez	30/09/2027

Descripción

La familia de firewall mid-range de Juniper Networks® 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 Procedimiento de Empleo Seguro Juniper SRX Series

INFORMACIÓN IMPORTANTE

i4000, i5000, i7000, i10000, i11000-DS, i15000, I15000-DF, VIPRION C2400/B2250, C4480/B4450, r4000, R5000, R10000, VELOS BX110/CX410, BIP-IP Virtual Edition	
Versión	F5 BIG-IP 17.1.0.1
Fabricante	F5
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	14/01/2025
Revisión de Validez	30/06/2027

Descripción

F5 BIG-IP es una herramienta clave en la publicación y entrega de aplicaciones, optimizando su disponibilidad, velocidad y fiabilidad a través de las capas de aplicación y red. Como dispositivo full-proxy, inspecciona, gestiona y da visibilidad al tráfico entrante y saliente de las aplicaciones corporativas. Proporciona desde balanceo de carga hasta decisiones avanzadas de gestión de tráfico basadas en cliente, servidor o estado de la aplicación, lo que permite distribuir usuarios de forma inteligente hacia los servidores. Totalmente programable y granular, se adapta a necesidades actuales y futuras de control de tráfico, mejorando el tiempo de respuesta y la experiencia de los usuarios. Además, en su configuración de firewall, BIG-IP actúa como solución de seguridad perimetral en centros de datos, protegiendo las capas 3 y 4 con políticas avanzadas y defensa frente a ataques de denegación de servicio distribuidos. Su interfaz de gestión intuitiva, con reportes y analíticas, ofrece una visión completa del estado de seguridad del perímetro de red y asegura la protección de los recursos críticos.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

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	31/05/2027

Descripción

Los firewalls de inteligencia artificial (IA) de las series HiSecEngine USG6000F y USG12000 de Huawei están diseñados para Data Centers de próxima generación en el extremo de la red. Basada en nuevas plataformas de software y hardware, la serie ofrece capacidades de pila doble de Protocolo de Internet versión 4 y 6 (IPv4)/(IPv6), lo que mejora enormemente el rendimiento del servicio, con tecnologías inteligentes que ayudan aún más a defenderse eficazmente contra las amenazas avanzadas de hoy en día.

Observaciones

CCN-STIC 1475. Procedimiento de Empleo Seguro Huawei USG6000F & USG12000F Series Firewall

INFORMACIÓN IMPORTANTE

Aruba Virtual Mobility Controllers (MC-VA-50, MC-VA-250 y MC-VA-1k) y puntos de acceso (serie 200, 300, 500 y 600)	
Versión	ArubaOS 8.10
Fabricante	HPE Aruba Networking
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	13/04/2027

Descripción

Los HPE Aruba Mobility Controllers, junto con los APs de las series 200, 300, 500 y 600, permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan características de seguridad avanzadas en el control de acceso a la red, en la asignación de políticas de seguridad por usuario mediante el uso de roles, así como la posibilidad de despliegues multizona y terminación de túneles VPN. También se soportan mecanismos de monitorización de espectro y wireless IDS/IPS.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS Controladoras y Puntos de Acceso

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	
Versión	PAN-OS 11.0
Fabricante	Palo Alto Networks
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/06/2024
Revisión de Validez	30/11/2026

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

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

FortiGate - Familia F

Versión	FortiOS 7.2
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/02/2026
Revisión de Validez	31/07/2028

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.
Modelos:
FortiGate-40F, ,FortiGate-40F-3G4G, FortiWifi-40F, FortiWifi-40F-3G4G, FortiGate-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-60F, FortiWifi-60F, FortiGate-61F, FortiGateRugged-70F, FortiGateRugged-70F-3G4G, FortiGate-70F, FortiGate-71F, FortiGate-80F, FortiGate-80F-PoE, FortiWifi-80F-2R, FortiWifi-80F-2R-3G4G-DSL, FortiGate-81F, FortiWifi-81F-2R-3G4G-DSL, FortiGate-81F-PoE, FortiWifi-81F-2R, FortiWifi-81F-2R-3G4G-PoE, FortiWifi-81F-2R-PoE, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-200F, FortiGate-201F, FortiGate-400F, FortiGate-600F, FortiGate-601F, FortiGate-1000F, FortiGate-1001F, FortiGate-1800F, FortiGate-1800F-DC, FortiGate-1801F, FortiGate-1801F-DC, FortiGate-2600F, FortiGate-2601F, FortiGate-2601F-DC, FortiGate-3000F, FortiGate-3000F-DC, FortiGate-3001F, FortiGate-3001F-DC, FortiGate-3200F, FortiGate-3201F, FortiGate-3500F, FortiGate-35011F, FortiGate-3700F, FortiGate-3701F, FortiGate-4200F, FortiGate-4200F-DC, FortiGate-4201F, FortiGate-4201F-DC, FortiGate-4400F, FortiGate-4400F-DC, FortiGate-4401F, FortiGate-4401F-DC, FortiGate-4800F, FortiGate-4801F, FortiGate-6001F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F.

Observaciones

CCN-STIC 1406 Procedimiento de Empleo Seguro FortiGate 7

INFORMACIÓN IMPORTANTE

FortiGate - Familia G

Versión	FortiOS 7.2
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/02/2026
Revisión de Validez	31/07/2028

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.
Modelos:
FortiGate-30G, FortiGate-31G, FortiGate-70G, FortiGate-70G-POE, FortiGate-71G, FortiGate-71G-POE, FortiGate-90G, FortiGate-91G, FortiGate-120G, FortiGate-121G, FortiGate-200G, FortiGate-201G, FortiGate-700G, FortiGate-701G, FortiGate-900G, FortiGate-900G-DC, FortiGate-901G, FortiGate-901G-DC, FortiWifi-30G, FortiWifi-31G, FortiWifi-70G, FortiWifi-71G, FortiWifi-70G-POE.

Observaciones

CCN-STIC 1406 Procedimiento de Empleo Seguro FortiGate 7

INFORMACIÓN IMPORTANTE

Firewall NSv Series (270, 470, 870)

Versión	SonicOS 7.0.1
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/02/2025
Revisión de Validez	31/07/2027

Descripción

La familia de firewalls de SonicWall están diseñados para adaptarse a una amplia gama de empresas, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones, centros de datos, carriers y proveedores de servicios.
Los firewalls de SonicWall son soluciones de seguridad de capa 7 que incorporan una amplia gama de servicios avanzados para la protección de redes. Entre sus funciones destacan la prevención de intrusiones, Gateway Antivirus, Antimalware, DNS Security, Botnet Filter, GeoIP Filter, filtrado de contenido/URL y control de aplicaciones.
Además, cuentan con inspección profunda de paquetes (DPI), descifrado e inspección de tráfico TLS/SSL (incluyendo TLS 1.3), inteligencia y control de aplicaciones, SD-WAN, y tecnologías avanzadas de prevención y detección de amenazas, como la inspección profunda de memoria en tiempo real (RTDMI).
Gracias a su integración con la nube, estos firewalls permiten un análisis proactivo de amenazas y una administración centralizada, garantizando una protección integral sin afectar el rendimiento de la red.
La serie NSv de generación 7 extiende la protección de SonicWall a entornos virtualizados en nubes públicas y privadas. Diseñada para arquitecturas híbridas y totalmente en la nube, ofrece la misma seguridad que un firewall físico con la flexibilidad necesaria para adaptarse a infraestructuras dinámicas y escalables.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Firewall TZ Series (270, 270W, 370, 330W, 470, 470W, 570, 570W, 570POE, 670)

Versión	SonicOS 7.0.1
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/02/2025
Revisión de Validez	31/07/2027

Descripción

La familia de firewalls de SonicWall están diseñados para adaptarse a una amplia gama de empresas, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones, centros de datos, carriers y proveedores de servicios.
Los firewalls de SonicWall son soluciones de seguridad de capa 7 que incorporan una amplia gama de servicios avanzados para la protección de redes. Entre sus funciones destacan la prevención de intrusiones, Gateway Antivirus, Antimalware, DNS Security, Botnet Filter, GeoIP Filter, filtrado de contenido/URL y control de aplicaciones.
Además, cuentan con inspección profunda de paquetes (DPI), descifrado e inspección de tráfico TLS/SSL (incluyendo TLS 1.3), inteligencia y control de aplicaciones, SD-WAN, y tecnologías avanzadas de prevención y detección de amenazas, como la inspección profunda de memoria en tiempo real (RTDMI).
Gracias a su integración con la nube, estos firewalls permiten un análisis proactivo de amenazas y una administración centralizada, garantizando una protección integral sin afectar el rendimiento de la red.
La serie TZ de generación 7 de está diseñada para pequeñas empresas y entornos departamentales que requieren seguridad avanzada con una gestión sencilla. Su arquitectura compacta ofrece un equilibrio entre rendimiento y protección, permitiendo implementar soluciones de seguridad de nivel empresarial en redes cableadas, con conectividad de hasta 10-GbE e inalámbricas, y con una fácil administración.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

OPNsense Business Edition

Versión	25.4
Fabricante	Deciso B.V
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2025
Revisión de Validez	31/07/2027

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

INFORMACIÓN IMPORTANTE

OPNsense Business Edition

Versión	25.10
Fabricante	Deciso B.V
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2026
Revisión de Validez	31/07/2027

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

INFORMACIÓN IMPORTANTE

OPNsense Business Edition

Versión	26.4
Fabricante	Deciso B.V
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	30/06/2026
Revisión de Validez	31/07/2027

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

INFORMACIÓN IMPORTANTE

FortiGate - Familia E

Versión	FortiOS 7.2
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/02/2026
Revisión de Validez	31/07/2028

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.
Modelos:
FortiGate-60E, FortiGate-60E-PoE, FortiGate-60E-DSL, FortiWifi-60E, FortiWifi-60E-DSL, FortiWifi-60E-DSLJ, FortiGate-61E, FortiWifi-61E, FortiGate-80E, FortiGate-80E-PoE, FortiGate-81E, FortiGate-81E-PoE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-140E, FortiGate-140E-PoE, FortiGate-200E, FortiGate-201E, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-401E, FortiGate-401E-DC, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-601E, FortiGate-1100E, FortiGate-1100E-DC, FortiGate-1101E, FortiGate-1101E-DC, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3400E-DC, FortiGate-3401E, FortiGate-3401E-DC, FortiGate-3600E, FortiGate-3600E-DC, FortiGate-3601E, FortiGate-3960E, FortiGate-3960E-DC, FortiGate-3980E, FortiGate-3980E-DC, FortiGate-50001E1.

Observaciones

CCN-STIC 1406 Procedimiento de Empleo Seguro FortiGate 7

INFORMACIÓN IMPORTANTE

7.5.4 PROXIES

Symantec WPS	
Versión	
Fabricante	Symantec a division of Broadcom
Familia	Proxies
Tipo	Servicio
Categoría ENS	MEDIA
Fecha Inclusión	01/02/2024
Revisión de Validez	31/10/2026

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

Guía CCN-STIC 1463 Procedimiento de Empleo Seguro Symantec Web Protection Suite

INFORMACIÓN IMPORTANTE

Zscaler Work from Anywhere (ZIA)

Versión

Fabricante Zscaler Spain

Familia Proxies

Tipo Producto

Categoría ENS MEDIA

Fecha Inclusión 01/01/2023

Revisión de Validez 31/12/2026

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

CCN-STIC-1477 Procedimiento de Empleo Seguro Zscaler Zia.

INFORMACIÓN IMPORTANTE

7.5.5 DISPOSITIVOS DE RED INALÁMBRICOS

Cisco 9120 Series Wi-Fi 6 Access Points (C9120AXI-x, C9120AXE-x, C9120AXP-x)	
Versión	IOS-XE 17.12
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	30/09/2027
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 4800 Access Point (AIR-AP4800-x-K9 y AIR-AP4800-x-K9C)	
Versión	IOS-XE 17.12
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	30/09/2027
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

FortiAP

Versión	7.2.0
Fabricante	Fortinet
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/07/2025
Revisión de Validez	31/01/2028

Descripción

Los puntos de acceso inalámbricos Fortinet, integrados con FortiGate (siendo posible integrarlo con cualquier versión y modelo cualificado de FortiGate), proporcionan conectividad WiFi segura en el perímetro de red. La solución está diseñada sobre FortiOS y puede gestionarse de forma centralizada mediante FortiManager (con cualquier versión y modelo cualificado). La arquitectura permite despliegues en modo controlado o distribuido, y proporciona segmentación dinámica de usuarios, autenticación 802.1X, visibilidad completa del tráfico, y políticas de acceso unificadas. Su integración con Fortinet Security Fabric permite aplicar análisis de amenazas, filtrado de contenido y respuesta automatizada a incidentes en entornos corporativos, educativos y críticos.

Observaciones

CCN-STIC 1485 Procedimiento de Empleo Seguro FortiAP v7.2.0

INFORMACIÓN IMPORTANTE

Huawei WLAN AirEngine Series

Versión	V600R024C00SPC100
Fabricante	Huawei Technologies
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2026
Revisión de Validez	31/10/2026

Descripción

Los productos de la serie AirEngine Wi-Fi de Huawei constituyen una nueva generación de soluciones de red inalámbrica diseñadas para entornos de oficina y de producción en empresas. Los productos de la serie AirEngine de Huawei son compatibles con métodos de acceso seguro, métodos de autenticación y diversos algoritmos que cumplen con los estándares del sector, y satisfacen plenamente las necesidades de acceso seguro a la red de clientes de diversos sectores.

Modelos:
- AirEngine 6776-57T
- AirEngine 6776-56TP
- AirEngine 5776-26
- AirEngine 5773-23H
- AirEngine 5773-22P
- AirEngine 5773-21
- AirEngine 5773-23HW
- AirEngine 5773-25HW
- AirEngine 5773-23WP
- AirEngine 6776-58TI
- AirEngine 6776I-X6TH
- AirEngine 6776I-X7TH

Observaciones

CCN-STIC 1426 Procedimiento de Empleo Seguro Huawei WLAN AirEngine Series

Cisco 9105 Series Wi-Fi 6 Access Points (C9105AXI-x, C9105AXW-x, C9105AXIT-x y C9105AXWT-x)

Versión	IOS-XE 17.12
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	30/09/2027

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 EW6300 Series Access Points (ESW-6300-CON-X-K9)

Versión	IOS-XE 17.12
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	30/09/2027

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

H3C Wireless Controllers and Access Points

Versión	H3C Comware Software, Version 7.1.064, H3C Comware
Fabricante	New H3C Technologies
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/07/2026
Revisión de Validez	31/12/2026

Descripción

Los controladores inalámbricos H3C WX5800, WX2800 y WX3800, junto con los puntos de acceso H3C WA6500, WA7200, WA7300, WA7500 y WA7600, conforman una solución WLAN empresarial para proporcionar acceso inalámbrico seguro en entornos corporativos, administraciones públicas e infraestructuras críticas.

La solución está formada por controladores (AC) y puntos de acceso (AP) que trabajan de forma conjunta para ofrecer conectividad Wi Fi, autenticación de usuarios, aplicación de políticas de acceso, monitorización de la red y gestión de la seguridad.

Entre sus principales funciones de seguridad destacan:
- Autenticación y control de acceso
- Protección de las comunicaciones mediante protocolos criptográficos estándar y soporte de WPA2/WPA3
- Gestión segura de credenciales y claves criptográficas
- Filtrado y control del tráfico mediante ACL y políticas de seguridad
- Supervisión del entorno radioeléctrico para detectar comportamientos anómalos
- Administración segura, registro de eventos y auditoría
- Mecanismos para garantizar la integridad y disponibilidad de los servicios, previniendo accesos no autorizados y ataques de red.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Aruba Mobility Controller (9004, 9012, 9240, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) y puntos de acceso (serie 200, 300, 500 y 600)

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	13/04/2027

Descripción

Los HPE Aruba Mobility Controllers, junto con los APs de las series 200, 300, 500 y 600, permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan características de seguridad avanzadas en el control de acceso a la red, en la asignación de políticas de seguridad por usuario mediante el uso de roles, así como la posibilidad de despliegues multizona y terminación de túneles VPN. También se soportan mecanismos de monitorización de espectro y wireless IDS/IPS.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS Controladoras y Puntos de Acceso

Aruba Virtual Mobility Controllers (MC-VA-50, MC-VA-250 y MC-VA-1k) y puntos de acceso (serie 200, 300, 500 y 600)

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	13/04/2027

Descripción

Los HPE Aruba Mobility Controllers, junto con los APs de las series 200, 300, 500 y 600, permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan características de seguridad avanzadas en el control de acceso a la red, en la asignación de políticas de seguridad por usuario mediante el uso de roles, así como la posibilidad de despliegues multizona y terminación de túneles VPN. También se soportan mecanismos de monitorización de espectro y wireless IDS/IPS.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS Controladoras y Puntos de Acceso

INFORMACIÓN IMPORTANTE

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
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 (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, 6760-51EI, 6760R-51, 6760-X1, 6760-X1E, 3562-10, 3562-10SW, 5562-10, 5562-10SW, 5562-17W, 5760-11DH, 5761-10WD, 5761-11EI, 5761-12, 5761-12W)	
Versión	V200R023C00SPC100 + V200R023C00SPH327T
Fabricante	Huawei Technologies
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 9115 Series Wi-Fi 6 Access Points (C9115AXI-x y C9115AXE-x)	
Versión	IOS-XE 17.12
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	30/09/2027
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 17.12
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	30/09/2027
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 9130 Series Wi-Fi 6 Access Points (C9130AXI-x, C9130AXE-x, C9130AXE-STA-x)	
Versión	IOS-XE 17.12
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	30/09/2027
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 17.12
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	30/09/2027
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 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 17.12
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	30/09/2027
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 2800 Series Access Points (AIR-AP2802I-x-K9, AIR-AP2802I-x-K9C, AIR-AP2802E-x-K9 y AIR-AP2802E-x-K9C)	
Versión	IOS-XE 17.12
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	30/09/2027
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 Catalyst 9800 Series Wireless Controllers and Access Points

Versión	IOS-XE17.12
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	16/07/2025
Revisión de Validez	30/11/2026

Descripción

Cisco Catalyst 9800 Series Wireless Controllers son controladores de última generación diseñados para redes inalámbricas basadas en intención. Funcionan con Cisco IOS XE y combinan las capacidades de radiofrecuencia de Cisco Aironet con las funciones avanzadas de redes basadas en intención. Los Cisco Catalyst 9800 Series Wireless Controllers, junto con los puntos de acceso Catalyst, forman parte de la solución de red inalámbrica empresarial de Cisco basada en arquitectura intent-based networking. Con la versión de software IOS XE 17.12, esta plataforma ofrece una conectividad Wi-Fi segura, resiliente y altamente escalable, ideal para organizaciones que requieren una infraestructura de red moderna y preparada para el futuro.Algunas características clave incluyen:

• Alta disponibilidad con actualizaciones de software sin interrupciones mediante parches en caliente y frío.

• Seguridad integrada, con arranque seguro, defensas en tiempo de ejecución, firma de imágenes y verificación de integridad.

• Flexibilidad de implementación, ya que pueden instalarse en dispositivos locales, en la nube o integrados en switches y puntos de acceso de Cisco.

Observaciones

Procedimiento de Empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

7.5.6 PASARELAS SEGURAS DE INTERCAMBIO DE DATOS

PSTatx	
Versión	1.7
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026
Descripción	

PSTatx es una pasarela segura de nivel de aplicación orientada a entornos militares y de defensa, basada en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL 4+ (AVA_VAN.5 + ALC_FLR.3).
PSTatx permite el intercambio controlado de Información de vigilancia aérea ASTERIX entre dominios de seguridad (cross-domain).
Más información: https://www.autek.es/cross-domain/pstgateways

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

PSTgateways Custom	
Versión	4.13
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026
Descripción	

PSTgateways es una familia de pasarelas seguras de nivel de aplicación que permiten el intercambio controlado de información entre dominios de seguridad (cross-domain). Todos los productos están basados en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL4+ (AVA_VAN.5 + ALC_FLR.3).
Los productos PSTgateways personalizados permiten combinaciones de servicios y/o filtros de datos (formato y contenido) a medida. Pueden incorporar comprobaciones de etiquetado de seguridad (STANAGs 4774/4778).

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

PSTacp

Versión	1.7
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

Descripción

PSTacp es una pasarela segura de nivel de aplicación orientada a entornos militares y de defensa, basada en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL 4+ (AVA_VAN.5 + ALC_FLR.3).
PSTacp permite el intercambio controlado de mensajería ACP-127 entre dominios de seguridad (cross-domain).
Más información: https://www.autek.es/cross-domain/pstgateways

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

PSTmip

Versión	1.7
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

Descripción

PSTmip es una pasarela segura de nivel de aplicación orientada a entornos militares y de defensa, basada en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL 4+ (AVA_VAN.5 + ALC_FLR.3).
PSTmip permite el intercambio controlado de datos tácticos MIP4 con comprobación de etiquetado y firma digital (STANAG 4774/8) entre Sistemas de mando y control desplegados en diferentes dominios de seguridad (cross-domain).
Más información: https://www.autek.es/cross-domain/pstgateways

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

PSTjreap

Versión	1.7
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

Descripción

PSTjreap es una pasarela segura de nivel de aplicación orientada a entornos militares y de defensa, basada en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL 4+ (AVA_VAN.5 + ALC_FLR.3).
PSTjreap permite el intercambio controlado de información Tactical Data Link mediante JREAP-C entre dominios de seguridad (cross-domain).
Más información: https://www.autek.es/cross-domain/pstgateways

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

PSTgateways (PSTfile, PSTmail, PSTudp)

Versión	4.13
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

Descripción

PSTgateways es una familia de pasarelas seguras de nivel de aplicación que permiten el intercambio controlado de información entre dominios de seguridad (cross-domain). Todos los productos están basados en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common CriteriaEAL4+ (AVA_VAN.5 + ALC_FLR.3). Productos de propósito general:
PSTfile: servicios de transferencia automática de ficheros.
PSTmail: servicios de transferencia de mensajes de correo electrónico.
PSTudp: servicios de transferencia de payload de paquetes UDP.
Más información: https://www.autek.es/cross-domain/pstgateways

Observaciones

Procedimiento de empleo seguro: CCN-STIC-1401 Configuración segura de pasarelas de AUTEK

INFORMACIÓN IMPORTANTE

PSTcsd	
Versión	1.7
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

Descripción

PSTcsd es una pasarela segura de nivel de aplicación orientada a entornos militares y de defensa, basada en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL 4+ (AVA_VAN.5 + ALC_FLR.3).
PSTcsd permite el intercambio controlado de información JISR (MAJIIC) entre dominios de seguridad (cross-domain).
Más información: https://www.autek.es/cross-domain/pstgateways

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

PSTgateways Web services (PSTws)	
Versión	1.7
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

Descripción

PSTgateways es una familia de pasarelas seguras de nivel de aplicación que permiten el intercambio controlado de información entre dominios de seguridad (cross-domain). Todos los productos están basados en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL4+ (AVA_VAN.5 + ALC_FLR.3).
Los productos PSTgateways basados en web services soportan flujos de datos a través de protocolo HTTP/s, permiten filtros a medida de formato y contenido sobre APIs REST o SOAP. Pueden incorporar comprobaciones de etiquetado de seguridad (STANAGs 4774/4778).
Más información: https://www.autek.es/cross-domain/pstgateways

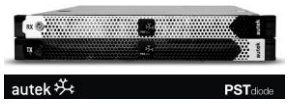
Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

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	31/10/2026



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

INFORMACIÓN IMPORTANTE

7.5.8 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	31/10/2026

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 permitirlas, o bien enviar desafíos, como verificaciones de CAPTCHA, al navegador o al usuario del cliente.

Observaciones

CCN-STIC 887A Guía de configuración segura AWS

INFORMACIÓN IMPORTANTE

7.5.9 REDES DEFINIDAS POR SOFTWARE (SDN)

Cisco Nexus 9000 Switch Series with ACI mode, APIC and NX-OS software-ACI	
Versión	NX-OS System Software-ACI 16.1(2g), APIC 6.1(2g)
Fabricante	Cisco Systems
Familia	Redes definidas por software (SDN)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	03/03/2026
Revisión de Validez	31/10/2026

Descripción

Cisco Application Policy Infrastructure Controller (APIC) con ACI (Application Centric Infrastructure) es una plataforma centralizada e integral para la administración, automatización y monitorización de redes definidas por software en centros de datos. Esta solución permite a las organizaciones gestionar su infraestructura desde un entorno on-premise, ofreciendo políticas de red consistentes, automatización avanzada y visibilidad profunda del tráfico y el rendimiento. Gracias a la arquitectura ACI, APIC facilita la implementación de aplicaciones de forma ágil y segura, adaptando automáticamente la red a las necesidades de los servicios. El sistema mejora la eficiencia operativa mediante flujos de trabajo simplificados, segmentación dinámica y soporte para actualizaciones centralizadas. Con una interfaz moderna y herramientas intuitivas, APIC-ACI permite a los equipos de TI estandarizar operaciones, optimizar la seguridad y garantizar la disponibilidad de aplicaciones críticas.

Modelos Hardware:
- Cisco 9300 ACI Leaf Models: 93108TC-FX3H, 93108TC-FX3P, 9348GC-FXP, 93216TC-FX2, 93180YC-FX3H, 93180YC-FX3, 93240YC-FX2, 93360YC-FX2, 9336C-FX2, 9336C-FX2-E, 9364C-GX, 9316D-GX, 93600CD-GX, 9364D-GX2A, 9348D-GX2A, 332D-GX2B.
- Cisco 9300, 9400, 9500 ACI Spine Models: 9316D-GX, 9332D-GX2B, 9348D-GX2A, 93600CD-GX, 9364C-GX, 9364D-GX2A, C9408, C9504, 9508, C9508-FM-E2, C9516.
- Cisco 9500 Model Components: Supervisor A/A+, Supervisor B /B+, Supervisor A, N9K-SC-A, APIC M4, APIC L4.

Observaciones

N/A

INFORMACIÓN IMPORTANTE

iMaster NCE Campus

Versión	V300R023C00SPC010T
Fabricante	Huawei Technologies
Familia	Redes definidas por software (SDN)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/10/2024
Revisión de Validez	31/03/2027

Descripción

iMaster NCE-Campus, es un sistema de gestión y control de redes autónomas de última generación de Huawei para redes de campus, integra funciones de gestión, control, análisis e inteligencia artificial (IA), lo que proporciona una automatización completa del ciclo de vida de las redes de campus. En cuanto a la capacidad NAC, introduce el nuevo protocolo de autenticación HTTP2.0 y puede autenticar un gran número de dispositivos de red y usuarios utilizando varios modos de autenticación de acceso. Esto incluye la autenticación 802.1X, la autenticación por portal, la autenticación por SMS y la autenticación por redes sociales. También proporciona múltiples políticas de control de acceso de usuarios, lo que mejora significativamente la seguridad de la red. Al mismo tiempo, ofrece la posibilidad de que los usuarios se desacoplen de las direcciones IP, lo que les permite acceder a la red en cualquier momento y lugar, con permisos consistentes. Esto garantiza la libre movilidad y una experiencia de usuario consistente, al tiempo que se cumplen los requisitos de control de permisos.

Observaciones

CCN-STIC 1474 PES Huawei iMaster NCE Campus

INFORMACIÓN IMPORTANTE

SDWAN Cisco vEdge Routers running on IOS XE 17.12 with Catalyst SD-WAN 20.12

Versión	SD-WAN 20.12
Fabricante	Cisco Systems
Familia	Redes definidas por software (SDN)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	24/02/2025
Revisión de Validez	31/07/2027

Descripción

Los routers Cisco vEdge que ejecutan IOS XE 17.12 con Catalyst SD-WAN 20.12 son dispositivos avanzados diseñados para optimizar la gestión y rendimiento de redes WAN. Combinando robustez de hardware con capacidades de software de SD-WAN, permitiendo una administración centralizada y una mayor visibilidad de la red.

Entre sus características se incluyen la capacidad de enrutar el tráfico de manera eficiente, mejorar la seguridad de la red y proporcionar una conectividad confiable y de alto rendimiento. Soportan una amplia gama de servicios y aplicaciones, facilitando la implementación de políticas de red basadas en la intención y mejorando la experiencia del usuario final.

Soportan alta capacidad de procesamiento de paquetes y manejan múltiples túneles de encriptación simultáneamente, mejorando la seguridad y el rendimiento de la red.

Permiten la optimización del tráfico en tiempo real e Incluyen características avanzadas de seguridad como el cifrado de extremo a extremo, firewalls integrados y capacidades de inspección profunda de paquetes (DPI). También soportan autenticación multifactor y segmentación de red para proteger los datos sensibles.

Están diseñados para proporcionar alta disponibilidad y redundancia, con capacidades de conmutación por error rápida y balanceo de carga asegurando que las aplicaciones críticas permanezcan accesibles incluso en caso de fallos de red.

Observaciones

CCN-STIC 1014 Procedimiento de Empleo Seguro Cisco Routers IOS-XE con SD-WAN

INFORMACIÓN IMPORTANTE

7.5.10 DISPOSITIVOS DE PREVENCIÓN Y DETECCIÓN DE INTRUSIONES (IDS E IPS)

Palo Alto Networks 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	
Versión	PanOs 11.2
Fabricante	Palo Alto Networks
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	17/02/2025
Revisión de Validez	31/07/2027
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

CCN-STIC-1413 Procedimiento de Empleo Seguro Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

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	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	18/11/2026
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

ISA 3000 (ISA 3000-4C y ISA 3000-2C2F)	
Versión	FTD 7.0 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	18/11/2026
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/FortiOS	
Versión	7.0
Fabricante	Fortinet
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/09/2024
Revisión de Validez	28/02/2027

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.
Modelos:
Familia F: FWF-81F-2R-3G4G-PoE, FWF-81F-2R-PoE, FG-101F, FG-201F, FG-401F, FG-601F, FG-1801F, FG-1801F-DC, FG-2601F, FG-3001F.
Familia E: FG-91E, FG-101E, FG-201E, FG-301E, FG-401E, FG-401E-DC, FG-501E, FG-601E, FG-1101E, FG-2000E, FG-2201E, FG-2500E, FG-3301E, FG-3401E, FG-3401E-DC, FG-3601E, FG-5001E1.
Familia VM: FortiGate-VM (FG-VM).

Observaciones

CCN-STIC-1406 Procedimiento de Empleo Seguro FortiGate 7.0

INFORMACIÓN IMPORTANTE

ASA 5500 Series (5508-X y 5516-X)	
Versión	FTD 7.0 y FMC/FMCv 7.0
Fabricante	Cisco Systems
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	18/11/2026

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

Firewall NSa Series (2700, 3700, 4700, 5700, 6700)

Versión	SonicOS 7.0.1
Fabricante	SonicWall
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/02/2025
Revisión de Validez	31/07/2027

Descripción

La familia de firewalls de SonicWall están diseñados para adaptarse a una amplia gama de empresas, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones, centros de datos, carriers y proveedores de servicios.
Los firewalls de SonicWall son soluciones de seguridad de capa 7 que incorporan una amplia gama de servicios avanzados para la protección de redes. Entre sus funciones destacan la prevención de intrusiones, Gateway Antivirus, Antimalware, DNS Security, Botnet Filter, GeoIP Filter, filtrado de contenido/URL y control de aplicaciones.
Además, cuentan con inspección profunda de paquetes (DPI), descifrado e inspección de tráfico TLS/SSL (incluyendo TLS 1.3), inteligencia y control de aplicaciones, SD-WAN, y tecnologías avanzadas de prevención y detección de amenazas, como la inspección profunda de memoria en tiempo real (RTDMI).
Gracias a su integración con la nube, estos firewalls permiten un análisis proactivo de amenazas y una administración centralizada, garantizando una protección integral sin afectar el rendimiento de la red.
La serie NSa de generación 7 está orientada a medianas y grandes empresas, así como a organizaciones con múltiples sucursales y centros de datos. Con hardware de alto rendimiento y conectividad de hasta 40-GbE, proporciona una capacidad ampliada para manejar entornos con mayor volumen de tráfico y necesidades avanzadas de inspección y control.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

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	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	18/11/2026
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 2100 Series (2110, 2120, 2130, 2140)	
Versión	FTD 7.0 y FMC 7.0
Fabricante	Cisco Systems
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	18/11/2026
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

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	
Versión	7.0
Fabricante	Cisco Systems
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	18/11/2026
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).

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	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	18/11/2026
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 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	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	18/11/2026

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 Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)	
Versión	7.0.6
Fabricante	Cisco Systems
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	18/11/2026
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).

La versión 7.0.6 corrige una vulnerabilidad crítica [CVE-2023-20048] detectada en la versión 7.0 inicialmente cualificada.

Observaciones

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

Deep Discovery Inspector	
Versión	6.5.1129
Fabricante	Trend Micro
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/11/2026
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

FortiGate Familias E, F y G

Versión	FortiOS 7.2
Fabricante	Fortinet
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/02/2026
Revisión de Validez	31/07/2028

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.

Modelos:

Familia E: FortiGate-60E, FortiGate-60E-PoE, FortiGate-60E-DSL, FortiWifi-60E, FortiWifi-60E-DSL, FortiWifi-60E-DSLJ, FortiGate-61E, FortiWifi-61E, FortiGate-80E, FortiGate-80E-PoE, FortiGate-81E, FortiGate-81E-PoE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-140E, FortiGate-140E-PoE, FortiGate-200E, FortiGate-201E, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-401E, FortiGate-401E-DC, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-601E, FortiGate-1100E, FortiGate-1100E-DC, FortiGate-1101E, FortiGate-1101E-DC, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3400E-DC, FortiGate-3401E, FortiGate-3401E-DC, FortiGate-3600E, FortiGate-3600E-DC, FortiGate-3601E, FortiGate-3960E, FortiGate-3960E-DC, FortiGate-3980E, FortiGate-3980E-DC, FortiGate-50001E1.

Familia F: FortiGate-40F, ,FortiGate-40F-3G4G, FortiWifi-40F, FortiWifi-40F-3G4G, FortiGate-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-60F, FortiWifi-60F, FortiGate-61F, FortiGateRugged-70F, FortiGateRugged-70F-3G4G, FortiGate-70F, FortiGate-71F, FortiGate-80F, FortiGate-80F-PoE, FortiWifi-80F-2R, FortiWifi-80F-2R-3G4G-DSL, FortiGate-81F, FortiWifi-81F-2R-3G4G-DSL, FortiGate-81F-PoE, FortiWifi-81F-2R, FortiWifi-81F-2R-3G4G-PoE, FortiWifi-81F-2R-PoE, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-200F, FortiGate-201F, FortiGate-400F, FortiGate-600F, FortiGate-601F, FortiGate-1000F, FortiGate-1001F, FortiGate-1800F, FortiGate-1800F-DC, FortiGate-1801F, FortiGate-1801F-DC, FortiGate-2600F, FortiGate-2601F, FortiGate-2601F-DC, FortiGate-3000F, FortiGate-3000F-DC, FortiGate-3001F, FortiGate-3001F-DC, FortiGate-3200F, FortiGate-3201F, FortiGate-3500F, FortiGate-35011F, FortiGate-3700F, FortiGate-3701F, FortiGate-4200F, FortiGate-4200F-DC, FortiGate-4201F, FortiGate-4201F-DC, FortiGate-4400F, FortiGate-4400F-DC, FortiGate-4401F, FortiGate-4401F-DC, FortiGate-4800F, FortiGate-4801F, FortiGate-6001F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F.

Familia G: FortiGate-30G, FortiGate-31G, FortiGate-70G, FortiGate-70G-POE, FortiGate-71G, FortiGate-71G-POE, FortiGate-90G, FortiGate-91G, FortiGate-120G, FortiGate-121G, FortiGate-200G, FortiGate-201G, FortiGate-700G, FortiGate-701G, FortiGate-900G, FortiGate-900G-DC, FortiGate-901G, FortiGate-901G-DC, FortiWifi-30G, FortiWifi-31G, FortiWifi-70G, FortiWifi-71G, FortiWifi-70G-POE.

Observaciones

CCN-STIC 1406 Procedimiento de Empleo Seguro FortiGate 7

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	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	18/11/2026
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

AWS Shield	
Versión	
Fabricante	AWS
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	18/11/2024
Revisión de Validez	31/10/2026
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

CCN-STIC 887A Guía de configuración segura AWS

INFORMACIÓN IMPORTANTE

Firewall NSsp Series (10700, 11700, 13700, 15700, 12800, 12400)	
Versión	SonicOS 7.0.1
Fabricante	SonicWall
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/02/2025
Revisión de Validez	31/07/2027

Descripción

La familia de firewalls de SonicWall están diseñados para adaptarse a una amplia gama de empresas, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones, centros de datos, carriers y proveedores de servicios.
Los firewalls de SonicWall son soluciones de seguridad de capa 7 que incorporan una amplia gama de servicios avanzados para la protección de redes. Entre sus funciones destacan la prevención de intrusiones, Gateway Antivirus, Antimalware, DNS Security, Botnet Filter, GeoIP Filter, filtrado de contenido/URL y control de aplicaciones.
Además, cuentan con inspección profunda de paquetes (DPI), descifrado e inspección de tráfico TLS/SSL (incluyendo TLS 1.3), inteligencia y control de aplicaciones, SD-WAN, y tecnologías avanzadas de prevención y detección de amenazas, como la inspección profunda de memoria en tiempo real (RTDMI).
Gracias a su integración con la nube, estos firewalls permiten un análisis proactivo de amenazas y una administración centralizada, garantizando una protección integral sin afectar el rendimiento de la red.
La serie NSSp de generación 7 responde a los requerimientos de grandes corporaciones, centros de datos, carriers y proveedores de servicios con conectividad de hasta 100-GbE,. Su plataforma de alto rendimiento permite gestionar millones de conexiones simultáneas con baja latencia, asegurando protección sin comprometer la velocidad ni la escalabilidad.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco FTD 7.4 on Cisco Secure Firewall 4200 Series with FMC-FMCv

Versión	7.4
Fabricante	Cisco Systems
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	22/04/2025
Revisión de Validez	30/11/2026

Descripción

Los Cisco FTD 7.4 en la serie Cisco Secure Firewall 4200 con FMC/FMCv están diseñados para proporcionar una defensa avanzada contra amenazas y una gestión centralizada de la seguridad.
Estos firewalls combinan capacidades de inspección profunda de paquetes (DPI) con la inteligencia de amenazas de Cisco Talos, ofreciendo una protección robusta contra ataques conocidos y desconocidos.
La serie 4200 está optimizada para un rendimiento alto y una baja latencia, soportando hasta 100 Gbps de rendimiento de firewall. Con la versión 7.4, se introducen mejoras en la gestión de políticas y la visibilidad de la red, facilitando la administración de grandes entornos de seguridad. Además, la integración con Cisco SecureX permite una respuesta rápida y coordinada a incidentes de seguridad.
El Cisco Firepower Management Center (FMC) y su versión virtual (FMCv) proporcionan una plataforma centralizada para la gestión de políticas, la monitorización de eventos y la generación de informes detallados. Estas herramientas permiten una administración eficiente y una visibilidad completa de la postura de seguridad de la red.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco FTD 7.4 on Firepower 1000 Series with FMC-FMCv

Versión	7.4
Fabricante	Cisco Systems
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	22/04/2025
Revisión de Validez	30/11/2026

Descripción

Los Cisco FTD 7.4 en la serie Firepower 1000 con FMC/FMCv están diseñados para ofrecer una protección avanzada contra amenazas y una gestión centralizada de la seguridad.
Estos firewalls combinan capacidades de inspección profunda de paquetes (DPI) con la inteligencia de amenazas de Cisco Talos, proporcionando una defensa robusta contra ataques conocidos y desconocidos.
La serie Firepower 1000 está optimizada para un rendimiento eficiente en entornos de pequeñas y medianas empresas, soportando hasta 8 Gbps de rendimiento de firewall2. Con la versión 7.4, se mejoran las capacidades de gestión de políticas y visibilidad de la red, facilitando la administración de la seguridad en entornos complejos. Además, la integración con Cisco SecureX permite una respuesta rápida y coordinada a incidentes de seguridad.
El Cisco Firepower Management Center (FMC) y su versión virtual (FMCv) proporcionan una plataforma centralizada para la gestión de políticas, la monitorización de eventos y la generación de informes detallados. Estas herramientas permiten una administración eficiente y una visibilidad completa de la postura de seguridad de la red.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

TippingPoint Threat Protection System

Versión	5.5.5
Fabricante	Trend Micro
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/11/2026

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

Cisco Firepower Threat Defense (FTD) on Cisco Secure Firewall 3100 Series with FMC/FMCv	
Versión	7.4
Fabricante	Cisco Systems
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	27/02/2025
Revisión de Validez	31/07/2027
Descripción	

Cisco FTD 7.4 (Firepower Threat Defense) es una solución de seguridad que combina capacidades de firewall de próxima generación (NGFW) y sistema de prevención de intrusiones (IPS).
En esta versión se incluyen mejoras en la detección de amenazas, bloqueo de malware en sesiones TLS cifradas y acceso a aplicaciones sin cliente para una postura de seguridad Zero Trust1.
Puede desplegarse como un dispositivo único o en modo multi-instancia, lo que permite ejecutar múltiples instancias independientes de FTD en el mismo hardware.
FMC (Firepower Management Center): Es la plataforma de gestión centralizada para soluciones de seguridad de Cisco. Permite la administración, monitoreo y análisis de las políticas de seguridad y eventos de red en tiempo real.
FMCv (Firepower Management Center Virtual): Es la versión virtualizada del FMC, que ofrece las mismas capacidades de gestión y análisis, pero está diseñada para entornos virtuales y de nube..

Observaciones

CCN-STIC 651B Procedimiento de Empleo Seguro Cortafuegos Cisco Secure Firewall

Nozomi Networks NS1 Guardian Appliance	
Versión	N2OS 24.2.0
Fabricante	Nozomi Networks
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	11/02/2025
Revisión de Validez	31/07/2027
Descripción	

NS1 Guardian es una solución para la seguridad y visibilidad en entornos OT, IoT y TI. Protege infraestructuras críticas con detección avanzada de amenazas y gestión de vulnerabilidades. Proporciona monitorización continua, análisis de riesgos y detección de anomalías, combinando técnicas basadas en comportamiento y firmas. Al integrarse con firewalls y herramientas de seguridad permite respuestas rápidas y efectivas ante anomalías y ataques. Empleando Threat Intelligence y Asset Intelligence ofrece inteligencia actualizada sobre amenazas y dispositivos proporcionando alertas precisas.

Observaciones

CCN-STIC 1306. Procedimiento de Empleo Seguro N2OS

INFORMACIÓN IMPORTANTE

Firewall NSv Series (270, 470, 870)

Versión	SonicOS 7.0.1
Fabricante	SonicWall
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/02/2025
Revisión de Validez	31/07/2027

Descripción

La familia de firewalls de SonicWall están diseñados para adaptarse a una amplia gama de empresas, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones, centros de datos, carriers y proveedores de servicios.
Los firewalls de SonicWall son soluciones de seguridad de capa 7 que incorporan una amplia gama de servicios avanzados para la protección de redes. Entre sus funciones destacan la prevención de intrusiones, Gateway Antivirus, Antimalware, DNS Security, Botnet Filter, GeoIP Filter, filtrado de contenido/URL y control de aplicaciones.
Además, cuentan con inspección profunda de paquetes (DPI), descifrado e inspección de tráfico TLS/SSL (incluyendo TLS 1.3), inteligencia y control de aplicaciones, SD-WAN, y tecnologías avanzadas de prevención y detección de amenazas, como la inspección profunda de memoria en tiempo real (RTDMI).
Gracias a su integración con la nube, estos firewalls permiten un análisis proactivo de amenazas y una administración centralizada, garantizando una protección integral sin afectar el rendimiento de la red.
La serie NSv de generación 7 extiende la protección de SonicWall a entornos virtualizados en nubes públicas y privadas. Diseñada para arquitecturas híbridas y totalmente en la nube, ofrece la misma seguridad que un firewall físico con la flexibilidad necesaria para adaptarse a infraestructuras dinámicas y escalables.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Firewall TZ Series (270, 270W, 370, 330W, 470, 470W, 570, 570W, 570POE, 670)	
Versión	SonicOS 7.0.1
Fabricante	SonicWall
Familia	Dispositivos de prevención y detección de intrusiones (IDS e IPS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/02/2025
Revisión de Validez	31/07/2027

Descripción

La familia de firewalls de SonicWall están diseñados para adaptarse a una amplia gama de empresas, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones, centros de datos, carriers y proveedores de servicios.
Los firewalls de SonicWall son soluciones de seguridad de capa 7 que incorporan una amplia gama de servicios avanzados para la protección de redes. Entre sus funciones destacan la prevención de intrusiones, Gateway Antivirus, Antimalware, DNS Security, Botnet Filter, GeoIP Filter, filtrado de contenido/URL y control de aplicaciones.
Además, cuentan con inspección profunda de paquetes (DPI), descifrado e inspección de tráfico TLS/SSL (incluyendo TLS 1.3), inteligencia y control de aplicaciones, SD-WAN, y tecnologías avanzadas de prevención y detección de amenazas, como la inspección profunda de memoria en tiempo real (RTDMI).
Gracias a su integración con la nube, estos firewalls permiten un análisis proactivo de amenazas y una administración centralizada, garantizando una protección integral sin afectar el rendimiento de la red.
La serie TZ de generación 7 de está diseñada para pequeñas empresas y entornos departamentales que requieren seguridad avanzada con una gestión sencilla. Su arquitectura compacta ofrece un equilibrio entre rendimiento y protección, permitiendo implementar soluciones de seguridad de nivel empresarial en redes cableadas, con conectividad de hasta 10-GbE e inalámbricas, y con una fácil administración.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.5.11 PROTECCIÓN DE CORREO ELECTRÓNICO

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	30/11/2026

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

CCN-STIC 1647 Procedimiento de Empleo Seguro Harmony Email & Collaboration

INFORMACIÓN IMPORTANTE

Trend Micro Vision One Email and Collaboration Security

Versión	
Fabricante	Trend Micro
Familia	Protección de correo electrónico
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	24/07/2025
Revisión de Validez	30/06/2027

Descripción

Vision One – Email and Collaboration Security, es la propuesta de Trend Micro para proteger Entornos de Correo electrónico y colaborativos independientemente de su ubicación (nube/Onpremise) o tecnología empleada.
Forma parte de la plataforma de Ciberseguridad Empresarial Trend Vision One y brinda en 2 capas complementarias de seguridad:
Transporte MTA:
Donde se integra en el flujo de correo SMTP entrante y/o saliente del cliente proporcionando seguridad robusta a nivel de conexión, transporte, contenido y comportamiento antes de que el correo sea entregado en su destino.
Integración API:
La cual se integra a nivel de API con distintos productos y servicios de correo y colaborativos: Microsoft 365 (Exchange Online (modo Inline/Online), SharePoint, OneDrive, Teams), Microsoft Exchange, Google Workspace (Modo Inline/Online), Box y Dropbox. Permitiendo un análisis y protección del correo entrante, saliente y correo interno así como los distintos flujos de información asociados a los entornos colaborativos.
Todo lo anterior proporcionado de manera activa o en modo monitorización y alimentando la telemetría XDR y de gestión del riesgo proporcionadas por Trend Vision One

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	31/12/2027

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

CCN-STIC 1614 Procedimiento de Empleo Seguro FortiMail

Proofpoint Email Protection & Targeted Email Protection

Versión	
Fabricante	Proofpoint
Familia	Protección de correo electrónico
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/11/2026

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

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	30/11/2026

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

CCN-STIC 1655. Procedimiento de Empleo Seguro Email Guardian

INFORMACIÓN IMPORTANTE

7.5.12 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
Familia	Balanceadores de carga
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/06/2027

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

i4000, i5000, i7000, i10000, i11000-DS, i15000, I15000-DF, VIPRION C2400/B2250, C4480/B4450, r4000, R5000, R10000, VELOS BX110/CX410, BIP-IP Virtual Edition	
Versión	F5 BIG-IP 17.1.0.1
Fabricante	F5
Familia	Balanceadores de carga
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	14/01/2025
Revisión de Validez	30/06/2027

Descripción

F5 BIG-IP es una herramienta clave en la publicación y entrega de aplicaciones, optimizando su disponibilidad, velocidad y fiabilidad a través de las capas de aplicación y red. Como dispositivo full-proxy, inspecciona, gestiona y da visibilidad al tráfico entrante y saliente de las aplicaciones corporativas. Proporciona desde balanceo de carga hasta decisiones avanzadas de gestión de tráfico basadas en cliente, servidor o estado de la aplicación, lo que permite distribuir usuarios de forma inteligente hacia los servidores. Totalmente programable y granular, se adapta a necesidades actuales y futuras de control de tráfico, mejorando el tiempo de respuesta y la experiencia de los usuarios. Además, en su configuración de firewall, BIG-IP actúa como solución de seguridad perimetral en centros de datos, protegiendo las capas 3 y 4 con políticas avanzadas y defensa frente a ataques de denegación de servicio distribuidos. Su interfaz de gestión intuitiva, con reportes y analíticas, ofrece una visión completa del estado de seguridad del perímetro de red y asegura la protección de los recursos críticos.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

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
Familia	Balanceadores de carga
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/06/2027

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

7.6 PROTECCIÓN DE LAS COMUNICACIONES

7.6.1 HERRAMIENTAS VOZ IP

COMSec Admin +	
Versión	v5.1
Fabricante	Indra
Familia	Herramientas Voz IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2026
Revisión de Validez	31/10/2026

Descripción

COMSec Admin + es una solución global de comunicaciones seguras que proporciona servicios cifrados resistentes a computación cuántica con mecanismos de hibridación de criptografía clásica y PQC en el ámbito de voz, mensajería instantánea y videollamada sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con 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 Admin + son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: www.indragroup.com

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Secret.T (iOS)

Versión	1.18
Fabricante	Telefónica Soluciones de Criptografía
Familia	Herramientas Voz IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/08/2027

Descripción

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

Secret.T (Android)

Versión	1.15
Fabricante	Telefónica Soluciones de Criptografía
Familia	Herramientas Voz IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	24/03/2025
Revisión de Validez	30/08/2027

Descripción

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco Unified Communications Manager (C220 M5 y C240 M5)	
Versión	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	31/10/2026

Descripción

Sistema de comunicaciones empresarial que suministra voz y videollamadas sobre una red IP.

Observaciones

CCN-STIC-1460 PES Cisco Unified Communications Manager

INFORMACIÓN IMPORTANTE

7.6.2 HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA (IM)

COMSec Admin +

Versión	v5.1
Fabricante	Indra
Familia	Herramientas de mensajería instantánea (IM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2026
Revisión de Validez	31/10/2026

Descripción

COMSec Admin + es una solución global de comunicaciones seguras que proporciona servicios cifrados resistentes a computación cuántica con mecanismos de hibridación de criptografía clásica y PQC en el ámbito de voz, mensajería instantánea y videollamada sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con 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 Admin + son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: www.indragroup.com

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Secret.T (iOS)

Versión	1.18
Fabricante	Telefónica Soluciones de Criptografía
Familia	Herramientas de mensajería instantánea (IM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/08/2027

Descripción

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

Secret.T (Android)

Versión	1.15
Fabricante	Telefónica Soluciones de Criptografía
Familia	Herramientas de mensajería instantánea (IM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	24/03/2025
Revisión de Validez	30/08/2027

Descripción

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

7.6.3 HERRAMIENTAS DE VIDEOCONFERENCIA

Pexip Infinity	
Versión	v.36.2
Fabricante	PEXIP
Familia	Herramientas de videoconferencia
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	26/03/2025
Revisión de Validez	31/08/2027

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

Secret.T (iOS)

Versión	1.18
Fabricante	Telefónica Soluciones de Criptografía
Familia	Herramientas de videoconferencia
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/08/2027

Descripción

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

Secret.T (Android)

Versión	1.15
Fabricante	Telefónica Soluciones de Criptografía
Familia	Herramientas de videoconferencia
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	24/03/2025
Revisión de Validez	30/08/2027

Descripción

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

7.6.4 REDES PRIVADAS VIRTUALES: IPSEC

Palo Alto Networks 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	
Versión	PanOs 11.2
Fabricante	Palo Alto Networks
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	17/02/2025
Revisión de Validez	31/07/2027

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

CCN-STIC-1413 Procedimiento de Empleo Seguro Cortafuegos NGFW Palo Alto Networks

Cisco Secure Client - AnyConnect 5.1 para Red Hat Enterprise Linux 8.2.	
Versión	v5.1
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/09/2024
Revisión de Validez	30/09/2027

Descripción

El Cisco AnyConnect 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

CCN-STIC 1448 Procedimiento de Empleo Seguro Cisco Secure AnyConnect

INFORMACIÓN IMPORTANTE

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	18/11/2026
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

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	18/11/2026
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/FortiOS	
Versión	7.0
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/09/2024
Revisión de Validez	28/02/2027

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.
Modelos:
Familia F: FWF-81F-2R-3G4G-PoE, FWF-81F-2R-PoE, FG-101F, FG-201F, FG-401F, FG-601F, FG-1801F, FG-1801F-DC, FG-2601F, FG-3001F.
Familia E: FG-91E, FG-101E, FG-201E, FG-301E, FG-401E, FG-401E-DC, FG-501E, FG-601E, FG-1101E, FG-2000E, FG-2201E, FG-2500E, FG-3301E, FG-3401E, FG-3401E-DC, FG-3601E, FG-5001E1.
Familia VM: FortiGate-VM (FG-VM).

Observaciones

CCN-STIC-1406 Procedimiento de Empleo Seguro FortiGate 7.0

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	18/11/2026

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

Firewall NSa Series (2700, 3700, 4700, 5700, 6700)

Versión	SonicOS 7.0.1
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/02/2025
Revisión de Validez	31/07/2027

Descripción

La familia de firewalls de SonicWall están diseñados para adaptarse a una amplia gama de empresas, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones, centros de datos, carriers y proveedores de servicios.
Los firewalls de SonicWall son soluciones de seguridad de capa 7 que incorporan una amplia gama de servicios avanzados para la protección de redes. Entre sus funciones destacan la prevención de intrusiones, Gateway Antivirus, Antimalware, DNS Security, Botnet Filter, GeoIP Filter, filtrado de contenido/URL y control de aplicaciones.
Además, cuentan con inspección profunda de paquetes (DPI), descifrado e inspección de tráfico TLS/SSL (incluyendo TLS 1.3), inteligencia y control de aplicaciones, SD-WAN, y tecnologías avanzadas de prevención y detección de amenazas, como la inspección profunda de memoria en tiempo real (RTDMI).
Gracias a su integración con la nube, estos firewalls permiten un análisis proactivo de amenazas y una administración centralizada, garantizando una protección integral sin afectar el rendimiento de la red.
La serie NSa de generación 7 está orientada a medianas y grandes empresas, así como a organizaciones con múltiples sucursales y centros de datos. Con hardware de alto rendimiento y conectividad de hasta 40-GbE, proporciona una capacidad ampliada para manejar entornos con mayor volumen de tráfico y necesidades avanzadas de inspección y control.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

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	18/11/2026

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 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	18/11/2026

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

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	
Versión	7.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	18/11/2026
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).

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	18/11/2026
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 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	18/11/2026

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 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	18/11/2026

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

Firewall NSsp Series (10700, 11700, 13700, 15700, 12800, 12400)

Versión	SonicOS 7.0.1
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/02/2025
Revisión de Validez	31/07/2027

Descripción

La familia de firewalls de SonicWall están diseñados para adaptarse a una amplia gama de empresas, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones, centros de datos, carriers y proveedores de servicios.
Los firewalls de SonicWall son soluciones de seguridad de capa 7 que incorporan una amplia gama de servicios avanzados para la protección de redes. Entre sus funciones destacan la prevención de intrusiones, Gateway Antivirus, Antimalware, DNS Security, Botnet Filter, GeoIP Filter, filtrado de contenido/URL y control de aplicaciones.
Además, cuentan con inspección profunda de paquetes (DPI), descifrado e inspección de tráfico TLS/SSL (incluyendo TLS 1.3), inteligencia y control de aplicaciones, SD-WAN, y tecnologías avanzadas de prevención y detección de amenazas, como la inspección profunda de memoria en tiempo real (RTDMI).
Gracias a su integración con la nube, estos firewalls permiten un análisis proactivo de amenazas y una administración centralizada, garantizando una protección integral sin afectar el rendimiento de la red.
La serie NSSp de generación 7 responde a los requerimientos de grandes corporaciones, centros de datos, carriers y proveedores de servicios con conectividad de hasta 100-GbE,. Su plataforma de alto rendimiento permite gestionar millones de conexiones simultáneas con baja latencia, asegurando protección sin comprometer la velocidad ni la escalabilidad.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

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	30/09/2027

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

CCN-STIC 1449 Procedimiento de Empleo Seguro Cisco Secure Client (AnyConnect) for iOS16

Cisco FTD 7.4 on Cisco Secure Firewall 4200 Series with FMC-FMCv

Versión	7.4
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	22/04/2025
Revisión de Validez	30/11/2026

Descripción

Los Cisco FTD 7.4 en la serie Cisco Secure Firewall 4200 con FMC/FMCv están diseñados para proporcionar una defensa avanzada contra amenazas y una gestión centralizada de la seguridad.
Estos firewalls combinan capacidades de inspección profunda de paquetes (DPI) con la inteligencia de amenazas de Cisco Talos, ofreciendo una protección robusta contra ataques conocidos y desconocidos.
La serie 4200 está optimizada para un rendimiento alto y una baja latencia, soportando hasta 100 Gbps de rendimiento de firewall. Con la versión 7.4, se introducen mejoras en la gestión de políticas y la visibilidad de la red, facilitando la administración de grandes entornos de seguridad. Además, la integración con Cisco SecureX permite una respuesta rápida y coordinada a incidentes de seguridad.
El Cisco Firepower Management Center (FMC) y su versión virtual (FMCv) proporcionan una plataforma centralizada para la gestión de políticas, la monitorización de eventos y la generación de informes detallados. Estas herramientas permiten una administración eficiente y una visibilidad completa de la postura de seguridad de la red.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco FTD 7.4 on Firepower 1000 Series with FMC-FMCv

Versión	7.4
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	22/04/2025
Revisión de Validez	30/11/2026

Descripción

Los Cisco FTD 7.4 en la serie Firepower 1000 con FMC/FMCv están diseñados para ofrecer una protección avanzada contra amenazas y una gestión centralizada de la seguridad.
Estos firewalls combinan capacidades de inspección profunda de paquetes (DPI) con la inteligencia de amenazas de Cisco Talos, proporcionando una defensa robusta contra ataques conocidos y desconocidos.
La serie Firepower 1000 está optimizada para un rendimiento eficiente en entornos de pequeñas y medianas empresas, soportando hasta 8 Gbps de rendimiento de firewall2. Con la versión 7.4, se mejoran las capacidades de gestión de políticas y visibilidad de la red, facilitando la administración de la seguridad en entornos complejos. Además, la integración con Cisco SecureX permite una respuesta rápida y coordinada a incidentes de seguridad.
El Cisco Firepower Management Center (FMC) y su versión virtual (FMCv) proporcionan una plataforma centralizada para la gestión de políticas, la monitorización de eventos y la generación de informes detallados. Estas herramientas permiten una administración eficiente y una visibilidad completa de la postura de seguridad de la red.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

HPE Aruba Networking Orchestrator and EdgeConnect Release

Versión	9.4.2
Fabricante	HPE Aruba Networking
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/04/2025
Revisión de Validez	31/10/2026

Descripción

Los productos incluidos en esta cualificación son los pertenecientes a las familias EC-101XX, EC-S-P y EC-M-H.
La solución EdgeConnect SD-WAN de HPE Aruba Networking permite desplegar redes SD-WAN seguras de cualquier tamaño, tanto locales como internacionales mediante el uso de diversas topologías como hub&spoke, mesh o regionales. La solución SD-WAN permite construir múltiples overlays con políticas diferenciadas de gestión de los enlaces y topologías específicas dependiendo del tipo de tráfico. EdgeConnect permite una gestión de enlaces muy avanzada que incluye balanceo por paquete y dynamic path control lo que permite ofrecer al usuario conexiones agregadas de alta capacidad y calidad incluso utilizando enlaces degradados. La solución EdgeConnect introduce múltiples funcionalidades de seguridad como VRFs, statefull firewall con zonas e IDS/IPS. La solución SD-WAN de Aruba ofrece funcionalidades de optimización WAN mediante aceleración de protocolo TCP y reducción de datos mediante compresión y deduplicación. EdgeConnect SD-WAN permite la integración con múltiples proveedores de seguridad SSE lo que permite, mediante el uso de políticas específicas, derivar el tráfico a los diferentes proveedores de seguridad

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

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	30/09/2027

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 Procedimiento de Empleo Seguro Cisco Secure AnyConnect

INFORMACIÓN IMPORTANTE

FortiGate - VPN

Versión	FortiOS 7.2
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	30/03/2026
Revisión de Validez	31/07/2028

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.
Modelos:

Familia E: FortiGate-60E, FortiGate-60E-PoE, FortiGate-60E-DSL, FortiWifi-60E, FortiWifi-60E-DSL, FortiWifi-60E-DSLJ, FortiGate-61E, FortiWifi-61E, FortiGate-80E, FortiGate-80E-PoE, FortiGate-81E, FortiGate-81E-PoE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-140E, FortiGate-140E-PoE, FortiGate-200E, FortiGate-201E, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-401E, FortiGate-401E-DC, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-601E, FortiGate-1100E, FortiGate-1100E-DC, FortiGate-1101E, FortiGate-1101E-DC, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3400E-DC, FortiGate-3401E, FortiGate-3401E-DC, FortiGate-3600E, FortiGate-3600E-DC, FortiGate-3601E, FortiGate-3960E, FortiGate-3960E-DC, FortiGate-3980E, FortiGate-3980E-DC, FortiGate-50001E1.

Familia F: FortiGate-40F, ,FortiGate-40F-3G4G, FortiWifi-40F, FortiWifi-40F-3G4G, FortiGate-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-60F, FortiWifi-60F, FortiGate-61F, FortiGateRugged-70F, FortiGateRugged-70F-3G4G, FortiGate-70F, FortiGate-71F, FortiGate-80F, FortiGate-80F-PoE, FortiWifi-80F-2R, FortiWifi-80F-2R-3G4G-DSL, FortiGate-81F, FortiWifi-81F-2R-3G4G-DSL, FortiGate-81F-PoE, FortiWifi-81F-2R, FortiWifi-81F-2R-3G4G-PoE, FortiWifi-81F-2R-PoE, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-200F, FortiGate-201F, FortiGate-400F, FortiGate-600F, FortiGate-601F, FortiGate-1000F, FortiGate-1001F, FortiGate-1800F, FortiGate-1800F-DC, FortiGate-1801F, FortiGate-1801F-DC, FortiGate-2600F, FortiGate-2601F, FortiGate-2601F-DC, FortiGate-3000F, FortiGate-3000F-DC, FortiGate-3001F, FortiGate-3001F-DC, FortiGate-3200F, FortiGate-3201F, FortiGate-3500F, FortiGate-35011F, FortiGate-3700F, FortiGate-3701F, FortiGate-4200F, FortiGate-4200F-DC, FortiGate-4201F, FortiGate-4201F-DC, FortiGate-4400F, FortiGate-4400F-DC, FortiGate-4401F, FortiGate-4401F-DC, FortiGate-4800F, FortiGate-4801F, FortiGate-6001F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F.

Familia G: FortiGate-30G, FortiGate-31G, FortiGate-70G, FortiGate-70G-POE, FortiGate-71G, FortiGate-71G-POE, FortiGate-90G, FortiGate-91G, FortiGate-120G, FortiGate-121G, FortiGate-200G, FortiGate-201G, FortiGate-700G, FortiGate-701G, FortiGate-900G, FortiGate-900G-DC, FortiGate-901G, FortiGate-901G-DC, FortiWifi-30G, FortiWifi-31G, FortiWifi-70G, FortiWifi-71G, FortiWifi-70G-POE.

Observaciones

CCN-STIC 1406 Procedimiento de Empleo Seguro FortiGate 7

INFORMACIÓN IMPORTANTE

Cisco Firepower Threat Defense (FTD) on Cisco Secure Firewall 3100 Series with FMC/FMCv

Versión	7.4
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	27/02/2025
Revisión de Validez	31/07/2027

Descripción

Cisco FTD 7.4 (Firepower Threat Defense) es una solución de seguridad que combina capacidades de firewall de próxima generación (NGFW) y sistema de prevención de intrusiones (IPS).
En esta versión se incluyen mejoras en la detección de amenazas, bloqueo de malware en sesiones TLS cifradas y acceso a aplicaciones sin cliente para una postura de seguridad Zero Trust1.
Puede desplegarse como un dispositivo único o en modo multi-instancia, lo que permite ejecutar múltiples instancias independientes de FTD en el mismo hardware.
FMC (Firepower Management Center): Es la plataforma de gestión centralizada para soluciones de seguridad de Cisco. Permite la administración, monitoreo y análisis de las políticas de seguridad y eventos de red en tiempo real.
FMCv (Firepower Management Center Virtual): Es la versión virtualizada del FMC, que ofrece las mismas capacidades de gestión y análisis, pero está diseñada para entornos virtuales y de nube..

Observaciones

CCN-STIC 651B Procedimiento de Empleo Seguro Cortafuegos Cisco Secure Firewall

Aruba Mobility Controller (9004, 9012, 9240, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) y puntos de acceso (serie 200, 300, 500 y 600)_

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	13/04/2027

Descripción

Los HPE Aruba Mobility Controllers, junto con los APs de las series 200, 300, 500 y 600, permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan características de seguridad avanzadas en el control de acceso a la red, en la asignación de políticas de seguridad por usuario mediante el uso de roles, así como la posibilidad de despliegues multizona y terminación de túneles VPN. También se soportan mecanismos de monitorización de espectro y wireless IDS/IPS.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS Controladoras y Puntos de Acceso

INFORMACIÓN IMPORTANTE

Aruba Virtual Mobility Controllers (MC-VA-50, MC-VA-250 y MC-VA-1k) y puntos de acceso (serie 200, 300, 500 y 600)_

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	13/04/2027

Descripción

Los HPE Aruba Mobility Controllers, junto con los APs de las series 200, 300, 500 y 600, permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan características de seguridad avanzadas en el control de acceso a la red, en la asignación de políticas de seguridad por usuario mediante el uso de roles, así como la posibilidad de despliegues multizona y terminación de túneles VPN. También se soportan mecanismos de monitorización de espectro y wireless IDS/IPS.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS Controladoras y Puntos de Acceso

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

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	30/11/2026

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

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

Firewall NSv Series (270, 470, 870)

Versión	SonicOS 7.0.1
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/02/2025
Revisión de Validez	31/07/2027

Descripción

La familia de firewalls de SonicWall están diseñados para adaptarse a una amplia gama de empresas, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones, centros de datos, carriers y proveedores de servicios.
Los firewalls de SonicWall son soluciones de seguridad de capa 7 que incorporan una amplia gama de servicios avanzados para la protección de redes. Entre sus funciones destacan la prevención de intrusiones, Gateway Antivirus, Antimalware, DNS Security, Botnet Filter, GeoIP Filter, filtrado de contenido/URL y control de aplicaciones.
Además, cuentan con inspección profunda de paquetes (DPI), descifrado e inspección de tráfico TLS/SSL (incluyendo TLS 1.3), inteligencia y control de aplicaciones, SD-WAN, y tecnologías avanzadas de prevención y detección de amenazas, como la inspección profunda de memoria en tiempo real (RTDMI).
Gracias a su integración con la nube, estos firewalls permiten un análisis proactivo de amenazas y una administración centralizada, garantizando una protección integral sin afectar el rendimiento de la red.
La serie NSv de generación 7 extiende la protección de SonicWall a entornos virtualizados en nubes públicas y privadas. Diseñada para arquitecturas híbridas y totalmente en la nube, ofrece la misma seguridad que un firewall físico con la flexibilidad necesaria para adaptarse a infraestructuras dinámicas y escalables.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Firewall TZ Series (270, 270W, 370, 330W, 470, 470W, 570, 570W, 570POE, 670)

Versión	SonicOS 7.0.1
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/02/2025
Revisión de Validez	31/07/2027

Descripción

La familia de firewalls de SonicWall están diseñados para adaptarse a una amplia gama de empresas, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones, centros de datos, carriers y proveedores de servicios.
Los firewalls de SonicWall son soluciones de seguridad de capa 7 que incorporan una amplia gama de servicios avanzados para la protección de redes. Entre sus funciones destacan la prevención de intrusiones, Gateway Antivirus, Antimalware, DNS Security, Botnet Filter, GeoIP Filter, filtrado de contenido/URL y control de aplicaciones.
Además, cuentan con inspección profunda de paquetes (DPI), descifrado e inspección de tráfico TLS/SSL (incluyendo TLS 1.3), inteligencia y control de aplicaciones, SD-WAN, y tecnologías avanzadas de prevención y detección de amenazas, como la inspección profunda de memoria en tiempo real (RTDMI).
Gracias a su integración con la nube, estos firewalls permiten un análisis proactivo de amenazas y una administración centralizada, garantizando una protección integral sin afectar el rendimiento de la red.
La serie TZ de generación 7 de está diseñada para pequeñas empresas y entornos departamentales que requieren seguridad avanzada con una gestión sencilla. Su arquitectura compacta ofrece un equilibrio entre rendimiento y protección, permitiendo implementar soluciones de seguridad de nivel empresarial en redes cableadas, con conectividad de hasta 10-GbE e inalámbricas, y con una fácil administración.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.6.5 REDES PRIVADAS VIRTUALES: TLS

Cisco Secure Client - AnyConnect para Windows 10	
Versión	5.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: TLS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2024
Revisión de Validez	30/09/2027

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

CCN-STIC 1448 Procedimiento de Empleo Seguro Cisco Secure AnyConnect

Ivanti Connect Secure (ICS)

Versión	22.7R2
Fabricante	Ivanti
Familia	Redes privadas virtuales: TLS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	30/06/2026
Revisión de Validez	30/11/2026

Descripción

Ivanti Connect Secure (ICS) es una pasarela VPN de acceso seguro que proporciona conectividad remota autenticada y cifrada mediante protocolos criptográficos estándar del sector. Es compatible con TLS 1.2 y TLS 1.3 con conjuntos de cifrado configurables, lo que permite un cifrado sólido, confidencialidad hacia adelante y autenticación basada en certificados. La aplicación obligatoria de TLS 1.3 garantiza el uso de algoritmos criptográficos modernos, mientras que los protocolos heredados pueden desactivarse por motivos de cumplimiento normativo. La solución utiliza certificados digitales, validación de integridad HMAC y gestión segura de claves para garantizar la confidencialidad y la integridad de las comunicaciones.

ICS se ejecuta en un sistema reforzado basado en Linux con SELinux habilitado en modo de aplicación por defecto, lo que proporciona un control de acceso obligatorio y restringe los procesos al mínimo privilegio. Está disponible para entornos locales, virtuales (VMware, Hyper-V, OpenStack) y en la nube (AWS, Azure, GCP), y admite clientes en las plataformas Windows, macOS, Linux, iOS y Android a través de Ivanti Secure Access Client y la gestión de acceso basada en navegador. Entre sus funciones principales se incluyen el acceso mediante VPN SSL, el control de acceso basado en roles, la integración AAA, el cumplimiento normativo de los terminales (Host Checker) y el acceso seguro a aplicaciones a través de redes no fiables.

Observaciones

Procedimiento de Empleo Pendiente de publicación

INFORMACIÓN IMPORTANTE

7.6.6 REDES PRIVADAS VIRTUALES: OTRAS

EP960	
Versión	1.09.17
Fabricante	Epicom
Familia	Redes privadas virtuales: Otras
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	31/12/2026



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

7.7 PROTECCIÓN DE LA INFORMACIÓN

7.7.1 ALMACENAMIENTO CIFRADO DE DATOS

Cryhod.gob.es	
Versión	2024.4
Fabricante	PrimX/Epicom
Familia	Almacenamiento cifrado de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	17/02/2025
Revisión de Validez	31/07/2027

Descripción

Cryhod.gob.es es un programa de cifrado moderno que asegura el cifrado completo de los discos duros de las estaciones de trabajo de la organización con criptografía específica para la Administración española tanto local, como autonómica o general. Cryhod.gob.es, al igual que Cryhod, implementa mecanismos 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. Es especialmente recomendable su uso en sistemas sensibles (ENS ALTO) o que manejen información clasificada.

Observaciones

CCN-STIC-1523 Procedimiento de Empleo Seguro Cryhod .DEF y .GOB de PRIM'x personalizado por EPICOM

Cryhod.def.es	
Versión	2024.4
Fabricante	PrimX/Epicom
Familia	Almacenamiento cifrado de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	17/02/2025
Revisión de Validez	31/07/2027

Descripción

Cryhod.def.es es un programa de cifrado moderno que asegura el cifrado completo de los discos duros de las estaciones de trabajo de la organización con criptografía específica para el Ministerio de Defensa y organismos dependientes. Cryhod.def.es, al igual que Cryhod, implementa mecanismos 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. Es especialmente recomendable su uso en sistemas sensibles (ENS ALTO) o que manejen información clasificada.

Observaciones

CCN-STIC-1523 Procedimiento de Empleo Seguro Cryhod .DEF y .GOB de PRIM'x personalizado por EPICOM

INFORMACIÓN IMPORTANTE

ZONE CENTRAL

Versión	Q.2023.2
Fabricante	PRIMX
Familia	Almacenamiento cifrado de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2023
Revisión de Validez	30/11/2026

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

CCN-STIC 1512 Procedimiento de Empleo Seguro ZONECENTRAL de PRIMX

CRYHOD

Versión	Q.2023.2
Fabricante	PRIMX
Familia	Almacenamiento cifrado de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2023
Revisión de Validez	30/09/2028

Descripción

Cryhod es un programa de cifrado moderno que asegura el cifrado completo de los discos duros de las estaciones de trabajo de la organización. Cryhod implementa mecanismos 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

INFORMACIÓN IMPORTANTE

7.7.2 CIFRADO Y COMPARTICIÓN SEGURA DE INFORMACIÓN

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	3.05
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2026
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

ZED!

Versión	Q.2023
Fabricante	PRIMX
Familia	Cifrado y compartición segura de información
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2026
Revisión de Validez	30/09/2028

Descripción

Solución de protección de la información basada en contenedores cifrados que permite almacenar y transportar archivos de forma segura mediante el uso de mecanismos criptográficos. Proporciona confidencialidad de los datos durante su intercambio y almacenamiento temporal, controlando el acceso a la información protegida y contribuyendo a reducir el riesgo de exposición, modificación o acceso no autorizado durante su distribución entre usuarios, sistemas u organizaciones.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

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	19/12/2027

Descripción

GuardedBox es una solución para almacenamiento e intercambio seguro en tiempo real de todo tipo de información sensible (secretos) mediante cifrado extremo a extremo (E2E) con total confidencialidad, trazabilidad, privacidad y control para los usuarios y la organización.
Permite la protección, envío, distribución y compartición de secretos de manera individual o colaborativa (grupos), tanto con usuarios internos como externos a la organización, incluyendo ficheros de tamaño ilimitado. Ofrece capacidades de control (estado actual e histórico de compartición, notificaciones, recordatorios, etc.). El panel de administración permite la gestión avanzada de usuarios y proporciona un módulo de auditoría inmutable (blockchain) con los eventos detallados de actividad. Su diseño (API) permite la personalización e integración con otras soluciones del entorno (SSO, logging, SIEM, etc.). Su esquema flexible de plantillas personalizables permite modelizar cualquier tipo de dato (gestión de contraseñas, credenciales, certificados, claves, archivos, documentos, informes, auditorías, grabaciones, logs, evidencias, historias clínicas, etc.), adaptándose a las necesidades de la organización.
GuardedBox es una solución web online escalable en modo SaaS disponible para despliegues privados on-premise o en nube, pública o privada, con todas las modalidades certificadas en cumplimiento con el ENS en categoría ALTA para las 5 dimensiones de seguridad. Implementa férreas medidas de zero-knowledge y zero-trust que protegen los datos frente a compromisos del servidor. Más información: https://guardedbox.es

Observaciones

CCN-STIC 1509 Procedimiento de empleo seguro Guardedbox

INFORMACIÓN IMPORTANTE

7.7.3 HERRAMIENTAS DE BORRADO SEGURO

Blancco File Eraser + Management Console Offline	
Versión	File Ereaser v8.6.2, Console 5.21.0a1
Fabricante	Blancco
Familia	Herramientas de borrado seguro
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/10/2026

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.

Observaciones

CCN-STIC 1502 Procedimiento de empleo seguro de Blancco File Eraser (En proceso de Actualización)

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	28/02/2027

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

7.7.4 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	31/12/2026
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

CCN-STIC 1238. Procedimiento de Empleo Seguro Microsoft Purview DLP

INFORMACIÓN IMPORTANTE

7.7.5 GESTIÓN DE METADATOS

MetaOLVIDO for Zimbra	
Versión	3.6.0
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2025
Revisión de Validez	30/10/2027

Descripción

Plugin para Zimbra que procesa automáticamente los metadatos de los ficheros adjuntos de los e-mails enviados por toda la organización, evitando de esta manera la fuga de información sensible que se produce de forma continuada en este tipo de comunicaciones y reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario.
• Los metadatos e información oculta serán procesados independientemente del cliente de correo utilizado (cliente de escritorio, cliente web, tablet o smartphone).
• Permite configurar los tipos de ficheros a procesar (Microsoft Office, Open/Libre Office, PDF y más de 150 extensiones de ficheros de imagen, audio y vídeo).
• Permite eliminar todos los metadatos o aplicar plantillas de metadatos.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente manteniendo la validez de la firma electrónica.
• Permite configurar dominios de exclusión (WhiteList) para el procesado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

MetaOLVIDO for Postfix

Versión	3.6.0
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2025
Revisión de Validez	30/10/2027

Descripción

Plugin para Postfix que procesa automáticamente los metadatos de los ficheros adjuntos de los e-mails enviados por toda la organización, evitando de esta manera la fuga de información sensible que se produce de forma continuada en este tipo de comunicaciones y reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario.
• Los metadatos e información oculta serán procesados independientemente del cliente de correo utilizado (cliente de escritorio, cliente web, tablet o smartphone).
• Permite configurar los tipos de ficheros a procesar (Microsoft Office, Open/Libre Office, PDF y más de 150 extensiones de ficheros de imagen, audio y vídeo).
• Permite eliminar todos los metadatos o aplicar plantillas de metadatos.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente manteniendo la validez de la firma electrónica.
• Permite configurar dominios de exclusión (WhiteList) para el procesado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

MetaOLVIDO for Outlook

Versión	5.3.4
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2025
Revisión de Validez	30/10/2027

Descripción

AddIn para Outlook que permite procesar automáticamente los metadatos de los ficheros adjuntos de los correos evitando la fuga de información que se produce de forma continuada en las comunicaciones vía e-mail, reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario, antes de enviar el correo electrónico se procesan los datos ocultos e información personal de todos los ficheros adjuntos.
• Dispone de una interfaz gráfica para configurar: Tipo de ficheros a procesar (.docx, .pdf, .jpg, …más de 150 extensiones de ficheros), borrado de metadatos o aplicación de plantillas.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente sin invalidar la firma electrónica.
• Detección de ficheros Word/Excel con control de cambios o comentarios activados.
• Permite configurar dominios de exclusión (WhiteList) para el borrado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.
• Compatible con todas las versiones de Microsoft Outlook en Windows.
• Integración con MetaOLVIDO Dashboard.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

MetaOLVIDO for Exchange

Versión	5.0.1
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2025
Revisión de Validez	30/10/2027

Descripción

Plugin para Exchange que procesa automáticamente los metadatos de los ficheros adjuntos de los e-mails enviados por toda la organización, evitando de esta manera la fuga de información sensible que se produce de forma continuada en este tipo de comunicaciones y reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario.
• Los metadatos e información oculta serán procesados independientemente del cliente de correo utilizado (cliente de escritorio, cliente web, tablet o smartphone).
• Permite configurar los tipos de ficheros a procesar (Microsoft Office, Open/Libre Office, PDF y más de 150 extensiones de ficheros de imagen, audio y vídeo).
• Permite eliminar todos los metadatos o aplicar plantillas de metadatos.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente manteniendo la validez de la firma electrónica.
• Permite configurar dominios de exclusión (WhiteList) para el procesado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

MetaClean Sync Workstation y MetaClean Sync Server

Versión	3.0.1
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	01/11/2028

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

INFORMACIÓN IMPORTANTE

MetaClean for Zimbra

Versión	3.6.0
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	17/02/2025
Revisión de Validez	30/07/2027

Descripción

Plugin para Zimbra que procesa automáticamente los metadatos de los ficheros adjuntos de los e-mails enviados por toda la organización, evitando de esta manera la fuga de información sensible que se produce de forma continuada en este tipo de comunicaciones y reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario.
• Los metadatos e información oculta serán procesados independientemente del cliente de correo utilizado (cliente de escritorio, cliente web, tablet o smartphone).
• Permite configurar los tipos de ficheros a procesar (Microsoft Office, Open/Libre Office, PDF y más de 150 extensiones de ficheros de imagen, audio y vídeo).
• Permite eliminar todos los metadatos o aplicar plantillas de metadatos.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente manteniendo la validez de la firma electrónica.
• Permite configurar dominios de exclusión (WhiteList) para el procesado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

MetaClean for Outlook

Versión	5.3.4
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	14/01/2025
Revisión de Validez	29/06/2027

Descripción

AddIn para Outlook que permite procesar automáticamente los metadatos de los ficheros adjuntos de los correos evitando la fuga de información que se produce de forma continuada en las comunicaciones vía e-mail, reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario, antes de enviar el correo electrónico se procesan los datos ocultos e información personal de todos los ficheros adjuntos.
• Dispone de una interfaz gráfica para configurar: Tipo de ficheros a procesar (.docx, .pdf, .jpg, …más de 150 extensiones de ficheros), borrado de metadatos o aplicación de plantillas.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente sin invalidar la firma electrónica.
• Detección de ficheros Word/Excel con control de cambios o comentarios activados.
• Permite configurar dominios de exclusión (WhiteList) para el borrado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.
• Compatible con todas las versiones de Microsoft Outlook en Windows.
• Integración con MetaClean Dashboard.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

metaOLVIDO Endpoint y metaOLVIDO Server	
Versión	3.0.1
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	01/11/2028

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

MetaClean for Exchange

Versión	5.0.1
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	17/02/2025
Revisión de Validez	30/07/2027

Descripción

Plugin para Exchange que procesa automáticamente los metadatos de los ficheros adjuntos de los e-mails enviados por toda la organización, evitando de esta manera la fuga de información sensible que se produce de forma continuada en este tipo de comunicaciones y reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario.
• Los metadatos e información oculta serán procesados independientemente del cliente de correo utilizado (cliente de escritorio, cliente web, tablet o smartphone).
• Permite configurar los tipos de ficheros a procesar (Microsoft Office, Open/Libre Office, PDF y más de 150 extensiones de ficheros de imagen, audio y vídeo).
• Permite eliminar todos los metadatos o aplicar plantillas de metadatos.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente manteniendo la validez de la firma electrónica.
• Permite configurar dominios de exclusión (WhiteList) para el procesado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

MetaClean for Postfix

Versión	3.6.0
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	17/02/2025
Revisión de Validez	30/07/2027

Descripción

Plugin para Postfix que procesa automáticamente los metadatos de los ficheros adjuntos de los e-mails enviados por toda la organización, evitando de esta manera la fuga de información sensible que se produce de forma continuada en este tipo de comunicaciones y reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario.
• Los metadatos e información oculta serán procesados independientemente del cliente de correo utilizado (cliente de escritorio, cliente web, tablet o smartphone).
• Permite configurar los tipos de ficheros a procesar (Microsoft Office, Open/Libre Office, PDF y más de 150 extensiones de ficheros de imagen, audio y vídeo).
• Permite eliminar todos los metadatos o aplicar plantillas de metadatos.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente manteniendo la validez de la firma electrónica.
• Permite configurar dominios de exclusión (WhiteList) para el procesado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.8 PROTECCIÓN DE INSTALACIONES E INFRAESTRUCTURAS

7.8.1 CÁMARAS IP

Axis P3265-LVE	
Versión	OS v12.10.26
Fabricante	Axis Communications
Familia	Cámaras IP
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	03/07/2026
Revisión de Validez	31/12/2026

Descripción

Domo de 2 MP preparado para exteriores con iluminación IR y aprendizaje profundo IA, dispone de Lightfinder 2.0, Forensic WDR y Optimized IR, la AXIS P3265-LVE ofrece una calidad de imagen excelente y capacidad de uso forense para cualquier condición de iluminación. Basada en el sistema en un chip (SoC) ARTPEC de Axis y el sistema operativo Axis OS, con una unidad de procesamiento de aprendizaje profundo, ofrece funciones avanzadas y análisis potentes basados en IA en el extremo. Y con la utilización de la aplicación AXIS Object Analytics preinstalada, ofrece una clasificación de objetos altamente resistente y una búsqueda rápida en el VMS. Además, gracias a las avanzadas características de ciberseguridad integradas, como el Axis Edge Vault, impide el acceso no autorizado y protege su sistema.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

7.8.2 CONTROL DE ACCESO FÍSICO

Sheld Plus	
Versión	1.2
Fabricante	DORLET
Familia	Control de Acceso Físico
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	18/12/2024
Revisión de Validez	31/05/2027

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

7.9 ESPACIO

7.9.1 PRODUCTOS CRIPTOGRÁFICOS PARA ACCESO A SERVICIOS GNSS

GMV GNSS Cryptographic Module	
Versión	2.1.7
Fabricante	GMV Aerospace and Defense
Familia	Productos criptográficos para acceso a servicios GNSS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	30/09/2025
Revisión de Validez	30/03/2028
Descripción	

La librería criptográfica "GMV GNSS Cryptographic Module" es una librería software para plataformas Linux (Ubuntu 22.04 o superior) que, a través de una API, proporciona servicios criptográficos necesarios para el acceso a determinados servicios de navegación por satélite. En particular, esta librería implementa los algoritmos establecidos por la Agencia Espacial Europea (ESA) para el servicio "Open Service Navigation Message Authentication" (OSNMA) del sistema Galileo .

Para más información, visite https://www.gmv.com/enes/productos/espacio/gmv-gnss-cryptographicmodule#supporting-documents-for-certification

Observaciones

Procedimiento de Empleo Seguro Pendiente de publicación

INFORMACIÓN IMPORTANTE

7.10 SOPORTE CRIPTOGRÁFICO

7.10.1 HERRAMIENTAS PARA FIRMA ELECTRÓNICA

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	02/01/2029

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

CCN-STIC 1541 Procedimiento de Empleo Seguro Tarjeta Criptográfica FNMT

INFORMACIÓN IMPORTANTE

Entrust Signature Activation Module

Versión	1.1.1
Fabricante	Entrust Solutions
Familia	Herramientas para firma electrónica
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/07/2026
Revisión de Validez	31/12/2026

Descripción

Entrust Signature Activation Module (SAM) es un componente de seguridad para sistemas de firma y sello electrónico remotos que implementa las funciones de un Signature Activation Module conforme al estándar CEN EN 419 241-2. El producto ha sido certificado Common Criteria EAL4+ AVA_VAN.5 y está diseñado para integrarse con módulos criptográficos certificados en entornos de firma remota de alta seguridad.

Su función es garantizar que las claves de firma o sello únicamente se utilicen bajo el control de la entidad autorizada y para operaciones expresamente autorizadas. Para ello, verifica la autenticidad e integridad de las solicitudes, valida las autorizaciones asociadas a cada operación y controla la activación de las claves antes de permitir el uso de las capacidades criptográficas.

El producto incorpora mecanismos de validación de autorizaciones, control de acceso, segregación de funciones, protección del proceso de activación de firma y generación de registros de auditoría.

Utilizado junto con módulos criptográficos certificados conforme a CEN EN 419 221-5, puede formar parte de una solución de creación remota de firmas y sellos electrónicos cualificados (QSCD) para servicios remotos bajo el reglamento eIDAS.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cryptomathic Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0

Versión	6.0
Fabricante	Cryptomathic
Familia	Herramientas para firma electrónica
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	07/11/2024
Revisión de Validez	30/04/2027

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. Respaldado 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

No aplica Procedimiento de Empleo Seguro

SIAVAL SafeCert Server Signing System (QSCD)

Versión	v3.1
Fabricante	Sistemas Informáticos Abiertos
Familia	Herramientas para firma electrónica
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2025
Revisión de Validez	31/03/2028

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 firmantes. Está diseñado para funcionar como un dispositivo remoto de creación de firma rQSCD, según los requisitos especificados en el Reglamento (UE) nº 2024/1183 del Parlamento Europeo (eIDAS 2), haciendo posible la generación de firmas electrónicas avanzadas (AdES) y de firmas electrónicas cualificadas o reconocidas (QES) en un servidor remoto, constituyéndose como un sistema confiable de firma en servidor, Trustworthy Systems Supporting Server Signing (TW4S), según se define en la norma CEN/TS 419 241 que rige este tipo de sistemas.

Observaciones

CCN-STIC-1521 Procedimiento de Empleo Seguro SIAVAL SafeCert Server Signing System (QSCD)

INFORMACIÓN IMPORTANTE

SIAVAL SafeCert Manager

Versión	v3
Fabricante	Sistemas Informáticos Abiertos
Familia	Herramientas para firma electrónica
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2025
Revisión de Validez	31/03/2028

Descripción

Producto de firma centralizada que facilita la gestión y el uso de las claves de los usuarios firmantes y que incorpora las características de un módulo SAM (Signature Activation Module).
Garantiza el control exclusivo de la clave de firma por parte del firmante, asegurando su vínculo con la clave, protegiéndola de forma que únicamente pueda ser utilizada por su propietario legítimo y dentro del entorno operativo y realizando una autenticación multicanal con segundo factor de autenticación (contraseña de un solo uso, biometría, etc.) que asegura la identidad del firmante.
Asegura todo el ciclo del proceso de firma cuando el firmante solicita una firma a través de la aplicación de creación de firma, haciendo uso de canales de transmisión que aseguran en todo momento la confidencialidad y la integridad de los datos.
La fortaleza de las firmas realizadas en el sistema se garantiza haciendo uso de módulos criptográficos certificados que aseguran la utilización de algoritmos criptográficos robustos y tamaños de claves recomendados.
SIAVAL SafeCert Manager 3 forma parte del sistema de firma remota cualificado SIAVAL SafeCert Server Signing System (QSCD) 3.1 que puede ser usado como rQSCD en un sistema confiable de firma en servidor.

Observaciones

CCN-STIC-1522 Procedimiento de Empleo Seguro SIAVAL SafeCert Manager

INFORMACIÓN IMPORTANTE

7.10.2 MÓDULO DE SEGURIDAD HARDWARE (HSM)

Thales Luna K7 Cryptographic Module (808-000048-002, 808-000048-003, 808-000073-001, 808-000073-002, 808-000066-001, 808-000069-001, 808-000070-001)	
Versión	7.7.1
Fabricante	Thales
Familia	Módulo de Seguridad Hardware (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	11/12/2024
Revisión de Validez	31/05/2027





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

INFORMACIÓN IMPORTANTE

Thales Luna K7 Cryptographic Module (808-000048-002, 808-000048-003, 808-000073-001, 808-000073-002, 808-000066-001, 808-000069-001, 808-000070-001)

Versión	7.7.2
Fabricante	Thales
Familia	Módulo de Seguridad Hardware (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	11/12/2024
Revisión de Validez	31/05/2027



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

INFORMACIÓN IMPORTANTE

Thales Luna K7 Cryptographic Module (808-000048-002, 808-000048-003, 808-000073-001, 808-000073-002, 808-000066-001, 808-000069-001, 808-000070-001)

Versión	7.7.0
Fabricante	Thales
Familia	Módulo de Seguridad Hardware (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	11/12/2024
Revisión de Validez	31/05/2027



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

INFORMACIÓN IMPORTANTE

nShield Solo XC Hardware Security Module

Versión	v12.60.15
Fabricante	Entrust Solutions
Familia	Módulo de Seguridad Hardware (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2021
Revisión de Validez	26/06/2027

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
Fabricante	UTIMACO
Familia	Módulo de Seguridad Hardware (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/03/2025
Revisión de Validez	31/08/2027

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.

Caracterísiticas 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

CCN-STIC 1513 Procedimiento de Empleo Seguro Ultimaco Cryptoserver CP5

INFORMACIÓN IMPORTANTE

Azure Managed HSM

Versión

Fabricante Microsoft

Familia Módulo de Seguridad Hardware (HSM)

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 25/10/2024

Revisión de Validez 31/12/2026

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

CCN-STIC 1516. Procedimiento de Empleo Seguro Microsoft Azure HSM

nShield 5s Hardware Security Module

Versión 13.5.1

Fabricante Entrust Solutions

Familia Módulo de Seguridad Hardware (HSM)

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 30/03/2026

Revisión de Validez 31/10/2026

Descripción

Los módulos de seguridad hardware (HSM) nShield 5s 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 productos, 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 5s 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

Procedimiento de Empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

Thales Luna K7 Cryptographic Module -StandAlone

Versión	7.8.5
Fabricante	Thales
Familia	Módulo de Seguridad Hardware (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	11/12/2024
Revisión de Validez	31/05/2027



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

INFORMACIÓN IMPORTANTE

u.trust Anchor

Versión	4.49.1
Fabricante	UTIMACO
Familia	Módulo de Seguridad Hardware (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	12/11/2025
Revisión de Validez	30/04/2028

Descripción

u.trust Anchor es un módulo de seguridad de hardware (HSM) de última generación que introduce el concepto de HSM contenedorizados (cHSM) dentro del límite protegido del HSM de hardware, cuyo objetivo principal es proporcionar servicios criptográficos seguros, como la firma y verificación de datos, el cifrado o descifrado, cálculo MAC, derivación y acuerdo de claves, hash, generación integrada de números aleatorios y generación segura de claves, almacenamiento interno y externo de claves protegidas y otras funciones de gestión de claves en un entorno a prueba de manipulaciones.

Se puede utilizar con todas las API criptográficas estándar, como PKCS#11, JCE, OpenSSL, CSP/CNG y EKM, y proporciona un mecanismo seguro de actualización de software.

Esta nueva generación de HSM mejora la escalabilidad, tanto en entornos de un solo usuario como de múltiples usuarios y proporciona a cualquier proveedor de servicios, una arquitectura HSM altamente elástica capaz de escalar rápidamente según la demanda, pero también una arquitectura que permite a los proveedores de servicios ofrecer HSM como servicio (HSMaaS) en múltiples casos de uso.

Observaciones

CCN-STIC-1002 Procedimiento de empleo seguro u.trust Anchor

INFORMACIÓN IMPORTANTE

7.10.3 INFRAESTRUCTURA PKI

Entrust Certificate Authority y Entrust Certificate Authority Administration	
Versión	10.2
Fabricante	Entrust Solutions
Familia	Infraestructura PKI
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2026
Revisión de Validez	31/12/2028

Descripción

Entrust Certificate Authority es una solución integral y de nueva generación de infraestructura de clave pública (PKI), diseñada para proteger identidades digitales de usuarios, dispositivos y aplicaciones mediante servicios escalables, de alta disponibilidad, ya sea en instalaciones locales o gestionados. Ofrece una gestión sólida y automatizada del ciclo de vida de los certificados, incluyendo su emisión, renovación y revocación.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

7.10.4 DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS

Google KMS with EKM solution

Versión

Fabricante Google

Familia Dispositivos para gestión de claves criptográficas

Tipo Servicio

Categoría ENS MEDIA

Fecha Inclusión 01/05/2023

Revisión de Validez 30/06/2027

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

Key Management Service

Versión

Fabricante Google

Familia Dispositivos para gestión de claves criptográficas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 14/03/2025

Revisión de Validez 27/02/2027

Descripción

Cloud Key Management Service es un servicio de gestión de claves alojado en la nube que le permite gestionar claves criptográficas para sus servicios en la nube del mismo modo que lo hace en las instalaciones. Puede generar, utilizar, rotar y destruir claves criptográficas AES-256, RSA-2048, RSA-3072, RSA-4096, EC-P256 y EC-P384.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

AWS KMS

Versión

Fabricante AWS

Familia Dispositivos para gestión de claves criptográficas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 31/01/2022

Revisión de Validez 30/08/2027

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

7.11 PROTECCIÓN DE PLATAFORMAS

7.11.1 DISPOSITIVOS MÓVILES

Galaxy Z Flip Series (Flip4, Flip5, Flip6, Flip7, Flip7 FE)	
Versión	Android 16
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	30/04/2026
Revisión de Validez	30/09/2028



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-1005 Procedimiento de empleo seguro Samsung Galaxy (Android 16)

Galaxy Z Fold Series (Fold4, Fold5, Fold6, Fold7)	
Versión	Android 16
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	30/04/2026
Revisión de Validez	30/09/2028



Descripción

La familia de dispositivos de la gama Galaxy Z Fold 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-1005 Procedimiento de empleo seguro Samsung Galaxy (Android 16)

INFORMACIÓN IMPORTANTE

Galaxy Tab S Series (S10 FE, S10 FE+, S9, S9+, S9 Ultra, S8, S8+, S8 Ultra)



Versión	Android 16
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	30/04/2026
Revisión de Validez	30/09/2028

Descripción

La familia de dispositivos de la gama Galaxy Tab S10 FE son tablets basadas 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 de la tablet de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC-1005 Procedimiento de empleo seguro Samsung Galaxy (Android 16)

Galaxy A Series (A36, A56, A53)



Versión	Android 16
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	30/04/2026
Revisión de Validez	30/09/2028

Descripción

La familia de dispositivos de la gama Galaxy A36 5G Qualcomm, A56 5G y A53 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-1005 Procedimiento de empleo seguro Samsung Galaxy (Android 16)

INFORMACIÓN IMPORTANTE

iPhone 14, 14 Pro, 14 Plus y 14 Pro max



Versión	iOS26
Fabricante	Apple
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/07/2025
Revisión de Validez	30/12/2027

Descripción

El iPhone 14, 14 Pro, 14 Plus y 14 Pro max 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

CCN-STIC 1654 Procedimiento de Empleo Seguro iOS18

Samsung Galaxy XCover6 Pro (SM-G736B)



Versión	Android 15
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/07/2024
Revisión de Validez	01/07/2027

Descripción

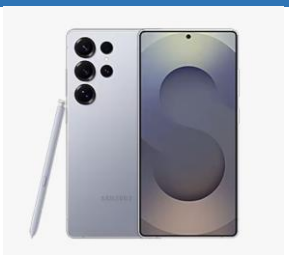
Galaxy Xcover6 Pro son dispositivos empresariales rugerizados basados en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 Procedimiento de Empleo Seguro Samsung Galaxy

INFORMACIÓN IMPORTANTE

Galaxy S Series (S25, S25+, S25 Ultra, S24, S24+, S24 FE, S24 Ultra, S23, S23+ S2 Ultra, S23 FE, S22, S22+, S22 Ultra)	
Versión	Android 16
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	30/04/2026
Revisión de Validez	30/09/2028
Descripción	



La familia de dispositivos de la gama Galaxy S25 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-1005 Procedimiento de empleo seguro Samsung Galaxy (Android 16)

iPhone 16, 16 Pro, 16 Plus, 16 Pro Max y 16e	
Versión	iOS26
Fabricante	Apple
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/07/2025
Revisión de Validez	30/12/2027
Descripción	



El iPhone 16, iPhone 16 Plus, iPhone 16 Pro, iPhone 16 Pro Max y el iPhone 16e basados en el chip de Apple A18 Pro, 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

CCN-STIC 1654 Procedimiento de Empleo Seguro iOS18

INFORMACIÓN IMPORTANTE

Galaxy Tab Active (5, 4 Pro)



Versión	Android 15
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/08/2025
Revisión de Validez	30/01/2028

Descripción

Galaxy Tab Active es una tableta rugerizada 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 Procedimiento de Empleo Seguro Samsung Galaxy

iPhone 15, 15 Pro, 15 Plus y 15 Pro Max



Versión	iOS26
Fabricante	Apple
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/07/2025
Revisión de Validez	30/12/2027

Descripción

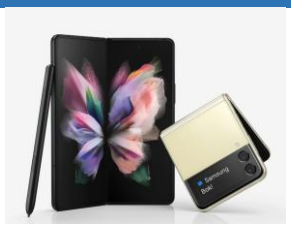
El iPhone 15, 15 Pro, 15 Plus y 15 Pro Max basados en el chip de Apple A16 Bionic, combina hardware, software y servicios que se han diseñado para funcionar conjuntamente con el fin de proporcionar seguridad y una experiencia de usuario transparente. El hardware de seguridad y el chip diseñados por Apple 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

CCN-STIC 1654 Procedimiento de Empleo Seguro iOS18

INFORMACIÓN IMPORTANTE

Galaxy Z Flip Series (Flip3, Flip4, Flip5, Flip6)



Versión	Android 15
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/08/2025
Revisión de Validez	30/01/2028

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 Procedimiento de Empleo Seguro Samsung Galaxy

Galaxy Z Fold Series (Fold3, Fold4, Fold5, Fold6)



Versión	Android 15
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/08/2025
Revisión de Validez	30/01/2028

Descripción

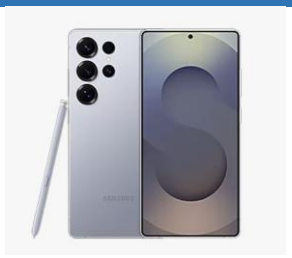
La familia de dispositivos de la gama Galaxy Z Fold son dispositivos empresariales plegables basados en Android que incorpora la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basados en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 Procedimiento de Empleo Seguro Samsung Galaxy

INFORMACIÓN IMPORTANTE

Galaxy S Series (S25, S25+, S25 Ultra, S24, S24+, S24 FE, S24 Ultra, S23, S23+ S2 Ultra, S23 FE, S22, S22+, S22 Ultra)	
Versión	Android 15
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/08/2025
Revisión de Validez	30/01/2028
Descripción	



La familia de dispositivos de la gama Galaxy S25 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 Procedimiento de Empleo Seguro Samsung Galaxy

Galaxy Tab S Series (S10 FE, S10 FE+, S9, S9+, S9 Ultra, S8, S8+, S8 Ultra)	
Versión	Android 15
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/08/2025
Revisión de Validez	30/01/2028
Descripción	



La familia de dispositivos de la gama Galaxy Tab S10 FE son tablets basadas 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 de la tablet de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1637 PES Samsung Galaxy Android 14.

INFORMACIÓN IMPORTANTE

Galaxy XCover7 Pro (SM-G766B)



Versión	Android 15
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/09/2025
Revisión de Validez	28/02/2028

Descripción

La familia de dispositivos de la gama Galaxy Xcover7 Pro 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 Procedimiento de Empleo Seguro Samsung Galaxy

Galaxy A Series (A36, A56, A53)



Versión	Android 15
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/08/2025
Revisión de Validez	30/01/2028

Descripción

La familia de dispositivos de la gama Galaxy A36 5G Qualcomm, A56 5G y A53 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 Procedimiento de Empleo Seguro Samsung Galaxy

INFORMACIÓN IMPORTANTE

iPhone 13	
Versión	iOS26
Fabricante	Apple
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	21/07/2025
Revisión de Validez	30/12/2027



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

CCN-STIC 1654 Procedimiento de Empleo Seguro iOS18

INFORMACIÓN IMPORTANTE

iPhone 17, iPhone 17 Pro, iPhone Air, iPhone 17e



Versión	Apple iOS 26
Fabricante	Apple
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	30/06/2026
Revisión de Validez	30/11/2028

Descripción

El iPhone 17 basado en el chip de Apple A19, 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.

El iPhone 17 Pro, iPhone 17 Pro Max y el iPhone Air basados en el chip de Apple A19 Pro, combinan 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

CCN-STIC 1654 Procedimiento de Empleo Seguro iOS18

INFORMACIÓN IMPORTANTE

7.11.2 SISTEMAS OPERATIVOS

SUSE Linux Enterprise Server	
Versión	Version 15 SP4
Fabricante	SUSE Software Solutions
Familia	Sistemas Operativos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2024
Revisión de Validez	14/12/2028

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

Red Hat Enterprise Linux 9.0 EUS

Versión	9.0
Fabricante	Red Hat
Familia	Sistemas Operativos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	23/07/2025
Revisión de Validez	31/12/2027

Descripción

Red Hat Enterprise Linux (RHEL) es una distribución comercial de Linux creada por Red Hat hace más de 30 años. Red Hat Enterprise Linux es un sistema operativo empresarial que destaca por su estabilidad y seguridad, estando certificado para multitud de proveedores de hardware, software y cloud providers. Red Hat Enterprise Linux es usado en servidores, tanto on-premise como en entornos cloud y en dispositivos edge. Además de ser usado por desarrolladores y también en estaciones de trabajo.

Observaciones

CCN-STIC-1658 Procedimiento de Empleo Seguro Red Hat Enterprise Linux

INFORMACIÓN IMPORTANTE

7.11.3 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	28/02/2027



Hewlett Packard Enterprise

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

CCN-STIC 1644 Procedimiento de Empleo Seguro HPE Simplivity

INFORMACIÓN IMPORTANTE

KATUA SDI PLATFORM

Versión	2.0.1
Fabricante	KRC ESPAÑOLA
Familia	Hiperconvergencia
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	14/10/2025
Revisión de Validez	31/03/2028

Descripción

Katua®SDI Platform es una plataforma hiperconvergente que unifica computación, almacenamiento, red y software en un único sistema para minimizar la complejidad del centro de datos y aumentar su escalabilidad. Está basada en el concepto Software Define Infraestructure, donde todos los elementos que conforman un CPD se definen en una única plataforma hardware + software. Permite el despliegue rápido de servicios (xaaS) y consolidación de CPDs. Puede ser instalado en distintos tipos de servidores y desplegado tanto en entornos móviles como en grandes centros de procesos de datos. Su flexibilidad permite que se puedan desplegar servicios sobre la plataforma de forma segura, sencilla y eficiente. Dispone de la capacidad para generar bibliotecas de imágenes de sistemas ya preconfigurados para su despliegue de manera sencilla 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 permitiendo, de esta forma, su instalación en nodos pequeños (desde un único equipo). 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-katua.com

Observaciones

CCN-STIC-1610 Procedimiento de Empleo Seguro KATUA SDI Platform

INFORMACIÓN IMPORTANTE

7.11.4 INFRAESTRUCTURA DE ESCRITORIO VIRTUAL (VDI)

UDS ENTERPRISE	
Versión	3.6
Fabricante	VIRTUAL CABLE
Familia	Infraestructura de escritorio virtual (VDI)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	13/03/2025
Revisión de Validez	31/08/2027

Descripción

UDS Enterprise es un software de conexión (broker) desarrollado por Virtual Cable para que las organizaciones desplieguen, gestionen y proporcionen acceso de forma centralizada a escritorios virtuales, aplicaciones virtuales, PCs y servidores. Su flexibilidad y compatibilidad con múltiples plataformas de virtualización, autenticación, protocolos de conexión y sistemas operativos garantizan una gestión eficiente y unificada de la infraestructura TI. Destacan características como Zero Trust, cifrado SSL que encripta los datos o un avanzado sistema de autenticación de múltiple factor (Desafío OTP, TOTP, etc.), que añade una capa adicional contra accesos no autorizados. La posibilidad de implementar múltiples sistemas de autenticación de manera simultánea (Active Directory, LDAP, etc.) facilita la gestión centralizada de credenciales y derechos de acceso. Además, permite la segregación de redes y entornos, limitando el acceso a recursos sensibles, minimizando el riesgo de incidentes de seguridad. También ofrece capacidades de monitorización y registro de eventos, facilitando la detección y garantizando una recuperación inmediata ante posibles amenazas. UDS Enterprise no solo optimiza la gestión y administración de entornos de digital workplace, también proporciona una infraestructura robusta y segura alineada con las mejores prácticas de ciberseguridad y compliance. Más información: https://udsenterprise.com/seguridad/

Observaciones

CCN-STIC 1656. Procedimiento de Empleo Seguro UDS Enterprise

INFORMACIÓN IMPORTANTE

ENDURANCE

Versión	1.1.9
Fabricante	COSMIKAL
Familia	Infraestructura de escritorio virtual (VDI)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	30/06/2026
Revisión de Validez	30/11/2026

Descripción

Endurance es un Espacio de Trabajo Remoto Blindado (RSW: Remote Shielded Workspace) que simplifica y aumenta la protección, control, uso y administración de los activos digitales de las organizaciones.
Gracias a la sencillez de su instalación, uso y mantenimiento, facilita la protección de activos tanto para gran corporación como para pyme. Endurance es un puente seguro entre los endpoints de los usuarios y los activos mediante un entorno de trabajo blindado que limita y customiza las funcionalidades de todas las aplicaciones. Cada usuario dispone de su propio escritorio remoto con los accesos autorizados accediendo mediante un bróker de conexión en aplicación nativa o mediante un navegador web desde cualquier tipo de dispositivo. Esta arquitectura, potenciada mediante funcionalidades de PAM (vault, permisos, roles, políticas, etc), deriva en tres ventajas fundamentales:

1. Simplifica la arquitectura de red de acceso a los activos.
2. Reduce los riesgos asociados a los endpoints.
3. Además de los accesos a activos IT/OT, protege archivos y transferencias.

Endurance es una combinación de tecnologías en una sola herramienta donde convergen seguridad, usabilidad y productividad.

Observaciones

CCN-STIC 1117. Procedimiento de Empleo Seguro Cosmikal Endurance

INFORMACIÓN IMPORTANTE

7.11.5 CONMUTADORES KVM

Secure KVM Switch (KVS4-2002VX, KVS4-2004VX, KVS4-4004VX, KVS4-1008VX, KVS4-2008VX)	
Versión	4.11.001
Fabricante	Black Box Corporation
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/08/2025
Revisión de Validez	11/10/2026
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

Procedimiento de Empleo Seguro pendiente de publicación.

Secure KVM Switch/Isolator (KVS4-8001DX)	
Versión	Firmware version 4.01.010
Fabricante	Black Box Corporation
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/08/2025
Revisión de Validez	11/10/2026
Descripción	

Aisladores KVM (Keyboard, Video and Mouse) seguros de Black Box, con conectividad de vídeo DVI, que proporcionan aislamiento entre circuitos garantizando que no existan fugas de datos a través de los puertos.
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

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Secure KVM Switch/Isolator (KVS4-8001VX)

Versión	Firmware version 4.01.001
Fabricante	Black Box Corporation
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/08/2025
Revisión de Validez	11/10/2026

Descripción

Aisladores KVM (Keyboard, Video and Mouse) seguros de Black Box, con conectividad de vídeo DisplayPort, que proporcionan aislamiento entre circuitos garantizando que no existan fugas de datos a través de los puertos.
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

Procedimiento de Empleo Seguro pendiente de publicación.

Secure KVM Switch/Isolator (KVS4-8001HX)

Versión	Firmware version 4.01.10002
Fabricante	Black Box Corporation
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/08/2025
Revisión de Validez	11/10/2026

Descripción

Aisladores KVM (Keyboard, Video and Mouse) seguros de Black Box, con conectividad de vídeo HDMI, que proporcionan aislamiento entre circuitos garantizando que no existan fugas de datos a través de los puertos.
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

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Secure KVM Switch (KVS4-2004DX, KVS4-1008DX, KVS4-2008DX)	
Versión	4.11.010
Fabricante	Black Box Corporation
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/08/2025
Revisión de Validez	11/10/2026

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

Procedimiento de Empleo Seguro pendiente de publicación.

Secure KVM Switch (KVS4-2002VX, KVS4-2002HVX, KVS4-1004HVX, KVS4-2004HVX)	
Versión	4.11.202
Fabricante	Black Box Corporation
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/08/2025
Revisión de Validez	11/10/2026

Descripción

Conmutadores KVM (Keyboard, Video and Mouse) seguros de Black Box, con conectividad de vídeo Flexible 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

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Secure KVM Switch (KVS4-4004DHVX)

Versión	4.11.111
Fabricante	Black Box Corporation
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/08/2025
Revisión de Validez	10/12/2026

Descripción

Conmutador KVM (Keyboard, Video and Mouse) seguros de Black Box, con conectividad de vídeo DVI/DisplayPort/HDMI, que proporcionan aislamiento de puertos entre redes garantizando que no existan fugas de datos entre los puertos seguros y el mundo exterior. Este dispositivos permite controlar múltiples ordenadores desde un solo teclado, ratón, hasta 4 monitores 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

Procedimiento de Empleo Seguro pendiente de publicación.

Secure KVM Switch (KVS4-8004VPX)

Versión	4.11.004
Fabricante	Black Box Corporation
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/08/2025
Revisión de Validez	11/10/2026

Descripción

Conmutador KVM (Keyboard, Video and Mouse) seguro de Black Box, con conectividad de vídeo DisplayPort con Multiviewer, 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, monitor 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

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Secure KVM Switch KVS4-1004KX & KVS4-1008KX

Versión	4.01.000
Fabricante	Black Box Corporation
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	03/10/2025
Revisión de Validez	31/03/2028

Descripción

KVS4-1004KX, KVS4-1008KX - Conmutadores de teclado y ratón de 4 y 8 puertos con conmutación por movimiento de ratón entre pantallas. 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

CCN-STIC-1659 Procedimiento de Empleo Seguro Conmutadores KVS4-1004KX KVS4-1008KX

INFORMACIÓN IMPORTANTE

7.12 SEGURIDAD OT

7.12.1 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	31/12/2026

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

INFORMACIÓN IMPORTANTE

7.13 COMUNICACIONES TÁCTICAS SEGURAS

7.13.1 SOLUCIONES PARA PROTECCIÓN DE LAS COMUNICACIONES TÁCTICAS

COMSec Admin +	
Versión	v5.1
Fabricante	Indra
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2026
Revisión de Validez	31/10/2026

Descripción

COMSec Admin + es una solución global de comunicaciones seguras que proporciona servicios cifrados resistentes a computación cuántica con mecanismos de hibridación de criptografía clásica y PQC en el ámbito de voz, mensajería instantánea y videollamada sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con 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 Admin + son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: www.indragroup.com

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Secret.T (iOS)

Versión	1.18
Fabricante	Telefónica Soluciones de Criptografía
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/08/2027

Descripción

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

Secret.T (Android)

Versión	1.15
Fabricante	Telefónica Soluciones de Criptografía
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	24/03/2025
Revisión de Validez	30/08/2027

Descripción

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

7.14 OTRAS HERRAMIENTAS

7.14.1 OTRAS HERRAMIENTAS

Amazon DynamoDB	
Versión	
Fabricante	AWS
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	07/11/2024
Revisión de Validez	31/10/2026

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

CCN-STIC-887A Guía de configuración segura AWS

AWS Route53 Resolver	
Versión	
Fabricante	AWS
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	18/06/2025
Revisión de Validez	31/05/2027

Descripción

Amazon Route 53 Resolver es un servicio de AWS que permite realizar resolución de DNS en la nube. Sus principales funcionalidades son la de resolver DNS dentro de nubes de Amazon privadas y resolución híbrida DNS, de forma que se puedan realizar consultas de resolución DNS entre redes on-premise y privadas alojadas en la nube de AWS. En la resolución híbrida, Amazon Route 53 Resolver crea puntos de conexión de Resolver salientes y entrantes, especificando las reglas de resolución DNS o integrándola entre redes on-premise y VPCs. Estos puntos de conexión están configurados para responder las peticiones DNS desde y hasta entornos on-premise. Adicionalmente, Amazon Route 53 Resolver incorpora un cortafuegos DNS que implementa listas blancas y negras para permitir o denegar tráfico DNS. Para más información consulte https://docs.aws.amazon.com/es_es/Route53/latest/DeveloperGuide/resolver.html

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	31/12/2026

Amazon CloudFront

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

INFORMACIÓN IMPORTANTE

Cartera Digital Beta (Android)

Versión	1.0
Fabricante	Agencia Estatal de Administración Digital
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	11/01/2026
Revisión de Validez	30/06/2028

Descripción

La aplicación Cartera Digital Beta ofrece una solución para la protección del menor en el entorno digital, evitando el acceso de menores a contenidos para adultos mediante un sistema de control de acceso que permite a los usuarios acreditar su mayoría de edad de forma anónima.

La solución se fundamenta en el uso de credenciales verificables emitidas por un emisor de confianza. Estas credenciales no incorporan datos personales identificativos y cuentan con un uso limitado por proveedor, reforzando la privacidad del usuario.

Adicionalmente, Cartera Digital Beta permite la gestión de otras credenciales, como las relativas a titulaciones académicas, la ausencia de antecedentes por delitos sexuales y datos del padrón.

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	31/12/2026

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 IAM+STS





Versión	
Fabricante	AWS
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/12/2026

Descripción

N/A

Observaciones

INFORMACIÓN IMPORTANTE

AWS Secrets Manager

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/02/2024

Revisión de Validez 31/12/2026

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

CCN-STIC 887A Guía de configuración segura AWS

Amazon S3

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 02/01/2025

Revisión de Validez 31/12/2026

Descripción

Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos y seguridad. Esto significa se puede utilizar para almacenar y proteger cualquier cantidad de datos para una serie de casos de uso, como sitios web, aplicaciones móviles, backup y restauración, archivo, aplicaciones empresariales, dispositivos IoT y análisis de big data. Amazon S3 ofrece características de administración fáciles de usar para que pueda organizar sus datos y configurar controles de acceso perfectamente adaptados a sus requisitos empresariales, organizativos y de conformidad específicos. Para más información visite AWS | Almacenamiento de datos seguro en la nube (S3).

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Check Point Infinity Portal

Versión

Fabricante Check Point Software Technologies

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/01/2026

Revisión de Validez 30/11/2026

Descripción

Check Point Infinity Portal es un servicio en la nube que ofrece una plataforma centralizada de administración y seguridad para los distintos servicios de Check Point. Proporciona una consola unificada desde la que los usuarios autorizados pueden gestionar identidades, autenticación, control de acceso, políticas de sesión y seguridad, así como los permisos asociados a cada servicio, ofreciendo una visión global y coherente del estado de seguridad del entorno.

El portal actúa como el núcleo operativo de la arquitectura Infinity y se basa en el enfoque "Prevention First", orientado a prevenir los ataques antes de que causen impacto. Esta capacidad se apoya en Check Point ThreatCloud AI, la infraestructura global de inteligencia de amenazas que recopila y analiza información procedente de múltiples fuentes mediante motores avanzados de inteligencia artificial, lo que permite la detección temprana de amenazas y la distribución rápida de protecciones a los entornos conectados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Cloud Logging

Versión

Fabricante Google

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 30/12/2024

Revisión de Validez 29/11/2026

Descripción

Cloud Logging es un servicio totalmente gestionado que funciona a tiempo real y puede ingerir datos de registro de aplicaciones y sistemas, así como datos de registro personalizados de miles de máquinas virtuales y contenedores. Cloud Logging permite analizar y exportar en tiempo real los registros seleccionados de distintos recursos de Google Cloud a un almacenamiento configurable a largo plazo.

Observaciones

Procedimiento de Empleo Seguro Pendiente de Publicación

INFORMACIÓN IMPORTANTE

Google Sensitive Data Protection (formerly Cloud Data Loss Prevention or DLP)

Versión

Fabricante Google

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 05/11/2024

Revisión de Validez 30/10/2026

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.

Cloud Asset Inventory

Versión

Fabricante Google

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 06/02/2025

Revisión de Validez 30/01/2027

Descripción

Cloud Asset Inventory es un inventario de activos en la nube con historial. Permite a los usuarios exportar metadatos de recursos en la nube de Google en una fecha y hora determinadas o su historial de metadatos de recursos dentro de una ventana temporal.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Amazon EC2

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/02/2024

Revisión de Validez 31/10/2026

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

CCN-STIC-887A Guía de configuración segura AWS

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 31/12/2026

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

metaOLVIDO Dashboard (modalidad Cloud)

Versión	2.2.3
Fabricante	Adarsus Technologies
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	01/11/2028

Descripción

metaOLVIDO Dashboard: Consola de administración de metaOLVIDO para las distintas modalidades de despliegue (On-Premise o Cloud). Administra, centraliza y controla la aplicación de políticas preventivas de seguridad corporativas. Permite obtener estadísticas de los metadatos procesados, gestión de licencias y controlar la exfiltración de información de forma global.

Observaciones

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard

AWS Systems Manager

Versión	
Fabricante	AWS
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	29/11/2024
Revisión de Validez	31/10/2026

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

CCN-STIC 887A Guía de configuración segura AWS

INFORMACIÓN IMPORTANTE

AWS Certificate Manager

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 21/10/2024

Revisión de Validez 31/12/2026

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

CCN-STIC 887A Guía de configuración segura AWS

Amazon EC2 Auto Scaling

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/02/2024

Revisión de Validez 31/12/2026

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

CCN-STIC-887A Guía de configuración segura AWS

INFORMACIÓN IMPORTANTE

AWS Firewall Manager

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/11/2024

Revisión de Validez 31/10/2026

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

CCN-STIC 887A Guía de configuración segura AWS

MiDNI Android

Versión v1.0

Fabricante FNMT-RCM

Familia Otras Herramientas

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/03/2025

Revisión de Validez 31/08/2027

Descripción

Policía Nacional pone a disposición de los ciudadanos una aplicación móvil gratuita, que complementa el Documento Nacional de Identidad. Con ella se podrán identificar de manera presencial y utilizarla de igual manera que el documento físico. Esta app es la única oficial y con pleno soporte legal.
La app incluye un verificador, para comprobar la autenticidad de las credenciales MiDNI de otros ciudadanos.
Antes de utilizar esta app se deberá completar el proceso de Registro, que consiste en asociar una línea telefónica móvil a la identidad del ciudadano.
Esta app no podrá utilizarse para acreditar la identidad sin conexión a datos o en otros países ni presentarlo como documento de viaje en pasos fronterizos.
Tampoco será válido para realizar gestiones telemáticas de autenticación o firma electrónica.
Esta app solicita los datos de identidad en el momento de ser usados y no los almacena en el dispositivo.
Tampoco queda registrado ningún dato de verificación ni la geolocalización de las operaciones.

Observaciones

No aplica Procedimiento de Empleo Seguro

INFORMACIÓN IMPORTANTE

MiDNI IOS

Versión v1.0.0

Fabricante FNMT-RCM

Familia Otras Herramientas

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/03/2025

Revisión de Validez 31/08/2027

Descripción

Policía Nacional pone a disposición de los ciudadanos una aplicación móvil gratuita, que complementa el Documento Nacional de Identidad. Con ella se podrán identificar de manera presencial y utilizarla de igual manera que el documento físico. Esta app es la única oficial y con pleno soporte legal.
La app incluye un verificador, para comprobar la autenticidad de las credenciales MiDNI de otros ciudadanos.
Antes de utilizar esta app se deberá completar el proceso de Registro, que consiste en asociar una línea telefónica móvil a la identidad del ciudadano.
Esta app no podrá utilizarse para acreditar la identidad sin conexión a datos o en otros países ni presentarlo como documento de viaje en pasos fronterizos.
Tampoco será válido para realizar gestiones telemáticas de autenticación o firma electrónica.
Esta app solicita los datos de identidad en el momento de ser usados y no los almacena en el dispositivo.
Tampoco queda registrado ningún dato de verificación ni la geolocalización de las operaciones.

Observaciones

No aplica Procedimiento de Empleo Seguro

Amazon S3 Glacier

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/02/2024

Revisión de Validez 31/10/2026

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 volts). 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

Yubikey 5 ES CCN Series

Versión	5.8
Fabricante	Yubico
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2028

Descripción

La serie Yubikey 5 ES CCN Series ofrece autenticación moderna resistente al phishing, respaldada por hardware. Disponible en formatos USB-A y USB-C, con capacidad NFC sin contacto, la Yubikey 5 ES CCN Series puede almacenar hasta 100 passkeys y 24 certificados PIV (tarjeta inteligente), sirviendo de puente entre las arquitecturas de seguridad basadas en FIDO y las infraestructuras tradicionales de tarjeta inteligente PIV.

La Yubikey 5 ES CCN Series cuenta con certificación IP68, es resistente a golpes, alta protección contra el agua y no incorpora partes móviles ni requiere baterías. Diseñada específicamente para entornos de alta seguridad, la Yubikey 5 ES CCN Series se fabrica y programa en Suecia, utilizando componentes y maquinaria de origen europeo, incluido el elemento seguro de Infineon.

Observaciones

CCN-STIC 1006 Procedimiento de Empleo Seguro Yubikey 5

Yubikey 5 ES CCN Series

Versión	5.7.4
Fabricante	Yubico
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2028

Descripción

La serie Yubikey 5 ES CCN Series ofrece autenticación moderna resistente al phishing, respaldada por hardware. Disponible en formatos USB-A y USB-C, con capacidad NFC sin contacto, la Yubikey 5 ES CCN Series puede almacenar hasta 100 passkeys y 24 certificados PIV (tarjeta inteligente), sirviendo de puente entre las arquitecturas de seguridad basadas en FIDO y las infraestructuras tradicionales de tarjeta inteligente PIV.

La Yubikey 5 ES CCN Series cuenta con certificación IP68, es resistente a golpes, alta protección contra el agua y no incorpora partes móviles ni requiere baterías. Diseñada específicamente para entornos de alta seguridad, la Yubikey 5 ES CCN Series se fabrica y programa en Suecia, utilizando componentes y maquinaria de origen europeo, incluido el elemento seguro de Infineon.

Observaciones

CCN-STIC 1006 Procedimiento de Empleo Seguro Yubikey 5

INFORMACIÓN IMPORTANTE

AWS Organizations

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/03/2023

Revisión de Validez 31/12/2026

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

Microsoft Purview Information Protection

Versión

Fabricante Microsoft

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 02/12/2024

Revisión de Validez 30/11/2026

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

CCN-STIC 1518. Procedimiento de Empleo Seguro Microsoft Purview Information Protection

INFORMACIÓN IMPORTANTE

Amazon Macie

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 07/05/2024

Revisión de Validez 31/12/2026

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

CCN-STIC-887A Guía de configuración segura AWS

MetaClean Dashboard (modalidad On-Premise)

Versión 2.2.3

Fabricante Adarsus Technologies

Familia Otras Herramientas

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/11/2023

Revisión de Validez 01/11/2028

Descripción

MetaClean Dashboard: Consola de administración de MetaClean para despliegue On-Premise. Administra, centraliza y controla la aplicación de políticas preventivas de seguridad corporativas. Permite obtener estadísticas de los metadatos procesados, gestión de licencias y controlar la exfiltración de información de forma global.

Observaciones

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard

INFORMACIÓN IMPORTANTE

metaOLVIDO Dashboard (modalidad On-Premise)

Versión	2.2.3
Fabricante	Adarsus Technologies
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/11/2028

Descripción

metaOLVIDO Dashboard: Consola de administración de metaOLVIDO para las distintas modalidades de despliegue (On-Premise o Cloud). Administra, centraliza y controla la aplicación de políticas preventivas de seguridad corporativas. Permite obtener estadísticas de los metadatos procesados, gestión de licencias y controlar la exfiltración de información de forma global.

Observaciones

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard

INFORMACIÓN IMPORTANTE

Cl@ve Android

Versión	5.8.3
Fabricante	Secretaría General de Administración Digital. Ministerio de Asuntos Económicos y Transformación Digital
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/08/2025
Revisión de Validez	30/01/2028

Descripción

(ES) La aplicación móvil Cl@ve permite a los ciudadanos identificarse y autenticarse de forma segura ante los servicios electrónicos de las Administraciones Públicas mediante el sistema Cl@ve, una plataforma común impulsada por diversas entidades del sector público. Esta app facilita el registro en el sistema Cl@ve, la activación del dispositivo móvil, la autenticación bien mediante códigos QR, o bien mediante la aceptación de peticiones de autenticación, informadas a través de notificaciones push, así como la consulta y gestión de los datos personales asociados. Solo se tratan los datos necesarios para prestar el servicio, incluyendo identificadores personales y del dispositivo, que se almacenan bajo control del usuario y se pueden eliminar en cualquier momento. El tratamiento se realiza conforme al Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y el Esquema Nacional de Seguridad, aplicando medidas técnicas y organizativas adecuadas. La aplicación está disponible de forma gratuita para dispositivos móviles Android (8 o superior) e iOS (15 o superior), y proporciona acceso ágil, seguro y sin necesidad de desplazamientos a los organismos adheridos al sistema Cl@ve.

(EN) The Cl@ve mobile application allows citizens to securely identify and authenticate themselves to electronic services provided by public administrations using the Cl@ve system, a common platform promoted by various public sector entities. This app facilitates registration in the Cl@ve system, activation of the mobile device, authentication via QR codes or by accepting authentication requests, notified via push notifications, as well as the consultation and management of associated personal data. Only the data necessary to provide the service is processed, including personal and device identifiers, which are stored under the user's control and can be deleted at any time. Processing is carried out in accordance with Regulation (EU) 2016/679, Organic Law 3/2018, and the National Security Framework, applying appropriate technical and organizational measures. The application is available free of charge for Android (8 or higher) and iOS (15 or higher) mobile devices, and provides fast, secure, and travel-free access to organizations participating in the Cl@ve system.

Observaciones

No aplica Procedimiento de Empleo Seguro

INFORMACIÓN IMPORTANTE

Cl@ve iOS

Versión	5.8.7
Fabricante	Secretaría General de Administración Digital. Ministerio de Asuntos Económicos y Transformación Digital
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/08/2025
Revisión de Validez	30/01/2028

Descripción

(ES) La aplicación móvil Cl@ve permite a los ciudadanos identificarse y autenticarse de forma segura ante los servicios electrónicos de las Administraciones Públicas mediante el sistema Cl@ve, una plataforma común impulsada por diversas entidades del sector público. Esta app facilita el registro en el sistema Cl@ve, la activación del dispositivo móvil, la autenticación bien mediante códigos QR, o bien mediante la aceptación de peticiones de autenticación, informadas a través de notificaciones push, así como la consulta y gestión de los datos personales asociados. Solo se tratan los datos necesarios para prestar el servicio, incluyendo identificadores personales y del dispositivo, que se almacenan bajo control del usuario y se pueden eliminar en cualquier momento. El tratamiento se realiza conforme al Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y el Esquema Nacional de Seguridad, aplicando medidas técnicas y organizativas adecuadas. La aplicación está disponible de forma gratuita para dispositivos móviles Android (8 o superior) e iOS (15 o superior), y proporciona acceso ágil, seguro y sin necesidad de desplazamientos a los organismos adheridos al sistema Cl@ve.

(EN) The Cl@ve mobile application allows citizens to securely identify and authenticate themselves to electronic services provided by public administrations using the Cl@ve system, a common platform promoted by various public sector entities. This app facilitates registration in the Cl@ve system, activation of the mobile device, authentication via QR codes or by accepting authentication requests, notified via push notifications, as well as the consultation and management of associated personal data. Only the data necessary to provide the service is processed, including personal and device identifiers, which are stored under the user's control and can be deleted at any time. Processing is carried out in accordance with Regulation (EU) 2016/679, Organic Law 3/2018, and the National Security Framework, applying appropriate technical and organizational measures. The application is available free of charge for Android (8 or higher) and iOS (15 or higher) mobile devices, and provides fast, secure, and travel-free access to organizations participating in the Cl@ve system.

Observaciones

No Aplica Procedimiento de Empleo Seguro

INFORMACIÓN IMPORTANTE

AWS CloudTrail

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 31/05/2022

Revisión de Validez 27/02/2027

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. Para más información visite: https://aws.amazon.com/es/cloudtrail/

Observaciones

CCN-STIC 887A Guía de configuración segura AWS

INFORMACIÓN IMPORTANTE

Viewtinet Observability

Versión	6.3
Fabricante	Viewtinet
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/09/2026
Revisión de Validez	28/02/2027

Descripción

Viewtinet es una plataforma de observabilidad unificada que integra en un mismo entorno la monitorización de infraestructuras TIC e IoT multifabricante y la gestión centralizada de registros (logs). Recopila métricas, estados y disponibilidad de dispositivos de red, sistemas, aplicaciones y equipos de seguridad mediante múltiples mecanismos (SNMP, ICMP, API, Syslog, CDR, Netflow, etc.), e ingiere, normaliza, indexa y almacena los registros procedentes de cualquier origen con independencia del fabricante y su formato. Proporciona análisis en tiempo real e histórico, búsqueda sobre grandes volúmenes de información, correlación de eventos entre distintas fuentes y generación de alertas, con retención a largo plazo para análisis forense y cumplimiento normativo. Incorpora gestión de configuraciones, análisis del tráfico IP con reconocimiento de aplicaciones y medición de la calidad de experiencia, detección de anomalías y funciones de cuadros de mando, informes y planificación de capacidad. Se despliega en arquitectura distribuida sobre entornos físicos, virtualizados o cloud, admite escenarios multiorganización y se integra con sistemas de terceros mediante API.

Viewtinet is a unified observability platform that combines multivendor IT and IoT infrastructure monitoring with centralized log management in a single environment. It collects metrics, status and availability from network devices, systems, applications and security appliances through multiple mechanisms (SNMP, ICMP, API, Syslog, CDR, NetFlow, etc.), and ingests, normalizes, indexes and stores records originating from any source, regardless of manufacturer and format. It provides real-time and historical analysis, search across large volumes of information, event correlation between different sources and alert generation, with long-term retention for forensic analysis and regulatory compliance. It incorporates configuration management, IP traffic analysis with application recognition and quality of experience measurement, anomaly detection, and dashboard, reporting and capacity planning functions. It is deployed in a distributed architecture on physical, virtualized or cloud environments, supports multi-tenant scenarios and integrates with third-party systems through APIs.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

INVISHIELD

Versión	1.0
Fabricante	AMLO Sistemas de Seguridad
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	04/03/2025
Revisión de Validez	30/08/2027

Descripción

Invishield es un sistema HARDWARE/SOFTWARE que automatiza la interconexión de todos los sistemas y dispositivos conectados a él, puede programarse la conexión y desconexión de cada puerto de salida con sus puertos de entrada por horario, de manera independiente según las necesidades de cada usuario, creando las reglas de programación que se ajusten a sus necesidades a través de una APK diseñada para que la programación de cada puerto sea fácil e intuitiva, puede crear programas offline y visualizarlos en tablas de tiempo semanales antes de enviar la programación, el control de la automatización de nuestro hardware es 100% invisible e inaccesible para que ningún ataque o terceras personas tengan acceso a la programación del dispositivo, sus dos sistemas independientes e invisibles entre sí: El control de la conmutación de los puertos y los datos que gestionamos.
Su sistema de puertos independientes, 3 USB y 3 RJ45, convierten a Invishield en un dispositivo versátil para cualquier empresa o usuario ya que en un solo dispositivo puedes utilizar los dos tipos de puertos para diferentes aplicaciones.
Invishield permite la automatización y el control total de los dispositivos conectados a su sistema, protegiéndolos y aislandolos de los diferentes peligros de la red. Permite tener las copias de seguridad en local y ofrecer una respuesta rápida y segura ante un ataque informático de cualquier tipo.

Observaciones

CCN-STIC 1483 Procedimiento de Empleo Seguro INVISHIELD

INFORMACIÓN IMPORTANTE

Cartera Digital Beta (IOS)

Versión 1.0.0

Fabricante Agencia Estatal de Administración Digital

Familia Otras Herramientas

Tipo Producto

Categoría ENS MEDIA

Fecha Inclusión 11/01/2026

Revisión de Validez 30/06/2028

Descripción

La aplicación Cartera Digital Beta ofrece una solución para la protección del menor en el entorno digital, evitando el acceso de menores a contenidos para adultos mediante un sistema de control de acceso que permite a los usuarios acreditar su mayoría de edad de forma anónima.

La solución se fundamenta en el uso de credenciales verificables emitidas por un emisor de confianza. Estas credenciales no incorporan datos personales identificativos y cuentan con un uso limitado por proveedor, reforzando la privacidad del usuario.

Adicionalmente, Cartera Digital Beta permite la gestión de otras credenciales, como las relativas a titulaciones académicas, la ausencia de antecedentes por delitos sexuales y datos del padrón.

Observaciones

Procedimiento de Empleo Seguro Pendiente de publicación

AWS Config

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/08/2022

Revisión de Validez 31/12/2027

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

INFORMACIÓN IMPORTANTE

VPC

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 14/03/2025

Revisión de Validez 27/02/2027

Descripción

Amazon Virtual Private Cloud (Amazon VPC) le permite crear una sección lógicamente aislada de la nube de AWS en la que puede lanzar recursos de AWS en una red virtual que usted defina. Tiene control total sobre su entorno de red virtual, incluida la selección de su propio rango de direcciones IP, la creación de subredes y la configuración de tablas de rutas y gateways de red. Puede utilizar tanto IPv4 como IPv6 en su VPC para un acceso seguro y sencillo a recursos y aplicaciones. Puede personalizar fácilmente la configuración de red de su VPC.
Para más información visite AWS | Red virtual privada en la nube (VPC). [https://aws.amazon.com/es/vpc/]

Observaciones

CCN-STIC 887A Guía de configuración segura AWS

MetaClean Dashboard (modalidad Cloud)

Versión 2.2.3

Fabricante Adarsus Technologies

Familia Otras Herramientas

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/11/2023

Revisión de Validez 01/11/2028

Descripción

MetaClean Dashboard: Consola de administración de MetaClean para despliegue Cloud. Administra, centraliza y controla la aplicación de políticas preventivas de seguridad corporativas. Permite obtener estadísticas de los metadatos procesados, gestión de licencias y controlar la exfiltración de información de forma global.

Observaciones

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard

INFORMACIÓN IMPORTANTE

Google Certificate Authority Service

Versión	
Fabricante	Google
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	28/02/2025
Revisión de Validez	30/01/2027

Descripción

Certificate Authority Service es un servicio de emisión de certificados alojado en la nube que permite a los clientes emitir y gestionar certificados para sus cargas de trabajo en la nube o locales. Certificate Authority Service puede utilizarse para crear autoridades de certificación utilizando claves de Cloud KMS para emitir, revocar y renovar certificados subordinados y de entidad final.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Amazon Route53

Versión	
Fabricante	AWS
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	02/09/2024
Revisión de Validez	31/10/2026

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

CCN-STIC-887A Guía de configuración segura AWS

INFORMACIÓN IMPORTANTE

AWS EKS

Versión

Fabricante AWS

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 19/11/2025

Revisión de Validez 31/10/2026

Descripción

Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio de Kubernetes totalmente administrado que le permite ejecutar Kubernetes sin problemas tanto en la nube de AWS como en los centros de datos en las instalaciones. En la nube, Amazon EKS automatiza la gestión de la infraestructura de clústeres de Kubernetes. Esto es fundamental para programar contenedores, administrar la disponibilidad de las aplicaciones, escalar los recursos de forma dinámica, optimizar el procesamiento, almacenar datos de clústeres y llevar a cabo otras funciones críticas. Con Amazon EKS, puede aprovechar el sólido rendimiento, escalabilidad, fiabilidad y disponibilidad de la infraestructura de AWS, así como integrarse de forma nativa con los servicios de red, seguridad y almacenamiento de AWS.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

Azure Confidential Computing

Versión

Fabricante Microsoft

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 14/03/2025

Revisión de Validez 28/02/2027

Descripción

Azure Confidential Computing es una solución de Microsoft Azure que protege datos en uso mediante entornos de ejecución confiables (TEE) basados en hardware. Cifra los datos y el código en memoria y los procesa solo después de verificar el entorno, previniendo el acceso no autorizado durante su ejecución. Facilita el cumplimiento normativo y permite la migración de cargas de trabajo confidenciales sin modificar el código existente. Esta tecnología permite a los clientes utilizar un root-of-trust que no es gestionado ni accesible por parte de Microsoft. Ofrece máquinas virtuales confidenciales, contenedores confidenciales y servicios de base de datos como Azure SQL Always Encrypted, ideal para organizaciones que manejan datos altamente sensibles y buscan maximizar la seguridad en la nube.

Observaciones

CCN-STIC-1519 Procedimiento de Empleo Seguro Azure Confidential Computing

INFORMACIÓN IMPORTANTE

Microsoft Defender for Cloud

Versión	
Fabricante	Microsoft
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	31/01/2025
Revisión de Validez	31/12/2026

Descripción

Microsoft Defender for Cloud es una plataforma de protección de aplicaciones nativas de la nube (CNAPP) que ofrece seguridad integral para entornos multinube (incluyendo Azure, AWS y GCP) e híbridos. Combina la gestión de la postura de seguridad en la nube (CSPM), la protección de cargas de trabajo en la nube (CWPP) y la seguridad en DevOps, proporcionando una defensa completa desde el desarrollo hasta la ejecución. Ofrece evaluaciones continuas, recomendaciones proactivas y detección de amenazas en tiempo real para servidores, contenedores, almacenamiento y bases de datos. Además, facilita la integración con herramientas de desarrollo, permitiendo a los equipos de seguridad y desarrollo colaborar eficazmente para mantener las aplicaciones seguras. Tiene capacidades para identificar y mitigar riesgos críticos con análisis contextuales y flujos de trabajo integrados para ayudar a las organizaciones a fortalecer su postura de seguridad y proteger sus recursos en la nube.

Observaciones

CCN-STIC 1237. Procedimiento de Empleo Seguro Microsoft Defender for Cloud

INFORMACIÓN IMPORTANTE

Chrome Enterprise Premium (formerly known as BeyondCorp Enterprise)

Versión

Fabricante Google

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 11/09/2025

Revisión de Validez 31/08/2027

Descripción

Chrome Enterprise Premium es una solución diseñada para permitir el acceso a aplicaciones de confianza cero a usuarios empresariales y proteger a las empresas de fugas de datos, malware y ataques de phishing. Chrome Enterprise Premium es una plataforma integrada que incorpora servicios y componentes de software en la nube, entre los que se incluyen:

Servicios Threat and Data Protection, que son un conjunto de servicios de seguridad que funcionan mediante la agregación de inteligencia sobre amenazas y están diseñados para proteger a los usuarios de la empresa de transferencias de malware, phishing, visitas a sitios maliciosos y filtración de datos confidenciales.

Chrome Enterprise Core, que permite la protección contra malware, phishing y fuga de datos para navegadores Chrome gestionados.

Context-Aware Access, que es un motor de reglas que permite un control de acceso detallado.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Google Cloud Identity

Versión

Fabricante Google

Familia Otras Herramientas

Tipo Servicio

Categoría ENS MEDIA

Fecha Inclusión 01/02/2026

Revisión de Validez 31/01/2028

Descripción

Cloud Identity es un producto de identidad como servicio (IDaaS) y gestión de la movilidad empresarial (EMM). Ofrece los servicios de identidad y la administración de terminales que están disponibles en Google Workspace como producto independiente.

Observaciones

CCN-STIC 1009 Procedimiento de Empleo Seguro Google Cloud Platform

INFORMACIÓN IMPORTANTE

Cloud Armor

Versión

Fabricante Google

Familia Otras Herramientas

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 18/11/2025

Revisión de Validez 31/10/2026

Descripción

Google Cloud Armor ofrece un marco de políticas y un lenguaje de reglas para personalizar el acceso a las aplicaciones conectadas a Internet y desplegar defensas contra ataques de denegación de servicio, así como contra ataques dirigidos a aplicaciones. Los componentes de Google Cloud Armor incluyen: protección volumétrica contra ataques DDoS de capa 3/4, reglas preconfiguradas para el firewall de aplicaciones web (WAF) y lenguaje de reglas personalizado.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

CosmicGuard for Linux

Versión v2.2

Fabricante GMV SOLUCIONES GLOBALES INTERNET

Familia Otras Herramientas

Tipo Producto

Categoría ENS ALTA

Fecha Inclusión 01/03/2026

Revisión de Validez 30/11/2026

Descripción

CosmicGuard es una herramienta de ciberseguridad diseñada para proteger, de una forma integral y coordinada, servidores y endpoints que operan en una plataforma o servicio común.
La solución consta de un servidor centralizado gestionado a través de una consola web y múltiples agentes de seguridad que protegen los equipos, bloqueando y reportando cualquier actividad que no esté expresamente autorizada según las reglas definidas en una política de seguridad.
Las reglas de la política de seguridad actúan bajo el paradigma de lista blanca, y permiten controlar aspectos como la ejecución de procesos, la carga de librerías, el acceso a archivos y directorios, el establecimiento de las conexiones de red entrantes y salientes, asegurando la integridad de todo el entorno.
La consola web cuenta con un sistema de acceso restringido y segmentado por roles que permite gestionar la red de agentes, distribuir las políticas de seguridad y auditar cualquier evento o violación de seguridad.
La herramienta incluye, además, políticas de seguridad probadas para proteger los centros de control de satélites proporcionados por GMV, bajo un enfoque de defensa en profundidad.
Más información en: https://www.gmv.com/es-es/productos/ciberseguridad/cosmicguard

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Quside PCIe One - FMC One

Versión	1.0
Fabricante	QUSIDE TECHNOLOGIES
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	18/02/2025
Revisión de Validez	31/12/2026

Descripción

La Quside Garnet™ Series (PCIe ONE) es un generador cuántico de números aleatorios (QRNG) con interfaz PCI Express, diseñado para entregar aleatoriedad de alta calidad a velocidades de hasta 1 Gb/s. Cumple con los estrictos estándares SP800-90B del NIST y proporciona entropía mínima condicional hasta 0.99 a temp. ambiente. Además, gracias a su metrología de aleatoriedad integrada, es capaz de medir la entropía en tiempo real. Esto garantiza transparencia y fiabilidad, sentando una base criptográfica robusta adaptable a entornos que requieren criptografía post-cuántica y criptoagilidad para afrontar futuras amenazas. La Quside Nellite™ Series (FMC ONE) está diseñada para usuarios de FPGA, ofreciendo una fuente de entropía de alta calidad a través de dispositivos que cumplen el estándar FMC (ANSI/VITA 57.1 2019). Opera a 1 Gb/s, incorpora IP cores de firmware para facilitar su control e integración y permite estimaciones en tiempo real de la entropía mínima condicional, asegurando privacidad y confiabilidad. Ambas series avalan la capacidad de Quside para generar entropía segura, esencial para aplicaciones en criptografía avanzada, distribución de claves cuánticas y sistemas de alta seguridad. https://quside.com/products/

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

PQC-Route

Versión	v2.5.5.0
Fabricante	Mumken
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/05/2026
Revisión de Validez	31/10/2026

Descripción

PQC Route es una solución de comunicaciones seguras "Quantum Resistant" orientada a infraestructuras críticas, entornos ENS y Administraciones Públicas.

La solución implementa un modelo Zero Trust basado en rutas explícitas hacia recursos concretos, eliminando conectividad lateral innecesaria y reduciendo la exposición de la infraestructura interna.

Su arquitectura distribuida permite establecer canales seguros multicapa TLS 1.3 y TLS PQC mediante conexiones exclusivamente salientes.

La solución incorpora seguridad basada en hibridación criptográfica con múltiples algoritmos PQC y tradicionales, capacidades avanzadas de cripto agilidad, autenticación híbrida, auditoría criptográfica avanzada, validación contextual de aplicaciones, control temporal de acceso y trazabilidad verificable sobre identidades, certificados, algoritmos criptográficos y eventos operacionales.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

8. PRODUCTOS APROBADOS



8.1 HERRAMIENTAS PARA EL DESARROLLO DE PRODUCTOS DE SEGURIDAD

Módulo criptográfico para aplicaciones móviles Telcryp	
Versión	1.3
Fabricante	Cryptographic and Security System (CS2)
Familia	-
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/12/2026





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 ACCESOS

8.2.1 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
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	31/12/2027

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, Forninet y mas) todo ello mediante la integración múltiples fuentes de autenticación (Directorios activos, LDAP, BBDD y provedores externos de identidad)

Observaciones

CCN-STIC 1103 Procedimiento de Empleo Seguro Aruba ClearPass 6.11

8.2.2 SERVIDORES DE AUTENTICACIÓN

Location-Based Identity Platform	
Versión	
Fabricante	Ironchip Telco
Familia	Servidores de Autenticación
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

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

Aruba ClearPass Policy Manager	
Versión	6.11
Fabricante	HPE Aruba Networking
Familia	Servidores de Autenticación
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	31/12/2027

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, Forninet y mas) todo ello mediante la integración múltiples fuentes de autenticación (Directorios activos, LDAP, BBDD y provedores externos de identidad)

Observaciones

CCN-STIC 1103 Procedimiento de Empleo Seguro Aruba ClearPass 6.11

8.2.3 GESTIÓN DE ACCESO PRIVILEGIADO (PAM)

Safeguard for Privilege Passwords	
Versión	7.0
Fabricante	One Identity
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/07/2025
Revisión de Validez	30/11/2026

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)

CyberArk Privileged Access Manager Self-Hosted

Versión	14.0
Fabricante	CYBERARK
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	31/10/2026

Descripción

CyberArk Privileged Access Manager es una solución de seguridad de la identidad que permite proteger, controlar y monitorizar el acceso privilegiado a infraestructuras locales, en la nube e híbridas. Permite a las organizaciones:
Administrar y proteger las credenciales de las cuentas privilegiadas y sus derechos de acceso.
• Asegurar y controlar, de forma centralizada, el acceso a las credenciales privilegiadas basadas en políticas de seguridad definidas administrativamente.
• Aislar y asegurar las sesiones de los usuarios privilegiados.
• Monitorizar y controlar la actividad de las cuentas privilegiadas, identificando actividades sospechosas y permitiendo responder a las amenazas.
• Ver sesiones privilegiadas en tiempo real, suspender automáticamente y terminar remotamente las sesiones sospechosas.
• Detectar, alertar y responder a actividades privilegiadas anómalas.
• Que los usuarios privilegiados ejecuten comandos administrativos autorizados desde sus sesiones nativas de Unix o Linux, eliminando los privilegios raíz innecesarios.
• Controlar el acceso de privilegios mínimos para multitud de objetivos, con una variedad de más de 350 conectores comprobados accesibles desde su Market Place sin cargo adicional.

Observaciones

CCN-STIC 1108 PES CyberArk Privileged Account Security Solution PAS (En proceso de actualización)

SOFFID IAM

Versión	3.5
Fabricante	SOFFID IAM
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	31/08/2027

Descripción

Soffid es la solución IAM que integra la gestión de acceso (AM), el gobierno de identidad (IGA), el riesgo y cumplimiento de identidad (IRC) y la gestión de cuentas privilegiadas (PAM) en una única plataforma integral. Su enfoque modular escalable y flexible, permite incorporar las anteriores soluciones en función de las necesidades particulares.

Con Soffid, las organizaciones gestionan las identidades de manera ágil y sin complicaciones porque la plataforma proporciona una visión centralizada y un control completo sobre identidades, accesos y cuentas privilegiadas.

- Gestión centralizada sin complejidad: Unifica el control de accesos, eliminando integraciones innecesarias y reduciendo el tiempo de implementación.
- Automatización eficiente: Para empleados y otros usuarios, permitiendo que accedan a las aplicaciones y a los datos estrictamente necesarios para desempeñar su trabajo, uso o colaboración.
- Protección de cuentas privilegiadas con controles avanzados, gestión de sesiones y monitorización de accesos críticos.
- Gobierno inteligente: Certificación de accesos, auditoría continua y cumplimiento normativo adaptado a cada organización.
- Facilidad operativa: Optimiza la gestión de identidades con procesos automatizados y ágiles, reduciendo la carga operativa de IT.

Observaciones

CCN-STIC 1118. Procedimiento de Empleo Seguro Soffid IAM

8.2.4 GESTIÓN DE IDENTIDADES (IM)

One Identity Manager	
Versión	v 9.0
Fabricante	One Identity
Familia	Gestión de identidades (IM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2026

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 desaprovisionamiento 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

SailPoint IdentityIQ

Versión	V8.3p5
Fabricante	Sailpoint
Familia	Gestión de identidades (IM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2026
Revisión de Validez	30/11/2028

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 Procedimiento de Empleo Seguro SailPoint IdentityIQ

SOFFID IAM

Versión	3.5
Fabricante	SOFFID IAM
Familia	Gestión de identidades (IM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	31/08/2027

Descripción

Soffid es la solución IAM que integra la gestión de acceso (AM), el gobierno de identidad (IGA), el riesgo y cumplimiento de identidad (IRC) y la gestión de cuentas privilegiadas (PAM) en una única plataforma integral. Su enfoque modular escalable y flexible, permite incorporar las anteriores soluciones en función de las necesidades particulares.
Con Soffid, las organizaciones gestionan las identidades de manera ágil y sin complicaciones porque la plataforma proporciona una visión centralizada y un control completo sobre identidades, accesos y cuentas privilegiadas.
- Gestión centralizada sin complejidad: Unifica el control de accesos, eliminando integraciones innecesarias y reduciendo el tiempo de implementación.
- Automatización eficiente: Para empleados y otros usuarios, permitiendo que accedan a las aplicaciones y a los datos estrictamente necesarios para desempeñar su trabajo, uso o colaboración.
- Protección de cuentas privilegiadas con controles avanzados, gestión de sesiones y monitorización de accesos críticos.
- Gobierno inteligente: Certificación de accesos, auditoría continua y cumplimiento normativo adaptado a cada organización.
- Facilidad operativa: Optimiza la gestión de identidades con procesos automatizados y ágiles, reduciendo la carga operativa de IT.

Observaciones

CCN-STIC 1118. Procedimiento de Empleo Seguro Soffid IAM

8.3 PROTECCIÓN DE DISPOSITIVOS

8.3.1 ANTI-VIRUS / EPP (ENDPOINT PROTECTION PLATFORM)

Falcon Sensor con Falcon Console Cloud	
Versión	7.21.19205
Fabricante	CrowdStrike
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2027

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 Procedimiento de Empleo Seguro Falcon Sensor

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

Trend Vision One Endpoint Security

Versión	20.0.1.4540
Fabricante	Trend Micro
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2028

Descripción

Vision One - Endpoint Security, es la propuesta EPP y EDR de Trend Micro para proteger Endpoints, Servidores como cargas de trabajo en nube.

Forma parte de la plataforma Trend Vision One, en conjunto con otras capacidades de protección: E-mail, NDR, CTEM, CNAPP, MDM, etc alimentando con la telemetría recogida la arquitectura XDR que facilita una detección temprana y protección frente a los retos que presenta el cibercrimen moderno.

El producto se ofrece tanto en formato SaaS (Trend Vision One Console) como On-Premise (Trend Vision One On-Prem Management Server).
El Trend Vision One On-Prem Management Server NO ESTÁ CUALIFICADO

Observaciones

CCN-STIC 1216 Procedimiento de Empleo Seguro Trend Vision One Endpoint Security

8.3.2 EDR (ENDPOINT DETECTION AND RESPONSE)

Falcon Sensor con Falcon Console Cloud	
Versión	7.21.19205
Fabricante	CrowdStrike
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2027

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 Procedimiento de Empleo Seguro Falcon Sensor

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

FortiEDR

Versión	6.0
Fabricante	Fortinet
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2026
Revisión de Validez	30/09/2027

Descripción

FortiEDR es una solución integral de seguridad para Endpoints que ofrece protección en tiempo real, automatizada y con respuesta a incidentes orquestada. Protege diversos sistemas operativos y plataformas, incluyendo la nube, mediante la prevención, detección y respuesta a amenazas avanzadas, incluso en dispositivos ya comprometidos. FortiEDR emplea aprendizaje automático a nivel de kernel (en Windows y Linux) para bloquear las brechas y proteger los datos de la exfiltración y el cifrado de ransomware.
Integra varias herramientas de Fortinet y de terceros, facilitando la gestión y automatización de la seguridad. Su arquitectura permite una implementación flexible y escalable, reduciendo los tiempos de detección y respuesta a incidentes. Finalmente, ofrece servicios gestionados opcionales para una mayor seguridad.

Observaciones

CCN-STIC 1010 Procedimiento de Empleo Seguro FortiEDR

Trend Vision One Endpoint Security

Versión	20.0.1.4540
Fabricante	Trend Micro
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2028

Descripción

Vision One - Endpoint Security, es la propuesta EPP y EDR de Trend Micro para proteger Endpoints, Servidores como cargas de trabajo en nube.

Forma parte de la plataforma Trend Vision One, en conjunto con otras capacidades de protección: E-mail, NDR, CTEM, CNAPP, MDM, etc alimentando con la telemetría recogida la arquitectura XDR que facilita una detección temprana y protección frente a los retos que presenta el cibercrimen moderno.

El producto se ofrece tanto en formato SaaS (Trend Vision One Console) como On-Premise (Trend Vision One On-Prem Management Server).
El Trend Vision One On-Prem Management Server NO ESTÁ CUALIFICADO

Observaciones

CCN-STIC 1216 Procedimiento de Empleo Seguro Trend Vision One Endpoint Security

8.4 PROTECCIÓN DE REDES Y SISTEMAS

8.4.1 SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM)

IBM QRadar Security Intelligence Platform	
Versión	7.5
Fabricante	IBM
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
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

LogPoint SIEM	
Versión	7.4.0.4
Fabricante	LogPoint
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2026
Revisión de Validez	31/08/2027
Descripción	

Logpoint SIEM es una herramienta de Analálisis y Gestión de eventos de seguridad. Logpoint ofrece un análisis rápido e informes enriquecidos.Por otro lado, es capaz de ofrecer una gran variedad de informes de cumplimiento gracias a la base de plantillas built-in de las que dispone.
Como parte de la infraestructura de Logpoint, el SIEM tiene la posibilidad de integracion con Logpoint SOAR y con Logpoint NDR.

Observaciones

CCN-STIC 1242 Procedimiento de Empleo Seguro LogPoint SIEM

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	30/09/2026

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

Splunk Enterprise

Versión	9.4
Fabricante	Splunk
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	30/06/2026
Revisión de Validez	16/12/2026

Descripción

Splunk Enterprise es una plataforma de gestión de eventos e información de seguridad (SIEM) que proporciona una visibilidad completa de la postura de seguridad de una organización. Permite gestionar el ciclo completo de seguridad, incluyendo capacidades de Detección, Monitorización, Investigación y Respuesta ante incidentes de seguridad (TDIR).

La plataforma incorpora capacidades avanzadas de búsqueda, generación de informes y análisis en tiempo real e histórico, 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 aquellos que afectan a activos o identidades críticas, así como generar alertas basadas en riesgo e identificar anomalías y amenazas tanto externas como internas.

Además, Splunk Enterprise permite la orquestación y automatización de respuestas a incidentes mediante Splunk SOAR, proporcionando correlación de eventos en tiempo real, análisis contextual, priorización basada en riesgos e integración con fuentes externas de inteligencia de amenazas. Las más de 2.500 reglas de detección abarcan todos los ámbitos de seguridad: IT, OT, IoT, IoMT y nubes públicas en cualquiera de sus formatos.

Observaciones

CCN-STIC-1225 Procedimiento de Empleo Seguro Splunk Enterprise 9.4

FortiAnalyzer

Versión	7.2
Fabricante	Fortinet
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2026
Revisión de Validez	31/12/2027

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 predefinidias (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.
Modelos:
Familia E: FAZ-400E, FAZ-2000E, FAZ-3500E.
Familia F: FAZ-200F, FAZ-300F, FAZ-800F, FAZ-1000F, FAZ-3000F, FAZ-3500F, FAZ-3700F.
Familia G: FAZ-150G, FAZ-300G, FAZ-800G, FAZ-810G, FAZ-1000G, FAZ-3000G, FAZ-3100G, FAZ-3500G, FAZ-3510G, FAZ-3700G.
Modelos VM: FAZ-VM, FAZ-VM64, FAZ-VM64-ALI, FAZ-VM64-AWS, FAZ-VM64-AWSOnDemand, FAZ-VM64-AZURE, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-IBM, FAZ-VM64-KVC, FAZ-VM64-OPC, FAZ-VM64-XEN.

Observaciones

CCN-STIC-1444 Procedimiento de empleo seguro FortiAnalyzer

NGSIEM Logica - Monica

Versión	8.0
Fabricante	ICA Sistemas y Seguridad
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/07/2026
Revisión de Validez	31/12/2026

Descripción

LogICA
La plataforma española LogICA Next Generation SIEM permite a los equipos de ciberseguridad recopilar y analizar información de seguridad a gran escala, detectar amenazas avanzadas mediante analítica de comportamiento, anomalías e inteligencia de amenazas, y automatizar procesos de investigación y respuesta ante incidentes en entornos IT, OT, IoT y cloud. LogICA integra información de cualquier fuente corporativa, tecnológica o de negocio, correlando y enriqueciendo datos en tiempo real para proporcionar visibilidad del riesgo y facilitar la priorización de incidentes. Su arquitectura abierta combina capacidades SIEM, análisis avanzado, threat hunting, detección basada en comportamiento e integración con fuentes de inteligencia externas, permitiendo identificar amenazas conocidas y emergentes con mayor precisión. Asimismo, se integra con herramientas y asistentes basados en Inteligencia Artificial que facilitan la investigación, contextualización y gestión de incidentes de seguridad, mejorando la productividad de los equipos SOC. Además, incorpora capacidades de monitorización operativa, cuadros de mando y automatización de procesos de seguridad, adaptándose a despliegues on-premise, virtualizados, híbridos o cloud.

MONICA
La plataforma española MONICA NG SIEM permite a los analistas de ciberseguridad recopilar, correlacionar y analizar información de seguridad de cualquier fuente tecnológica o de negocio, ofreciendo capacidades avanzadas de detección, investigación y respuesta ante amenazas en entornos IT, OT, IoT y cloud. MONICA procesa eventos y telemetría en tiempo real mediante correlación avanzada, analítica de comportamiento, detección de anomalías e inteligencia de amenazas para identificar actividades maliciosas, vulnerabilidades y riesgos emergentes. Facilita la contextualización y priorización de incidentes mediante el enriquecimiento de la información y casos de uso especializados. Asimismo, se integra con herramientas y asistentes basados en Inteligencia Artificial para apoyar la investigación y gestión de incidentes, reduciendo los tiempos de detección y respuesta. MONICA dispone además de capacidades nativas de integración con herramientas y servicios del ecosistema del Centro Criptológico Nacional, favoreciendo la interoperabilidad y el intercambio seguro de información. Su arquitectura abierta y escalable permite automatizar operaciones e integrarse en despliegues on-premise, virtualizados, híbridos o cloud.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

GLORIA

Versión	6.26.0
Fabricante	S2 Grupo Soluciones de Seguridad S.L
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2026
Revisión de Validez	28/02/2027

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

8.4.2 HERRAMIENTAS DE GESTIÓN DE RED

NetinDS	
Versión	2.0.2
Fabricante	Mytra Control
Familia	Herramientas de gestión de red
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/04/2027

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

CCN-STIC 1235. Procedimiento de Empleo Seguro NetinDS

FortiManager

Versión	7.2
Fabricante	Fortinet
Familia	Herramientas de gestión de red
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	31/03/2027

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".
Modelos:
Familia E: FMG-300E, FMG-400E y FMG-2000E.
Familia F: FMG-200F, FMG-300F, FMG-1000F, FMG-3000F y FMG-3700F.
Familia G: FMG-200G, FMG-400G, FMG-410G, FMG-1000G, FMG-3000G, FMG-3100G y FMG-3700G.
Familia VM: FMG-VM.

Observaciones

CCN-STIC-1443 Procedimiento de empleo seguro FortiManager

8.4.3 DETECCIÓN Y RESPUESTA DE AMENAZAS EN RED (NDR)

CARMEN	
Versión	Versión 7.24.3
Fabricante	S2 GRUPO / CCN
Familia	Detección y respuesta de amenazas en red (NDR)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2022
Revisión de Validez	31/10/2026

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 PERÍMETRO

8.5.1 ENRUTADORES

QFX Series (QFX5700)	
Versión	Junos OS 23.4R2-S2-EVO
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2027

Descripción

La línea QFX5700 que incluye el QFX5700 y QFX5700E admite funciones avanzadas de Capa 2, Capa 3 y EVPN-VXLAN. La plataforma está diseñada para su uso en centros de datos, campus, interconexión de centros de datos (DCI) y conexión de clústeres de firewall. La elección de velocidad de interfaz para la conectividad de servidores o dentro de un solución de fabric permite versatilidad en el despliegue y protección de la inversión.
Los proveedores de nube pública y de servicios que buscan satisfacer el crecimiento explosivo obtienen soporte de puertos 400GbE a escala de Internet. Para los clientes empresariales que están haciendo la transición de sus granjas de servidores de 10GbE a 25GbE, el QFX5700 proporciona la opción de ser usado como spine para arquitectura EVPN-VXLAN de 100GbE/400GbE con bajo consumo de energía en un espacio reducido. Con hasta 25.6 Tbps de rendimiento bidireccional, el switch está optimizado para despliegues de leaf & spine en centros de datos empresariales, computación de alto rendimiento, proveedores de servicios o en la nube.

Observaciones

CCN-STIC-1440 Procedimiento de Empleo Seguro Juniper QFX Series

MX Series (204, 304, 10003)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

Descripción

Las plataformas de enrutamiento universal MX204, MX304 y 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 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. 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.

Observaciones

CCN-STIC-1456 Procedimiento de Empleo Seguro Juniper Routers MX Series

EX 4400 Series (4400-24T|24P|24MP|48T|48P|48F|48MP)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

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, asi 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

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

MX Series (240, 480, 960) con tarjetas MPC10E y MX-SPC3

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

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

CCN-STIC-1456 Procedimiento de Empleo Seguro Juniper Routers MX Series

EX 9200 Series (9204, 9208, 9214) con tarjetas EX9200-15C

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las 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 de las funcionalidades de seguridad. Como switch de nivel 2 en la capa OSI, realiza un análisis de los 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 trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

EX3400 Series (3400-24T|24P|48T|48P)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las 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 de las funcionalidades de seguridad. Como switch de nivel 2 en la capa OSI, realiza un análisis de los 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 trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

QFX Series (5120-48YM|48T|48Y|32C, 5200-48Y|32C, 5210-64C) y EX4650-48Y

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

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 Procedimiento de Empleo Seguro Juniper QFX Series

QFX Series (QFX5700)

Versión	Junos OS 24.4R1-EVO
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

Descripción

La línea QFX5700 que incluye el QFX5700 y QFX5700E admite funciones avanzadas de Capa 2, Capa 3 y EVPN-VXLAN. La plataforma está diseñada para su uso en centros de datos, campus, interconexión de centros de datos (DCI) y conexión de clústeres de firewall. La elección de velocidad de interfaz para la conectividad de servidores o dentro de un solución de fabric permite versatilidad en el despliegue y protección de la inversión.
Los proveedores de nube pública y de servicios que buscan satisfacer el crecimiento explosivo obtienen soporte de puertos 400GbE a escala de Internet. Para los clientes empresariales que están haciendo la transición de sus granjas de servidores de 10GbE a 25GbE, el QFX5700 proporciona la opción de ser usado como spine para arquitectura EVPN-VXLAN de 100GbE/400GbE con bajo consumo de energía en un espacio reducido. Con hasta 25.6 Tbps de rendimiento bidireccional, el switch está optimizado para despliegues de leaf & spine en centros de datos empresariales, computación de alto rendimiento, proveedores de servicios o en la nube.

Observaciones

CCN-STIC-1440 Procedimiento de Empleo Seguro Juniper QFX Series

EX4100 Series (4100-24P|24T|24MP|48P|48T|48MP|F-12P|F-24P|F-48P|F-12T|F-24T|F-48T)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

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, reenvia 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

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

EX2300 Series (EX2300-C-12T|12P|24T|24P|48T|48P|24MP|48MP)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las 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 de las funcionalidades de seguridad. Como switch de nivel 2 en la capa OSI, realiza un análisis de los 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 trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

HPE Aruba Networking CX 4100i, 6000, 6100, 6200, 6300, 6400, 8100, 8320, 8325, 8360, 8400, 9300, y 10000



Versión	10.13
Fabricante	HPE Aruba Networking
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2027

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

CCN-STIC 1432 Procedimiento de Empleo Seguro Aruba CX Series

ACX Series (5448, 5448-M, 5448-D)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

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 Procedimiento de Empleo Seguro ACX Routers

Atlas-840, M10-Smart Series, M2 Series, 4GePlus Series, Teldat-5Ge Series, 5Ge-Rail Series, Connect-4GePlus Series, Connect-5Ge Series, Connect-FW Series, Regesta SmartV2 Series, H5 Rail Series	
Versión	11.02.04.85.02
Fabricante	TELDAT
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	28/02/2028

Descripción

Familia de routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones

Observaciones

CCN-STIC 1471 Procedimiento de Empleo Seguro Teldat Router

SRX Series (300, 320, 340, 345, 345-DUAL-AC, 380, 1500, 1600, 2300, 4100, 4200, 4300, 4600, 5400, 5600, 5800)	
Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

Descripción

La familia de firewall mid-range de Juniper Networks® 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 Procedimiento de Empleo Seguro Juniper SRX Series

Juniper PTX10000 Series (PTX10004, PTX10016, PTX10001-36MR, PTX10002-36QDD)

Versión	JunOs 23.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/03/2026
Revisión de Validez	29/02/2028

Descripción

La familia de routers PTX10k de HPE Juniper Networking está diseñada para ofrecer un rendimiento extremo en redes IP/MPLS de alto rendimiento, combinando capacidades avanzadas de routing y switching con sólidas funciones de seguridad integradas. Basados en la arquitectura de ASIC Express, proporcionan alta capacidad de conmutación, baja latencia y alta eficiencia energética, ideales para operadores y grandes proveedores de servicios. La familia PTX incorporan protección a nivel de infraestructura, mitigación de ataques DDoS y telemetría en tiempo real para detectar anomalías. Sus funcionalidades de segmentación de red en capa L2 y L3 basadas en estándares de la industria, el control del plano de routing y la compatibilidad con protocolos como MP-BGP, IS-IS, MPLS y SRv6 garantizan un enrutamiento basado en estándares, fiable, seguro y escalable en entornos redes WAN y centros de datos de misión crítica.

Observaciones

Pendiente PES

Juniper MX Series (10004, 10008, 10016)

Versión	JunOS 23.4R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/03/2026
Revisión de Validez	29/02/2028

Descripción

Las plataformas de enrutamiento universal MX10000, compuestas por el MX10003, MX10004, MX10008, MX10016, 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 MX es altamente escalable desde desde los 2.4Tbps en 3U, pasando por 38,4 Tbps en 7 slots hasta un rendimiento de 76,8 Tbps en 13 slots.

Observaciones

8.5.2 SWITCHES

QFX Series (QFX5700)	
Versión	Junos OS 23.4R2-S2-EVO
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2027

Descripción

La línea QFX5700 que incluye el QFX5700 y QFX5700E admite funciones avanzadas de Capa 2, Capa 3 y EVPN-VXLAN. La plataforma está diseñada para su uso en centros de datos, campus, interconexión de centros de datos (DCI) y conexión de clústeres de firewall. La elección de velocidad de interfaz para la conectividad de servidores o dentro de un solución de fabric permite versatilidad en el despliegue y protección de la inversión.
Los proveedores de nube pública y de servicios que buscan satisfacer el crecimiento explosivo obtienen soporte de puertos 400GbE a escala de Internet. Para los clientes empresariales que están haciendo la transición de sus granjas de servidores de 10GbE a 25GbE, el QFX5700 proporciona la opción de ser usado como spine para arquitectura EVPN-VXLAN de 100GbE/400GbE con bajo consumo de energía en un espacio reducido. Con hasta 25.6 Tbps de rendimiento bidireccional, el switch está optimizado para despliegues de leaf & spine en centros de datos empresariales, computación de alto rendimiento, proveedores de servicios o en la nube.

Observaciones

CCN-STIC-1440 Procedimiento de Empleo Seguro Juniper QFX Series

MX Series (204, 304, 10003)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

Descripción

Las plataformas de enrutamiento universal MX204, MX304 y 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 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. 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.

Observaciones

CCN-STIC-1456 Procedimiento de Empleo Seguro Juniper Routers MX Series

Fortiswitch

Versión	7.6
Fabricante	Fortinet
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2026
Revisión de Validez	28/02/2029

Descripción

La gama de switches FortiSwitch ofrece conmutación segura de capa 2 y capa 3 integrada con FortiGate mediante FortiLink, permitiendo convertir la red Ethernet en una extensión directa del Security Fabric. Esto permite aplicar políticas de segmentación dinámica, control de acceso basado en 802.1X y visibilidad de dispositivos sin necesidad de licencias adicionales. Con soporte para PoE, redundancia y calidad de servicio (QoS) entre otras características, FortiSwitch está diseñado para entornos críticos como campus, SD-Branch y centros de datos. Su gestión centralizada a través de FortiGate o FortiManager simplifica la operación y mejora la visibilidad global del acceso a la red.

Observaciones

CCN-STIC 1482 Procedimiento de Empleo Seguro FortiSwitch v7.6

EX 4400 Series (4400-24T|24P|24MP|48T|48P|48F|48MP)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

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, asi 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

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

H3C IE4320 Series, IE4320-EI Series, IE4500-G Series and IE4520 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	09/11/2029

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.

Modelos:

IE4320 Series, H3C Comware Software Version 7.1.070 Release 6369

IE4320-28S-HPWR model

IE4320-EI Series, H3C Comware Software Version 7.1.070 Release 6815P03

IE4320-8T2P2X-PWR-EI model, IE4320-8T2P2X-EI model, IE4320-16T4X-EI model, IE4320-8T8P4X-EI model, IE4320-16T8TP4P model, IE4320-24T4X-EI model, IE4320-16T8TP4X-EI model, IE4320-16T8TP4X-HPWR-EI model, IE4320-12P4TP4X-C-EI model, IE4320-24T16P4X-EI model.

IE4500-G Series, H3C Comware Software Version 7.1.070 Release 8307P15

IE4500-14S-UPWR-G model, IE4500-14S-G model, IE4500-36S-C-UPWR-G model, IE4500-28S-G model, IE4500-28F-G model, IE4520-56S-C-G model.

IE4520 Series, H3C Comware Software Version 7.1.070 Release 6816

IE4520-30S-C model

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

MX Series (240, 480, 960) con tarjetas MPC10E y MX-SPC3

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

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

CCN-STIC-1456 Procedimiento de Empleo Seguro Juniper Routers MX Series

EX 9200 Series (9204, 9208, 9214) con tarjetas EX9200-15C

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las 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 de las funcionalidades de seguridad. Como switch de nivel 2 en la capa OSI, realiza un análisis de los 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 trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

EX3400 Series (3400-24T|24P|48T|48P)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las 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 de las funcionalidades de seguridad. Como switch de nivel 2 en la capa OSI, realiza un análisis de los 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 trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

QFX Series (5120-48YM|48T|48Y|32C, 5200-48Y|32C, 5210-64C) y EX4650-48Y

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

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 Procedimiento de Empleo Seguro Juniper QFX Series

QFX Series (QFX5700)

Versión	Junos OS 24.4R1-EVO
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

Descripción

La línea QFX5700 que incluye el QFX5700 y QFX5700E admite funciones avanzadas de Capa 2, Capa 3 y EVPN-VXLAN. La plataforma está diseñada para su uso en centros de datos, campus, interconexión de centros de datos (DCI) y conexión de clústeres de firewall. La elección de velocidad de interfaz para la conectividad de servidores o dentro de un solución de fabric permite versatilidad en el despliegue y protección de la inversión.
Los proveedores de nube pública y de servicios que buscan satisfacer el crecimiento explosivo obtienen soporte de puertos 400GbE a escala de Internet. Para los clientes empresariales que están haciendo la transición de sus granjas de servidores de 10GbE a 25GbE, el QFX5700 proporciona la opción de ser usado como spine para arquitectura EVPN-VXLAN de 100GbE/400GbE con bajo consumo de energía en un espacio reducido. Con hasta 25.6 Tbps de rendimiento bidireccional, el switch está optimizado para despliegues de leaf & spine en centros de datos empresariales, computación de alto rendimiento, proveedores de servicios o en la nube.

Observaciones

CCN-STIC-1440 Procedimiento de Empleo Seguro Juniper QFX Series

EX4100 Series (4100-24P|24T|24MP|48P|48T|48MP|F-12P|F-24P|F-48P|F-12T|F-24T|F-48T)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

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, reenvia 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

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

EX2300 Series (EX2300-C-12T|12P|24T|24P|48T|48P|24MP|48MP)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las 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 de las funcionalidades de seguridad. Como switch de nivel 2 en la capa OSI, realiza un análisis de los 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 trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1472 Procedimiento de Empleo Seguro Juniper EX Switches

HPE Aruba Networking CX 4100i, 6000, 6100, 6200, 6300, 6400, 8100, 8320, 8325, 8360, 8400, 9300, y 10000



Versión	10.13
Fabricante	HPE Aruba Networking
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2027

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

CCN-STIC 1432 Procedimiento de Empleo Seguro Aruba CX Series

H3C S5500 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	02/02/2026
Revisión de Validez	30/11/2029

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.
Modelos:

S5500 Series

- S5570S-28S-EI, S5570S-54S-EI, S5570S-54F-EI, S5570S-36F-EI ,S5570S-54S-PWR-EI-A, S5570S-28S-HPWR-EI-A, S5560X-30C-EI, S5560X-54C-EI, S5560X-30C-PWR-EI, S5560X-54C-PWR-EI, S5560X-30F-EI, S5560X-54F-EI, S5560X-34S-EI, S5560X-54S-EI, S5560X-30F-EIF, S5590-28T8XC-EI ,S5590-48T4XC-EI, S5590-28S8XC-EI, S5590-48S4XC-EI, S5590-28P8XC-EI, S5590-48P6XC-EI, S5590-48TS4X2QC-EI, S5590-24X4YC-EI, S5590-24UXM4YC-EI, S5590-48UXM4YC-EI, S5590-24UXMC-EI, S5590-32UN4X4Y2CC-EI, S5590-48UN4Y2CC-EI,, S5590-48UM4YC-EI.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

ACX Series (5448, 5448-M, 5448-D)

Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

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 Procedimiento de Empleo Seguro ACX Routers

Atlas-840, M10-Smart Series, M2 Series, 4GePlus Series, Teldat-5Ge Series, 5Ge-Rail Series, Connect-4GePlus Series, Connect-5Ge Series, Connect-FW Series, Regesta SmartV2 Series, H5 Rail Series	
Versión	11.02.04.85.02
Fabricante	TELDAT
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	28/02/2028

Descripción

Familia de routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones

Observaciones

CCN-STIC 1471 Procedimiento de Empleo Seguro Teldat Router

H3C 7500 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	02/02/2026
Revisión de Validez	30/11/2029

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.
Modelos:

S7500 Series

- S7503X, S7503E-M, S7506X-POE, S7506X-S, S7510X-POE, S7503X-M-G, S7503X-G, S7506X-G-POE, S7510X-G-POE, S7506X-G, S7510X-G, S7506X-G-MF.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

H3C S5000 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	02/02/2026
Revisión de Validez	30/11/2029

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.
Modelos:

S5000 Series

- S5000NV6-12T4N4NS-EI, S5000NV6-12P4UN4NS-EI, S5000NV6-20T4N4NS-EI, S5000NV6-20P4UN4NS-EI, S5000NV6-48T4NS-EI, S5000NV6-48P4NS-EI, S5000NV6-4T4N2NS-EI, S5000NV6-4P4UN2NS-EI.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

H3C 12500 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	02/02/2026
Revisión de Validez	30/11/2029

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.
Modelos:

S12500 Series

- S12504X-AF, S12508X-AF, S12516X-AF, S12504G-AF, S12508G-AF, S12516G-AF, S12504G-AF (Type S), S12508G-AF (Type S), S12516G-AF (Type S), S12504CR (Type S), S12508CR (Type S), S12516CR (Type S).

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

Juniper PTX10000 Series (PTX10004, PTX10016, PTX10001-36MR, PTX10002-36QDD)

Versión	JunOs 23.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/03/2026
Revisión de Validez	29/02/2028

Descripción

La familia de routers PTX10k de HPE Juniper Networking está diseñada para ofrecer un rendimiento extremo en redes IP/MPLS de alto rendimiento, combinando capacidades avanzadas de routing y switching con sólidas funciones de seguridad integradas. Basados en la arquitectura de ASIC Express, proporcionan alta capacidad de conmutación, baja latencia y alta eficiencia energética, ideales para operadores y grandes proveedores de servicios. La familia PTX incorporan protección a nivel de infraestructura, mitigación de ataques DDoS y telemetría en tiempo real para detectar anomalías. Sus funcionalidades de segmentación de red en capa L2 y L3 basadas en estándares de la industria, el control del plano de routing y la compatibilidad con protocolos como MP-BGP, IS-IS, MPLS y SRv6 garantizan un enrutamiento basado en estándares, fiable, seguro y escalable en entornos redes WAN y centros de datos de misión crítica.

Observaciones

Pendiente PES

Juniper MX Series (10004, 10008, 10016)

Versión	JunOS 23.4R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/03/2026
Revisión de Validez	29/02/2028

Descripción

Las plataformas de enrutamiento universal MX10000, compuestas por el MX10003, MX10004, MX10008, MX10016, 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 MX es altamente escalable desde desde los 2.4Tbps en 3U, pasando por 38,4 Tbps en 7 slots hasta un rendimiento de 76,8 Tbps en 13 slots.

Observaciones

H3C 10500 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	02/02/2026
Revisión de Validez	30/11/2029

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.
Modelos:

S10500 Series

-,S10506X, S10508X, S10510X, S10506X-G, S10508X-G, S10512X-G, S10506X-G-PoE, S10512X-G-PoE.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

H3C 6500 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	02/02/2026
Revisión de Validez	30/11/2029

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.
Modelos:

S6500 Series

- S6520X-18C-SI, S6520X-26C-SI, S6520X-26MC-UPWR-SI, S6520X-26MC-SI, S6520X-16ST-SI, S6520X-24ST-SI, S6520X-10XT-SI, S6520X-16XT-SI, S6520X-26XC-UPWR-SI, S6520X-54XC-UPWR-SI, S6520X-30HC-EI, S6520X-30QC-EI, S6520X-54HC-EI, S6520X-54QC-EI, S6520X-54HC-HI, S6520X-54QC-HI, S6520X-30HC-HI, S6520X-30QC-HI, S6520X-54HF-EI, S6520X-54HF-HI, S6520X-30HF-EI, S6520X-30HF-HI, S6520X-54HC-UPWR-EI, S6526XE-48X4CC-EI, S6526XE-32X4CC-EI, S6526XE-32X6CC-HI, S6526XE-48X6CC-HI.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

H3C 6800 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	02/02/2026
Revisión de Validez	30/11/2029

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.
Modelos:

S6800 Series

- S6890-54HF, S6890-30HF, S6890-44HF, S6825-54HF, S6805-54HF, S6805-54HT, S6850-56HF ,S6850-2C ,S6800-54HT, S6800-54HF, S6800-32Q-H1, S6800-2C-H1, S6800-4C-H1, S6800-54QF-H3, S6800-54QT-H3, S6800-54QF-H5, S6812-24X6C, S6812-48X6C, S6813-24X6C, S6813-48X6C, S6805-54HF-H1 , S6805-54HT-H1, S6850-56HF-H1, S6850-56HF-SAN.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

H3C 9800 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	02/02/2026
Revisión de Validez	30/11/2029

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.
Modelos:

S9800 Series

- S9820-8C, S9820-8C-SAN, S9850-32H, S9850-4C, S9850-32H-H1, S9850-4C-H1, S9820-64H, S9820-64H-H1, S9820-8M, S9850-32H-G.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

H3C S5100 Series

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	02/02/2026
Revisión de Validez	30/11/2029

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.
Modelos:

S5100 Series

- S5130S-28T8X-EI-G-V2, ,S5130S-48T6X-EI-G-V2, S5130S-24UN8X-EI-G-V2, S5130S-48UN6X-EI-G-V2, S5136S-48P4S-EI, S5136S-8FP4XS-EI-Q, S5136S-24FP4T4S-EI, S5136S-48T4S-EI-Q, S5136S-24T4X-EI-Q, S5136S-48S2T4X-EI, S5136S-10T4X-EI-Q, S5136S-16FP4X-EI, S5136S-24P4X-EI, S5136S-48FP4X-EI, S5136S-48P4X-EI, S5136S-24T4S-EI-Q, S5136S-16T4X-EI-Q, S5136S-24S8T4X-EI, S5136S-48ST4X-EI, S5136S-48FP4S-EI, S5136S-24FP4S4X-EI, S5136S-8T4XS-EI-Q, S5136S-10FPT4X-EI-Q, S5136S-48T4X-EI-Q, S5130S-28S-HI, S5130S-52S-HI, S5130S-28S-PWR-HI, S5130S-52S-PWR-HI, S5130S-28C-HI, S5130S-52C-HI, S5130S-28C-PWR-HI, S5130S-52C-PWR-HI, S5130S-10P-EI, S5130S-12TP-EI, S5130S-20P-EI, S5130S-28P-EI, S5130S-52P-EI, S5130S-10P-HPWR-EI, S5130S-12TP-HPWR-EI, S5130S-20P-PWR-EI, S5130S-28P-PWR-EI, S5130S-28P-HPWR-EI, S5130S-52P-PWR-EI, S5130S-28S-EI, S5130S-52S-EI, S5130S-28F-EI, S5130S-52F-EI, S5130S-28TP-EI, S5130S-52TP-EI, S5130S-28S-PWR-EI, S5130S-28S-HPWR-EI, S5130S-52S-PWR-EI, S5170-28S-EI, S5170-54S-EI, S5170-54S-PWR-EI, S5170-28S-HPWR-EI.

Observaciones

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

8.5.3 CORTAFUEGOS

Check Point Maestro Hyperscale Appliances (CPAP-MHO-140, CPAP-MHO-175-xC)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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 15000 (CPAP-SG15400, CPAP-SG15600)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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	

CloudGuard Network (VMware ESXi/NSX)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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 Threat Emulation/Extraction (CPAP-SBTE250XN y CPAP-SBTE2000XN)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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 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
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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 6000 (CPAP-SG6200, CPAP-SG6400, CPAP-SG6600, CPAP-SG6700, CPAP-SG6900)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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 26000 y 28000 (CPAP-SG26000, CPAP-SG28000, CPAP-SG28600)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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 7000 (CPAP-SG7000)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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

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
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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

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
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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 3000 (CPAP-SG3100, CPAP-SG3200, CPAP-SG3600, CPAP-SG3800)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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 N120 series (N120, N120W, N120WL) y N60	
Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	29/09/2027
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

Stormshield Network Security UTM/NG-Firewall (Appliances desde SN210 a SN6200 en 4 compilaciones distintas: i, xr, XS, S, M, L y XL) y modelos virtuales (SNEVA1 a SNEVA4 y SNEVAU)	
Versión	4.3
Fabricante	Stormshield
Familia	Cortafuegos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2024
Revisión de Validez	31/03/2027
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

CCN-STIC 1415 Procedimiento de Empleo Seguro UTM/NG-Firewall de Stormshield

Sophos Firewall

Versión	SFOS v20.0
Fabricante	Sophos
Familia	Cortafuegos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/02/2026
Revisión de Validez	31/01/2027

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

CCN-STIC 1469 Procedimiento de Empleo Seguro Sophos Firewall

Aruba Mobility Controller (9004, 9012, 9240, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) y puntos de acceso (serie 200, 300, 500 y 600)

Versión	ArubaOS 8.10
Fabricante	HPE Aruba Networking
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	13/04/2027

Descripción

Los HPE Aruba Mobility Controllers, junto con los APs de las series 200, 300, 500 y 600, permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan características de seguridad avanzadas en el control de acceso a la red, en la asignación de políticas de seguridad por usuario mediante el uso de roles, así como la posibilidad de despliegues multizona y terminación de túneles VPN. También se soportan mecanismos de monitorización de espectro y wireless IDS/IPS.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS Controladoras y Puntos de Acceso

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
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027

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 rugerizado 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

Atlas-840, M10-Smart Series, M2 Series, 4GePlus Series, Teldat-5Ge Series, 5Ge-Rail Series, Connect-4GePlus Series, Connect-5Ge Series, Connect-FW Series, Regesta SmartV2 Series, H5 Rail Series

Versión	11.02.04.85.02
Fabricante	TELDAT
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	29/02/2028

Descripción

Familia de routers corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones

Observaciones

CCN-STIC 1471 Procedimiento de Empleo Seguro Teldat Router

CIBER ARMOUR CLAVISTER COS CORE

Versión	15.00 VE
Fabricante	CLAVISTER
Familia	Cortafuegos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2026
Revisión de Validez	28/02/2027

Descripción

Clavister cOS Core es el software Next Generation Firewall (NGFW) que se despliega tanto en el hardware Clavister NetWall como en el hardware de grado militar Clavister CyberArmour RSG, o en entornos virtualizados. Funcionalidades clave que permite gestionar y protecciones que ofrece: IP Routing: Estático, Dinámico, Virtual, Multicast. Políticas Firewall: Stateful para TCP, UDP e ICMP. Traducción de direcciones: Basada en políticas, Traducción Dinámica (NAT) y Estática (SAT). Detección de Anomalías por IA: Análisis de series temporales mediante machine learning para detecciones en tiempo real. ALG's. VPN: IPsec, L2TP, L2TPv3, PPTP, y SSL VPN. Terminación TLS/SSL. Control de Aplicación. Escáner Anti-Virus. Capacidades IDP (Intrusion Detection and Prevention). Filtrado por contenido Web. Gestión del tráfico: Traffic Shaping, Threshold Rules y Server Load Balancing. Autenticación de usuarios. Interfaz de usuario basada en web, CLI, REST API, logging, SNMP, Cloud-Init. Alta Disponibilidad (HA) Activa y pasiva. Routers Virtuales. Soporte IPv6. ZoneDefense. Virtualización: VMware, KVM (x86 y ARM) e Hyper-V. Adicionalmente: RADIUS, Accounting, DHCP, protección DoS, PPPoE, GRE, DNS dinámico.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

Forcepoint Virtual Appliance (ESXi)

Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	29/09/2027

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

Forcepoint NGFW 3400 series (N3401, N3405, N3410)

Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	29/09/2027

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 2200 series (N2201, N2205, N2210)

Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	29/09/2027

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

Check Point Security Gateway Serie 23000 (CPAP-SG23500, CPAP-SG23800, CPAP-SG23900)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/05/2027
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	

SRX Series (300, 320, 340, 345, 345-DUAL-AC, 380, 1500, 1600, 2300, 4100, 4200, 4300, 4600, 5400, 5600, 5800)_	
Versión	Junos OS 24.4R1
Fabricante	Juniper Networks
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	30/09/2027

Descripción

La familia de firewall mid-range de Juniper Networks® 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 Procedimiento de Empleo Seguro Juniper SRX Series

Aruba Virtual Mobility Controllers (MC-VA-50, MC-VA-250 y MC-VA-1k) y puntos de acceso (serie 200, 300, 500 y 600)	
Versión	ArubaOS 8.10
Fabricante	HPE Aruba Networking
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	13/04/2027

Descripción

Los HPE Aruba Mobility Controllers, junto con los APs de las series 200, 300, 500 y 600, permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan características de seguridad avanzadas en el control de acceso a la red, en la asignación de políticas de seguridad por usuario mediante el uso de roles, así como la posibilidad de despliegues multizona y terminación de túneles VPN. También se soportan mecanismos de monitorización de espectro y wireless IDS/IPS.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS Controladoras y Puntos de Acceso

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	
Versión	PAN-OS 11.0
Fabricante	Palo Alto Networks
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

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

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

FortiGate - Familia F

Versión	FortiOS 7.2
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	01/10/2026
Revisión de Validez	31/07/2028

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.
Modelos:
FortiGate-40F, ,FortiGate-40F-3G4G, FortiWifi-40F, FortiWifi-40F-3G4G, FortiGate-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-60F, FortiWifi-60F, FortiGate-61F, FortiGateRugged-70F, FortiGateRugged-70F-3G4G, FortiGate-70F, FortiGate-71F, FortiGate-80F, FortiGate-80F-PoE, FortiWifi-80F-2R, FortiWifi-80F-2R-3G4G-DSL, FortiGate-81F, FortiWifi-81F-2R-3G4G-DSL, FortiGate-81F-PoE, FortiWifi-81F-2R, FortiWifi-81F-2R-3G4G-PoE, FortiWifi-81F-2R-PoE, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-200F, FortiGate-201F, FortiGate-400F, FortiGate-600F, FortiGate-601F, FortiGate-1000F, FortiGate-1001F, FortiGate-1800F, FortiGate-1800F-DC, FortiGate-1801F, FortiGate-1801F-DC, FortiGate-2600F, FortiGate-2601F, FortiGate-2601F-DC, FortiGate-3000F, FortiGate-3000F-DC, FortiGate-3001F, FortiGate-3001F-DC, FortiGate-3200F, FortiGate-3201F, FortiGate-3500F, FortiGate-35011F, FortiGate-3700F, FortiGate-3701F, FortiGate-4200F, FortiGate-4200F-DC, FortiGate-4201F, FortiGate-4201F-DC, FortiGate-4400F, FortiGate-4400F-DC, FortiGate-4401F, FortiGate-4401F-DC, FortiGate-4800F, FortiGate-4801F, FortiGate-6001F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F.

Observaciones

CCN-STIC 1406 Procedimiento de Empleo Seguro FortiGate 7

FortiGate - Familia G

Versión	FortiOS 7.2
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	01/10/2026
Revisión de Validez	31/07/2028

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.
Modelos:
FortiGate-30G, FortiGate-31G, FortiGate-70G, FortiGate-70G-POE, FortiGate-71G, FortiGate-71G-POE, FortiGate-90G, FortiGate-91G, FortiGate-120G, FortiGate-121G, FortiGate-200G, FortiGate-201G, FortiGate-700G, FortiGate-701G, FortiGate-900G, FortiGate-900G-DC, FortiGate-901G, FortiGate-901G-DC, FortiWifi-30G, FortiWifi-31G, FortiWifi-70G, FortiWifi-71G, FortiWifi-70G-POE.

Observaciones

CCN-STIC 1406 Procedimiento de Empleo Seguro FortiGate 7

OPNsense Business Edition

Versión	25.4
Fabricante	Deciso B.V
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2027

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

OPNsense Business Edition

Versión	25.10
Fabricante	Deciso B.V
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2027

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

OPNsense Business Edition

Versión	26.4
Fabricante	Deciso B.V
Familia	Cortafuegos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	30/06/2026
Revisión de Validez	31/07/2027

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

FortiGate - Familia E

Versión	FortiOS 7.2
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	01/10/2026
Revisión de Validez	31/07/2028

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.
Modelos:
FortiGate-60E, FortiGate-60E-PoE, FortiGate-60E-DSL, FortiWifi-60E, FortiWifi-60E-DSL, FortiWifi-60E-DSLJ, FortiGate-61E, FortiWifi-61E, FortiGate-80E, FortiGate-80E-PoE, FortiGate-81E, FortiGate-81E-PoE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-140E, FortiGate-140E-PoE, FortiGate-200E, FortiGate-201E, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-401E, FortiGate-401E-DC, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-601E, FortiGate-1100E, FortiGate-1100E-DC, FortiGate-1101E, FortiGate-1101E-DC, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3400E-DC, FortiGate-3401E, FortiGate-3401E-DC, FortiGate-3600E, FortiGate-3600E-DC, FortiGate-3601E, FortiGate-3960E, FortiGate-3960E-DC, FortiGate-3980E, FortiGate-3980E-DC, FortiGate-50001E1.

Observaciones

CCN-STIC 1406 Procedimiento de Empleo Seguro FortiGate 7

8.5.4 DISPOSITIVOS DE RED INALÁMBRICOS

FortiAP	
Versión	7.2.0
Fabricante	Fortinet
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2026
Revisión de Validez	31/12/2028
Descripción	

Los puntos de acceso inalámbricos Fortinet, integrados con FortiGate (siendo posible integrarlo con cualquier versión y modelo cualificado de FortiGate), proporcionan conectividad WiFi segura en el perímetro de red. La solución está diseñada sobre FortiOS y puede gestionarse de forma centralizada mediante FortiManager (con cualquier versión y modelo cualificado). La arquitectura permite despliegues en modo controlado o distribuido, y proporciona segmentación dinámica de usuarios, autenticación 802.1X, visibilidad completa del tráfico, y políticas de acceso unificadas. Su integración con Fortinet Security Fabric permite aplicar análisis de amenazas, filtrado de contenido y respuesta automatizada a incidentes en entornos corporativos, educativos y críticos.

Observaciones

CCN-STIC 1485 Procedimiento de Empleo Seguro FortiAP v7.2.0

Aruba Mobility Controller (9004, 9012, 9240, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) y puntos de acceso (serie 200, 300, 500 y 600)	
Versión	ArubaOS 8.10
Fabricante	HPE Aruba Networking
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	13/04/2027
Descripción	

Los HPE Aruba Mobility Controllers, junto con los APs de las series 200, 300, 500 y 600, permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan características de seguridad avanzadas en el control de acceso a la red, en la asignación de políticas de seguridad por usuario mediante el uso de roles, así como la posibilidad de despliegues multizona y terminación de túneles VPN. También se soportan mecanismos de monitorización de espectro y wireless IDS/IPS.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS Controladoras y Puntos de Acceso

Aruba Virtual Mobility Controllers (MC-VA-50, MC-VA-250 y MC-VA-1k) y puntos de acceso (serie 200, 300, 500 y 600)	
Versión	ArubaOS 8.10
Fabricante	HPE Aruba Networking
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	13/04/2027

Descripción

Los HPE Aruba Mobility Controllers, junto con los APs de las series 200, 300, 500 y 600, permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan características de seguridad avanzadas en el control de acceso a la red, en la asignación de políticas de seguridad por usuario mediante el uso de roles, así como la posibilidad de despliegues multizona y terminación de túneles VPN. También se soportan mecanismos de monitorización de espectro y wireless IDS/IPS.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS Controladoras y Puntos de Acceso

8.5.5 PASARELAS SEGURAS DE INTERCAMBIO DE DATOS

PSTatx	
Versión	1.7
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026
Descripción	

PSTatx es una pasarela segura de nivel de aplicación orientada a entornos militares y de defensa, basada en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL 4+ (AVA_VAN.5 + ALC_FLR.3).
PSTatx permite el intercambio controlado de Información de vigilancia aérea ASTERIX entre dominios de seguridad (cross-domain).
Más información: https://www.autek.es/cross-domain/pstgateways

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

PSTgateways Custom	
Versión	4.13
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026
Descripción	

PSTgateways es una familia de pasarelas seguras de nivel de aplicación que permiten el intercambio controlado de información entre dominios de seguridad (cross-domain). Todos los productos están basados en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL4+ (AVA_VAN.5 + ALC_FLR.3).
Los productos PSTgateways personalizados permiten combinaciones de servicios y/o filtros de datos (formato y contenido) a medida. Pueden incorporar comprobaciones de etiquetado de seguridad (STANAGs 4774/4778).

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

PSTacp

Versión	1.7
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

Descripción

PSTacp es una pasarela segura de nivel de aplicación orientada a entornos militares y de defensa, basada en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL 4+ (AVA_VAN.5 + ALC_FLR.3).
PSTacp permite el intercambio controlado de mensajería ACP-127 entre dominios de seguridad (cross-domain).
Más información: https://www.autek.es/cross-domain/pstgateways

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

PSTmip

Versión	1.7
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

Descripción

PSTmip es una pasarela segura de nivel de aplicación orientada a entornos militares y de defensa, basada en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL 4+ (AVA_VAN.5 + ALC_FLR.3).
PSTmip permite el intercambio controlado de datos tácticos MIP4 con comprobación de etiquetado y firma digital (STANAG 4774/8) entre Sistemas de mando y control desplegados en diferentes dominios de seguridad (cross-domain).
Más información: https://www.autek.es/cross-domain/pstgateways

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

PSTjreap

Versión	1.7
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

Descripción

PSTjreap es una pasarela segura de nivel de aplicación orientada a entornos militares y de defensa, basada en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL 4+ (AVA_VAN.5 + ALC_FLR.3).
PSTjreap permite el intercambio controlado de información Tactical Data Link mediante JREAP-C entre dominios de seguridad (cross-domain).
Más información: https://www.autek.es/cross-domain/pstgateways

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

PSTgateways (PSTfile, PSTmail, PSTudp)

Versión	4.13
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

Descripción

PSTgateways es una familia de pasarelas seguras de nivel de aplicación que permiten el intercambio controlado de información entre dominios de seguridad (cross-domain). Todos los productos están basados en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common CriteriaEAL4+ (AVA_VAN.5 + ALC_FLR.3). Productos de propósito general:
PSTfile: servicios de transferencia automática de ficheros.
PSTmail: servicios de transferencia de mensajes de correo electrónico.
PSTudp: servicios de transferencia de payload de paquetes UDP.
Más información: https://www.autek.es/cross-domain/pstgateways

Observaciones

Procedimiento de empleo seguro: CCN-STIC-1401 Configuración segura de pasarelas de AUTEK

PSTcsd

Versión	1.7
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

Descripción

PSTcsd es una pasarela segura de nivel de aplicación orientada a entornos militares y de defensa, basada en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL 4+ (AVA_VAN.5 + ALC_FLR.3).
PSTcsd permite el intercambio controlado de información JISR (MAJIIC) entre dominios de seguridad (cross-domain).
Más información: https://www.autek.es/cross-domain/pstgateways

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

PSTgateways Web services (PSTws)

Versión	1.7
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/02/2026
Revisión de Validez	30/11/2026

Descripción

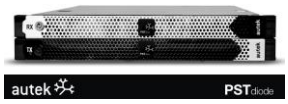
PSTgateways es una familia de pasarelas seguras de nivel de aplicación que permiten el intercambio controlado de información entre dominios de seguridad (cross-domain). Todos los productos están basados en el núcleo común PSTgateways Framework 4.16.8-A, certificado Common Criteria EAL4+ (AVA_VAN.5 + ALC_FLR.3).
Los productos PSTgateways basados en web services soportan flujos de datos a través de protocolo HTTP/s, permiten filtros a medida de formato y contenido sobre APIs REST o SOAP. Pueden incorporar comprobaciones de etiquetado de seguridad (STANAGs 4774/4778).
Más información: https://www.autek.es/cross-domain/pstgateways

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

8.5.6 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	31/10/2026





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

8.5.7 PROTECCIÓN DE CORREO ELECTRÓNICO

Fortimail	
Versión	7.4
Fabricante	Fortinet
Familia	Protección de correo electrónico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2026
Revisión de Validez	31/12/2027
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

CCN-STIC 1614 Procedimiento de Empleo Seguro FortiMail

8.5.8 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
Familia	Balanceadores de carga
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/06/2027

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

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
Familia	Balanceadores de carga
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	30/06/2027

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

8.6 PROTECCIÓN DE LAS COMUNICACIONES

8.6.1 HERRAMIENTAS VOZ IP

COMSec Admin +	
Versión	v5.1
Fabricante	Indra
Familia	Herramientas Voz IP
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/03/2026
Revisión de Validez	31/10/2026

Descripción

COMSec Admin + es una solución global de comunicaciones seguras que proporciona servicios cifrados resistentes a computación cuántica con mecanismos de hibridación de criptografía clásica y PQC en el ámbito de voz, mensajería instantánea y videollamada sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con 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 Admin + son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: www.indragroup.com

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Secret.T (iOS)

Versión	1.18
Fabricante	Telefónica Soluciones de Criptografía
Familia	Herramientas Voz IP
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/08/2027

Descripción

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

Secret.T (Android)

Versión	1.15
Fabricante	Telefónica Soluciones de Criptografía
Familia	Herramientas Voz IP
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	24/03/2025
Revisión de Validez	30/08/2027

Descripción

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

8.6.2 HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA (IM)

COMSec Admin +	
Versión	v5.1
Fabricante	Indra
Familia	Herramientas de mensajería instantánea (IM)
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/03/2026
Revisión de Validez	31/10/2026
Descripción	

COMSec Admin + es una solución global de comunicaciones seguras que proporciona servicios cifrados resistentes a computación cuántica con mecanismos de hibridación de criptografía clásica y PQC en el ámbito de voz, mensajería instantánea y videollamada sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con 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 Admin + son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: www.indragroup.com

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Secret.T (iOS)	
Versión	1.18
Fabricante	Telefónica Soluciones de Criptografía
Familia	Herramientas de mensajería instantánea (IM)
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/08/2027
Descripción	

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

Secret.T (Android)

Versión	1.15
Fabricante	Telefónica Soluciones de Criptografía
Familia	Herramientas de mensajería instantánea (IM)
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	24/03/2025
Revisión de Validez	30/08/2027

Descripción

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

8.6.3 HERRAMIENTAS DE VIDEOCONFERENCIA

Secret.T (iOS)	
Versión	1.18
Fabricante	Telefónica Soluciones de Criptografía
Familia	Herramientas de videoconferencia
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/08/2027
Descripción	

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

Secret.T (Android)	
Versión	1.15
Fabricante	Telefónica Soluciones de Criptografía
Familia	Herramientas de videoconferencia
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	24/03/2025
Revisión de Validez	30/08/2027
Descripción	

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

8.6.4 REDES PRIVADAS VIRTUALES: OTRAS

EP960	
Versión	1.09.17
Fabricante	Epicom
Familia	Redes privadas virtuales: Otras
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/09/2020
Revisión de Validez	31/12/2026
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.

EP430GX	
Versión	v.1.08
Fabricante	Epicom
Familia	Redes privadas virtuales: Otras
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2027
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	Redes privadas virtuales: Otras
Tipo	Producto
Clasificación	RESERVADO
Fecha Inclusión	01/12/2022
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	1.12
Fabricante	Epicom
Familia	Redes privadas virtuales: Otras
Tipo	Producto
Clasificación	RESERVADO
Fecha Inclusión	01/12/2022
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	2.5
Fabricante	Epicom
Familia	Redes privadas virtuales: Otras
Tipo	Producto
Clasificación	RESERVADO
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.

EP430TX





Versión	1.04
Fabricante	Epicom
Familia	Redes privadas virtuales: Otras
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2027

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.

EP430GU/B

Versión	2.01
Fabricante	Epicom
Familia	Redes privadas virtuales: Otras
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	01/09/2020
Revisión de Validez	31/12/2026



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 1Gpbs, 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

8.7 PROTECCIÓN DE LA INFORMACIÓN

8.7.1 ALMACENAMIENTO CIFRADO DE DATOS

Cryhod.def.es	
Versión	2024.4
Fabricante	PrimX/Epicom
Familia	Almacenamiento cifrado de datos
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/02/2026
Revisión de Validez	31/07/2027

Descripción

Cryhod.def.es es un programa de cifrado moderno que asegura el cifrado completo de los discos duros de las estaciones de trabajo de la organización con criptografía específica para el Ministerio de Defensa y organismos dependientes. Cryhod.def.es, al igual que Cryhod, implementa mecanismos 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. Es especialmente recomendable su uso en sistemas sensibles (ENS ALTO) o que manejen información clasificada.

Observaciones

CCN-STIC-1523 Procedimiento de Empleo Seguro Cryhod .DEF y .GOB de PRIM'x personalizado por EPICOM

8.7.2 CIFRADO Y COMPARTICIÓN SEGURA DE INFORMACIÓN

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	3.05
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2026
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)

GuardedBox-NAR

Versión	11.0.0
Fabricante	GuardedBox
Familia	Cifrado y compartición segura de información
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/01/2028

Descripción

GuardedBox-NAR es una solución con cifrado post-cuántico (PQC) extremo a extremo (E2E) para almacenamiento e intercambio seguro en tiempo real de todo tipo de información sensible (incluyendo ficheros sin límite de tamaño), gracias a un esquema flexible de plantillas personalizables que permiten modelizar cualquier tipo de dato: contraseñas, certificados, informes, logs, evidencias, grabaciones, etc.

Su modelo de compartición flexible permite gestionar los secretos de la organización de forma individual y/o colaborativa, y tanto con usuarios internos como externos a la organización, asegurando el control y la total trazabilidad sobre la información. Entre estas capacidades de control, figuran: estado actual e histórico de compartición, notificaciones, recordatorios, borrado programado y etiquetado de la información.

El panel de administración permite la gestión avanzada de usuarios y proporciona un módulo de auditoría inmutable (basado en tecnología blockchain) que registra toda la actividad de los usuarios.

Ofrece un SDK que permite la personalización e integración con otras soluciones del entorno, extendiendo las capacidades de protección post-cuántica a otros servicios de la organización.

GuardedBox-NAR opera como una solución web que puede desplegarse on-premise o en nube, implementando férreas medidas de zero-knowledge y zero-trust que protegen los datos incluso frente a compromisos del servidor. Más información: https://guardedbox.es

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

8.7.3 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	28/02/2027

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

8.7.4 GESTIÓN DE METADATOS

MetaOLVIDO for Zimbra	
Versión	3.6.0
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	30/04/2025
Revisión de Validez	30/10/2027

Descripción

Plugin para Zimbra que procesa automáticamente los metadatos de los ficheros adjuntos de los e-mails enviados por toda la organización, evitando de esta manera la fuga de información sensible que se produce de forma continuada en este tipo de comunicaciones y reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario.
• Los metadatos e información oculta serán procesados independientemente del cliente de correo utilizado (cliente de escritorio, cliente web, tablet o smartphone).
• Permite configurar los tipos de ficheros a procesar (Microsoft Office, Open/Libre Office, PDF y más de 150 extensiones de ficheros de imagen, audio y vídeo).
• Permite eliminar todos los metadatos o aplicar plantillas de metadatos.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente manteniendo la validez de la firma electrónica.
• Permite configurar dominios de exclusión (WhiteList) para el procesado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

MetaOLVIDO for Postfix

Versión	3.6.0
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	30/04/2025
Revisión de Validez	30/10/2027

Descripción

Plugin para Postfix que procesa automáticamente los metadatos de los ficheros adjuntos de los e-mails enviados por toda la organización, evitando de esta manera la fuga de información sensible que se produce de forma continuada en este tipo de comunicaciones y reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario.
• Los metadatos e información oculta serán procesados independientemente del cliente de correo utilizado (cliente de escritorio, cliente web, tablet o smartphone).
• Permite configurar los tipos de ficheros a procesar (Microsoft Office, Open/Libre Office, PDF y más de 150 extensiones de ficheros de imagen, audio y vídeo).
• Permite eliminar todos los metadatos o aplicar plantillas de metadatos.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente manteniendo la validez de la firma electrónica.
• Permite configurar dominios de exclusión (WhiteList) para el procesado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

MetaOLVIDO for Exchange

Versión	5.0.1
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	30/04/2025
Revisión de Validez	30/10/2027

Descripción

Plugin para Exchange que procesa automáticamente los metadatos de los ficheros adjuntos de los e-mails enviados por toda la organización, evitando de esta manera la fuga de información sensible que se produce de forma continuada en este tipo de comunicaciones y reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario.
• Los metadatos e información oculta serán procesados independientemente del cliente de correo utilizado (cliente de escritorio, cliente web, tablet o smartphone).
• Permite configurar los tipos de ficheros a procesar (Microsoft Office, Open/Libre Office, PDF y más de 150 extensiones de ficheros de imagen, audio y vídeo).
• Permite eliminar todos los metadatos o aplicar plantillas de metadatos.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente manteniendo la validez de la firma electrónica.
• Permite configurar dominios de exclusión (WhiteList) para el procesado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

MetaClean Sync Workstation y MetaClean Sync Server	
Versión	3.0.1
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/05/2024
Revisión de Validez	01/11/2028

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 for Zimbra

Versión	3.6.0
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	16/02/2025
Revisión de Validez	30/07/2027

Descripción

Plugin para Zimbra que procesa automáticamente los metadatos de los ficheros adjuntos de los e-mails enviados por toda la organización, evitando de esta manera la fuga de información sensible que se produce de forma continuada en este tipo de comunicaciones y reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario.
• Los metadatos e información oculta serán procesados independientemente del cliente de correo utilizado (cliente de escritorio, cliente web, tablet o smartphone).
• Permite configurar los tipos de ficheros a procesar (Microsoft Office, Open/Libre Office, PDF y más de 150 extensiones de ficheros de imagen, audio y vídeo).
• Permite eliminar todos los metadatos o aplicar plantillas de metadatos.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente manteniendo la validez de la firma electrónica.
• Permite configurar dominios de exclusión (WhiteList) para el procesado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

metaOLVIDO Endpoint y metaOLVIDO Server	
Versión	3.0.1
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/05/2024
Revisión de Validez	01/11/2028

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

MetaClean for Exchange

Versión	5.0.1
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	16/02/2025
Revisión de Validez	30/07/2027

Descripción

Plugin para Exchange que procesa automáticamente los metadatos de los ficheros adjuntos de los e-mails enviados por toda la organización, evitando de esta manera la fuga de información sensible que se produce de forma continuada en este tipo de comunicaciones y reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario.
• Los metadatos e información oculta serán procesados independientemente del cliente de correo utilizado (cliente de escritorio, cliente web, tablet o smartphone).
• Permite configurar los tipos de ficheros a procesar (Microsoft Office, Open/Libre Office, PDF y más de 150 extensiones de ficheros de imagen, audio y vídeo).
• Permite eliminar todos los metadatos o aplicar plantillas de metadatos.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente manteniendo la validez de la firma electrónica.
• Permite configurar dominios de exclusión (WhiteList) para el procesado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

MetaClean for Postfix

Versión	3.6.0
Fabricante	Adarsus Technologies
Familia	Gestión de metadatos
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	16/02/2025
Revisión de Validez	30/07/2027

Descripción

Plugin para Postfix que procesa automáticamente los metadatos de los ficheros adjuntos de los e-mails enviados por toda la organización, evitando de esta manera la fuga de información sensible que se produce de forma continuada en este tipo de comunicaciones y reduciendo así el impacto económico y reputacional derivado del uso malintencionado de los metadatos.

Principales Funcionalidades:
• Funciona de forma automática sin requerir intervención por parte del usuario.
• Los metadatos e información oculta serán procesados independientemente del cliente de correo utilizado (cliente de escritorio, cliente web, tablet o smartphone).
• Permite configurar los tipos de ficheros a procesar (Microsoft Office, Open/Libre Office, PDF y más de 150 extensiones de ficheros de imagen, audio y vídeo).
• Permite eliminar todos los metadatos o aplicar plantillas de metadatos.
• Procesa los metadatos de los ficheros PDF firmados electrónicamente manteniendo la validez de la firma electrónica.
• Permite configurar dominios de exclusión (WhiteList) para el procesado de metadatos: Se puede configurar que para los emails internos a la Organización no se modifiquen los metadatos de los ficheros adjuntos enviados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

8.8 ESPACIO

8.8.1 PRODUCTOS CRIPTOGRÁFICOS PARA ACCESO A SERVICIOS GNSS

Módulo de Seguridad Galileo PRS PRESENCE2	
Versión	2.0.0
Fabricante	Cipherbit (Grupo Oesía)
Familia	Productos criptográficos para acceso a servicios GNSS
Tipo	Producto
Clasificación	RESERVADO
Fecha Inclusión	30/09/2025
Revisión de Validez	30/09/2029



Descripción

El Módulo de Seguridad PRS PRESENCE2 implementa los algoritmos criptográficos y gestiona los activos que permiten el acceso al Servico Público Regulado (PRS) del Sistema Galileo. El módulo de seguridad, junto a un módulo de navegación abierta, proporciona la solución PNT robusta (posición, navegación y tiempo) del servicio Galileo PRS.

Observaciones

El equipo no podrá considerarse UNCLASSIFIED CCI hasta que se complete la evaluación de segunda parte para aprobación UE. Utilización según el procedimiento de empleo seguro PE-2025-10.

8.9 SOPORTE CRIPTOGRÁFICO

8.9.1 INFRAESTRUCTURA PKI

Entrust Certificate Authority y Entrust Certificate Authority Administration	
Versión	10.2
Fabricante	Entrust Solutions
Familia	Infraestructura PKI
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/10/2025
Revisión de Validez	31/12/2028

Descripción

Entrust Certificate Authority es una solución integral y de nueva generación de infraestructura de clave pública (PKI), diseñada para proteger identidades digitales de usuarios, dispositivos y aplicaciones mediante servicios escalables, de alta disponibilidad, ya sea en instalaciones locales o gestionados. Ofrece una gestión sólida y automatizada del ciclo de vida de los certificados, incluyendo su emisión, renovación y revocación.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

8.9.2 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	31/12/2026
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	CONFIDENCIAL
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2027
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	31/12/2026

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

8.10 PROTECCIÓN DE PLATAFORMAS

8.10.1 DISPOSITIVOS MÓVILES

Färist Mobile en Nokia XR21 (FM T140)



Versión	7.7
Fabricante	Tutus
Familia	Dispositivos móviles
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	21/01/2025
Revisión de Validez	28/02/2027

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 “Färist Mobile operational doctrine ”. Comercializado en España por la empresa Epicom.

8.10.2 SISTEMAS OPERATIVOS

SUSE Linux Enterprise Server	
Versión	Version 15 SP4
Fabricante	SUSE Software Solutions
Familia	Sistemas Operativos
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	14/12/2028

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
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

8.10.3 HIPERCONVERGENCIA

HPE SimpliVity



Hewlett Packard Enterprise

Versión	4.2.0.97
Fabricante	HPE
Familia	Hiperconvergencia
Tipo	Producto
Clasificación	TODOS LOS NIVELES (OTAN y Nacional)
Fecha Inclusión	01/02/2026
Revisión de Validez	28/02/2027

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

CCN-STIC 1644 Procedimiento de Empleo Seguro HPE Simplivity

KATUA SDI PLATFORM

Versión	2.0.1
Fabricante	KRC ESPAÑOLA
Familia	Hiperconvergencia
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	14/10/2025
Revisión de Validez	31/03/2028

Descripción

Katua®SDI Platform es una plataforma hiperconvergente que unifica computación, almacenamiento, red y software en un único sistema para minimizar la complejidad del centro de datos y aumentar su escalabilidad. Está basada en el concepto Software Define Infraestructure, donde todos los elementos que conforman un CPD se definen en una única plataforma hardware + software. Permite el despliegue rápido de servicios (xaaS) y consolidación de CPDs. Puede ser instalado en distintos tipos de servidores y desplegado tanto en entornos móviles como en grandes centros de procesos de datos. Su flexibilidad permite que se puedan desplegar servicios sobre la plataforma de forma segura, sencilla y eficiente. Dispone de la capacidad para generar bibliotecas de imágenes de sistemas ya preconfigurados para su despliegue de manera sencilla 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 permitiendo, de esta forma, su instalación en nodos pequeños (desde un único equipo). 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-katua.com

Observaciones

CCN-STIC-1610 Procedimiento de Empleo Seguro KATUA SDI Platform

8.11 COMUNICACIONES TÁCTICAS SEGURAS

8.11.1 SOLUCIONES PARA PROTECCIÓN DE LAS COMUNICACIONES TÁCTICAS

COMSec Admin +

Versión	v5.1
Fabricante	Indra
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/03/2026
Revisión de Validez	31/10/2026

Descripción

COMSec Admin + es una solución global de comunicaciones seguras que proporciona servicios cifrados resistentes a computación cuántica con mecanismos de hibridación de criptografía clásica y PQC en el ámbito de voz, mensajería instantánea y videollamada sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con 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 Admin + son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: www.indragroup.com

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Secret.T (iOS)

Versión	1.18
Fabricante	Telefónica Soluciones de Criptografía
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/02/2026
Revisión de Validez	31/08/2027

Descripción

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

Secret.T (Android)

Versión	1.15
Fabricante	Telefónica Soluciones de Criptografía
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	24/03/2025
Revisión de Validez	30/08/2027

Descripción

El sistema Secret.T® es una solución integral de comunicaciones de última generación. Su diseño proporciona diversos métodos de intercambio de información, facilitando una actividad colaborativa versátil tanto entre individuos como entre grupos, manteniendo un alto nivel de seguridad y privacidad.
Esta solución consta de dos elementos principales: una aplicación que ofrece acceso intuitivo a las distintas funciones y unos servidores optimizados para garantizar la seguridad, privacidad y escalabilidad.
El uso de cifrado de extremo a extremo en todos los modos de comunicación asegura la protección y confidencialidad total entre los usuarios. Entre sus características destacadas se incluyen: llamadas individuales y grupales de audio y vídeo, mensajería de texto, intercambio de archivos de diversos formatos tanto a nivel individual como grupal, comunicaciones tácticas, posicionamiento de usuarios, retransmisión de vídeo en directo, entre otras.

Observaciones

Procedimiento de empleo pendiente de publicación

Enrutador y Cifrador Táctico GESCOM VCS G5 y G5A

Versión	FW 3.1 y FW criptográfico 2.1
Fabricante	RF ESPAÑOLA
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/06/2026
Revisión de Validez	31/12/2030



Descripción

El GESCOM G5 es el sistema de comunicaciones vehiculares de RF Española, diseñado para ofrecer comunicaciones tácticas de voz y datos cifradas en una amplia variedad de plataformas y configuraciones militares. El sistema incorpora enrutamiento de datos de alta velocidad, redes MESH dinámicas y gestión avanzada del tráfico, con capacidad para integrar hasta cinco radios CNR, incluyendo conectividad SATCOM y 5G. Su chasis rugerizado de aluminio cumple con los estándares MIL-STD-810, garantizando su fiabilidad en las condiciones operativas más adversas.

El G5 dispone de cifrado de voz y datos homologado por la OTAN mediante los protocolos TSVCIS y SCIP 214.6 (STaC-IS), con carga segura de claves a través de interfaces DS-101 para SKL, ERMES y otros cargadores OTAN. Además, integra servidor de telefonía SIP, intercomunicación embarcada avanzada, telecontrol remoto de radios y compatibilidad con sistemas C2 como BMS, TALOS y ATAK. El sistema puede configurarse en su totalidad mediante Tablet, PC o interfaz web, lo que facilita su integración y mantenimiento en el entorno operativo.

La variante GESCOM G5A incorpora un terminal de voz completo, proporcionando una solución integrada que permite utilizar todas las funciones de voz desde un único dispositivo.

Observaciones

Utilización según el Procedimiento de empleo PE-2025-8.

8.11.2 PLATAFORMAS Y DISPOSITIVOS TÁCTICOS CONFIABLES

Galleon Embedded Computing Encryption Module (EM)

Versión	4.0.11
Fabricante	Galleon Embedded Computing
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/03/2026
Revisión de Validez	29/02/2028



Descripción

El almacenamiento conectado a red (NAS) robusto de Galleon ofrece un rendimiento superior en un formato ultracompacto. El almacenamiento extraíble garantiza tiempos mínimos en tierra para aplicaciones aerotransportadas.

El NAS es capaz de manejar un alto número de conexiones simultáneas sin comprometer el rendimiento del sistema. Están disponibles conexiones ópticas de 10Gb y Ethernet Gigabit tradicionales, tanto ópticas como de cobre, para adaptarse a la infraestructura existente.

Las capas de cifrado de hardware y software certificadas Common Criteria proporcionan un alto nivel de seguridad de los datos con opciones flexibles de gestión de claves, incluyendo puertos locales y carga remota a través de conexiones de red seguras.

Observaciones

N/A

GETAC F110

Versión	G7 con firmware GETAC 16.1.32.2418
Fabricante	GETAC
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA, NATO RESTRCITED
Fecha Inclusión	01/06/2021
Revisión de Validez	31/07/2028



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”.

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	30/04/2028

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	13/10/2026

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	13/10/2026

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”.

8.12 TEMPEST

8.12.1 ARMARIOS APANTALLADOS

P.AT-06F	
Versión	
Fabricante	CONSUEGRA S. COOP.
Familia	Armarios apantallados
Tipo	Producto
Clasificación	Apto ZONA 0
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2026



Descripción

El armario P.AT-06F es un armario de hasta 38 U's útiles, diseñado y fabricado para uso en entornos que necesiten alta inmunidad frente a emanaciones radioeléctricas de equipos informáticos y como principal barrera de protección contra intervenciones TEMPEST.
El armario dispone de cerraduras para garantizar que no se hace uso indebido de los equipos encerrados en el armario. Así mismo, la configuración del armario ha sido concebida para dificultar su desmontaje desde el exterior para evitar un acceso fraudulento a su interior.
Dispone de dos puertas ciegas, una en su parte delantera y otra en la trasera, de unos 1.500 mm. de altura, que facilita el cableado y mantenimiento de los equipos alojados dentro del armario.
La alimentación de los equipos internos se realiza mediante filtros adecuados a la capacidad del armario. Para las conexiones exteriores se utilizan dos paneles con conectores a medida. Se dispone de un panel de 12 guía-ondas para fibra óptica . Este panel se podrá personalizar a las necesidades de cada instalación.
La ventilación se asegura mediante la utilización de rejillas protegidas mediante "paneles de abeja" y se fuerza la circulación mediante dos ventiladores con un caudal de 1.865 m3/h .

Observaciones

BSR1930-TA



Versión

Fabricante GESAB

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0

Fecha Inclusión 01/03/2025

Revisión de Validez 31/12/2026

Descripción

Armario apantallado de 19” y 30 U con atenuación certificada ≥ 80 dB entre 100 MHz y 10 GHz, otorgada por laboratorio acreditado. Su estructura monobloque soldada — una auténtica jaula de Faraday en acero— incorpora puerta frontal con cerradura Moturra de cuatro pernos que garantizan un cierre EMI estanco y chapa trasera removible. Las dimensiones exteriores, con ruedas instaladas, son 1750 mm (Al) × 1100 mm (Prof) × 800 mm (An); el chasis interno admite 1200 kg de carga estática y el armario pesa 240 kg en vacío

Observaciones

N/A

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 31/12/2026

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 31/12/2026

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-07



Versión _

Fabricante CONSUEGRA S. COOP.

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0

Fecha Inclusión 01/12/2017

Revisión de Validez 31/12/2026

Descripción

El ARMARIO TEMPEST P.AT-07 está fabricado en acero que proporciona las características de apantallamiento necesarias para cumplir con las especificaciones de Apto para locales ZONA 0.
Lleva una puerta apantallada frontal que da acceso a la CPU, mientras que un interruptor externo permite desconectar la CPU y ventiladores.
La CPU va montada en una bandeja extraíble mediante guías telescópicas que permite acceder para la reparación, modificación o substitución de la CPU.
Todas las salidas de alimentación eléctrica y de datos están debidamente filtradas para garantizar la protección TEMPEST y se encuentran en un panel de conexiones sustituible que permite futuras expansiones.
El armario internamente va electrificado disponiendo de 660 vatios de 220V. A.C. de energía filtrada para poder conectar una CPU comercial. El armario lleva su cable para conexión a la red eléctrica de 220V. A.C.
Incorpora ventilación forzada, tomando aire de la parte inferior a través de paneles de ventilación guía ondas y expulsándolo por la parte superior trasera mediante dos ventiladores también a través de este tipo de paneles.

Observaciones

P.AT07E



Versión _

Fabricante CONSUEGRA S. COOP.

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0

Fecha Inclusión 01/04/2019

Revisión de Validez 31/12/2026

Descripción

Armario Tempest de sobremesa de dimensiones reducidas con dos posibles funciones. El armario P.AT0-07E ofrece protección electromagnética para que el cliente incluya su propia CPU, convirtiendo el conjunto en una CPU Tempest adecuada para locales ZONA 0. En este caso, 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. Dimensiones de equipo Ancho: 270 mm, fondo: 310 mm, alto: 97 mm

Observaciones

SHATEM - SHELTER ARPA TEMPEST MULTIPROPOSITO



Versión

Fabricante ARPA, EQUIPOS MÓVILES DE CAMPAÑA

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0

Fecha Inclusión 30/09/2019

Revisión de Validez 30/12/2026

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

8.12.2 MONITORES

P.MONT0-12



Versión

Fabricante CONSUEGRA S. COOP.

Familia Monitores

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 01/02/2022

Revisión de Validez 31/12/2026

Descripción

Monitor de 22" con formato panorámico. Dispone de conexión VGA estándar. Los monitores P.MONT0-12 están basados en modelo comercial convenientemente adaptado para cumplir con las especificaciones TEMPEST SDIP-27/2 LEVEL A

Observaciones

8.12.3 PERIFÉRICOS

P.RATT0-04



Versión _
Fabricante CONSUEGRA S. COOP.
Familia Periféricos
Tipo Producto
Clasificación SDIP-27 Level A
Fecha Inclusión 31/10/2018
Revisión de Validez 30/12/2026
Descripción

A. RATON P.RATT0-04 SDIP 27/2 LEVEL A. Basado en el ratón HP BASIC
Observaciones

P.TECT0-12



Versión
Fabricante CONSUEGRA S. COOP.
Familia Periféricos
Tipo Producto
Clasificación SDIP-27 Level A
Fecha Inclusión 29/02/2024
Revisión de Validez 30/12/2026
Descripción

Los teclados P.TECT0-12 están basados en el modelo comercial HP de teclados estándar de tecnología USB con que se suelen equipar muchos de los equipos PC HP de sobremesa que utilizan preferente sistemas Microsoft Windows y que han sido convenientemente adaptado para cumplir con las especificaciones TEMPEST SDIP-27 categoría A
Observaciones
N/A

P.TECT0-10



Versión

Fabricante CONSUEGRA S. COOP.

Familia Periféricos

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 31/10/2022

Revisión de Validez 30/12/2026

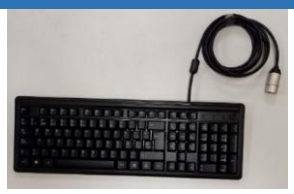
Descripción

Los teclados P.TECT0-10 están basados en el modelo comercial HP de teclados estándar de tecnología USB con que se suelen equipar muchos de los equipos PC HP de sobremesa que utilizan preferente sistemas Microsoft Windows y que han sido convenientemente adaptado para cumplir con las especificaciones TEMPEST SDIP-27 categoría A

Observaciones

N/A

P.TECT0-11



Versión

Fabricante CONSUEGRA S. COOP.

Familia Periféricos

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 30/11/2021

Revisión de Validez 30/12/2026

Descripción

Los teclados P.TECT0-11 están basados en el modelo comercial HP de teclados estándar de tecnología USB con que se suelen equipar muchos de los equipos PC HP de sobremesa que utilizan preferente sistemas Microsoft Windows y que han sido convenientemente adaptado para cumplir con las especificaciones TEMPEST SDIP-27 categoría A

Observaciones

N/A

P.TECT0-15



Versión

Fabricante CONSUEGRA S. COOP.

Familia Periféricos

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 31/12/2024

Revisión de Validez 30/12/2026

Descripción

Los teclados P.TECT0-15 están basados en el modelo comercial HP de teclados estándar de tecnología USB con que se suelen equipar muchos de los equipos PC HP de sobremesa que utilizan preferente sistemas Microsoft Windows y que han sido convenientemente adaptado para cumplir con las especificaciones TEMPEST SDIP-27 categoría A

Observaciones

N/A

P.TECT0-16



Versión

Fabricante CONSUEGRA S. COOP.

Familia Periféricos

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 30/04/2025

Revisión de Validez 30/12/2026

Descripción

El teclado P.TECT0-16 está basado en el modelo comercial HP de teclados estándar con tecnología USB que suelen equipar desde hace tiempo los equipos PC HP de sobremesa, adaptado tanto a personas diestras como zurdas y que han sido convenientemente modificado para cumplir con las especificaciones TEMPEST SDIP-27 categoría A.

Observaciones

N/A

P.RATT0-05



Versión

Fabricante CONSUEGRA S. COOP.

Familia Periféricos

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 31/05/2021

Revisión de Validez 30/12/2026

Descripción

El ratón P.RATT0-05 está basado en el modelo comercial HP de ratones estándar con tecnología USB que suelen equipar desde hace tiempo los equipos PC HP de sobremesa, adaptado tanto a personas diestras como zurdas y que han sido convenientemente modificado para cumplir con las especificaciones TEMPEST SDIP-27 categoría A

Observaciones

N/A

P.RATT0-09



Versión

Fabricante CONSUEGRA S. COOP.

Familia Periféricos

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 31/12/2024

Revisión de Validez 30/12/2026

Descripción

El ratón P.RATT0-09 está basado en el modelo comercial HP de ratones estándar con tecnología USB que suelen equipar desde hace tiempo los equipos PC HP de sobremesa, adaptado tanto a personas diestras como zurdas y que han sido convenientemente modificado para cumplir con las especificaciones TEMPEST SDIP-27 categoría A

Observaciones

N/A

P.RATT0-10



Versión

Fabricante CONSUEGRA S. COOP.

Familia Periféricos

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 30/04/2025

Revisión de Validez 30/12/2026

Descripción

El ratón P.RATT0-10 está basado en el modelo comercial HP de ratones estándar con tecnología USB que suelen equipar desde hace tiempo los equipos PC HP de sobremesa, adaptado tanto a personas diestras como zurdas y que han sido convenientemente modificado para cumplir con las especificaciones TEMPEST SDIP-27 categoría A

Observaciones

N/A

8.12.4 CPU

P.COMPT0-08

Versión _

Fabricante CONSUEGRA S. COOP.

Familia CPU

Tipo Producto



Clasificación SDIP-27 Level A

Fecha Inclusión 01/03/2024

Revisión de Validez 31/12/2026

Descripción

La CPU P.COMT0-08 incluye en su interior el modelo de HP PC HP 400 G9 Pro Desktop Mini PC con procesador i5.

Observaciones

P.COMPT0-10

Versión

Fabricante CONSUEGRA S. COOP.

Familia CPU

Tipo Producto



Clasificación SDIP-27 Level A

Fecha Inclusión 31/12/2024

Revisión de Validez 30/12/2026

Descripción

La CPU P.COMT0-10 incluye en su interior el modelo de HP PC HP 400 G9 Pro Desktop Mini PC con procesador i7

Observaciones

N/A

P.COMPT0-09



Versión

Fabricante CONSUEGRA S. COOP.

Familia CPU

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 01/03/2024

Revisión de Validez 31/12/2026

Descripción

La CPU P.COMT0-09 incluye en su interior el modelo de HP Mini Pro 400 G9 con procesador i7 con panel de conexiones trasero, todo ello convenientemente protegido tanto de las emisiones emitidas como conducidas mediante materiales y filtros especiales para adaptarse a las especificaciones TEMPEST SDIP-27/2 Level A

Observaciones

N/A

8.12.5 IMPRESORAS

P.IMPT0-05-HP



Versión	_
Fabricante	CONSUEGRA S. COOP.
Familia	Impresoras
Tipo	Producto
Clasificación	SDIP-27 Level A
Fecha Inclusión	31/12/2021
Revisión de Validez	30/12/2026

Descripción

Esta impresora está basada en la máquina comercial HP® Color LaserJet Enterprise M554dn sobre la que se han realizado las intervenciones necesarias para adaptarse a las especificaciones TEMPEST SDIP-27 categoría A.

Observaciones

8.12.6 SERVIDOR

SOC-1-TP	
Versión	-
Fabricante	KRC ESPAÑOLA
Familia	Servidor
Tipo	Producto
Clasificación	SDIP-27/2 Level B
Fecha Inclusión	15/10/2023
Revisión de Validez	30/12/2026



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

8.12.7 PORTÁTIL

BSLi7L-TA



Versión

Fabricante GESAB

Familia Portátil

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 30/04/2025

Revisión de Validez 30/12/2026

Descripción

Portátil apantallado de 15,6 ” que garantiza una atenuación mínima de 60 dB en el rango crítico especificado por SDIP-27/2 Nivel A, adecuado para operar equipos línea roja en salas ZONA 0.
Incorpora procesador Intel® Core™ i7-1355U (10 núcleos/12 hilos, hasta 5 GHz) con plataforma Intel vPro®, 16 GB DDR4-3200 ampliables a 64 GB y SSD NVMe 512 GB, proporcionando rendimiento de clase profesional dentro del blindaje

Observaciones

N/A

SRUG-004



Versión

Fabricante KRC ESPAÑOLA

Familia Portátil

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 31/05/2025

Revisión de Validez 30/12/2026

Descripción

Solución tempest basada en portátil semirugerizado de alto rendimiento con procesador i7 diseñado para ofrecer alta resistencia en todo tipo de situaciones. Compatible con distintos sistemas operativos. Consúltanos para más información. krc-katua.com

Observaciones

N/A

SRUG-003



Versión	
Fabricante	KRC ESPAÑOLA
Familia	Portátil
Tipo	Producto
Clasificación	SDIP-27 Level A
Fecha Inclusión	31/05/2025
Revisión de Validez	30/12/2026

Descripción

Solución tempest basada en portátil semirugerizado de alto rendimiento con procesador i5 diseñado para ofrecer alta resistencia en todo tipo de situaciones. Compatible con distintos sistemas operativos. Consúltanos para más información. krc-katua.com

Observaciones

N/A

8.13 OTRAS HERRAMIENTAS

8.13.1 OTRAS HERRAMIENTAS

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	31/12/2026



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

MetaClean Dashboard (modalidad On-Premise)

Versión	2.2.3
Fabricante	Adarsus Technologies
Familia	Otras Herramientas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/11/2023
Revisión de Validez	01/11/2028



Descripción

MetaClean Dashboard: Consola de administración de MetaClean para despliegue On-Premise. Administra, centraliza y controla la aplicación de políticas preventivas de seguridad corporativas. Permite obtener estadísticas de los metadatos procesados, gestión de licencias y controlar la exfiltración de información de forma global.

Observaciones

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard

metaOLVIDO Dashboard (modalidad On-Premise)

Versión	2.2.3
Fabricante	Adarsus Technologies
Familia	Otras Herramientas
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2026
Revisión de Validez	01/11/2028

Descripción

metaOLVIDO Dashboard: Consola de administración de metaOLVIDO para las distintas modalidades de despliegue (On-Premise o Cloud). Administra, centraliza y controla la aplicación de políticas preventivas de seguridad corporativas. Permite obtener estadísticas de los metadatos procesados, gestión de licencias y controlar la exfiltración de información de forma global.

Observaciones

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard

9. PRODUCTOS Y SERVICIOS DE CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD



PRODUCTOS Y SERVICIOS STIC

CONFORMIDAD Y GOBERNANZA

9.1 GOBERNANZA Y PLANIFICACIÓN DE LA SEGURIDAD

Proactivanet - Cloud SaaS

Versión

Fabricante Espiral Microsistemas

Familia Gobernanza y Planificación de la Seguridad

Tipo Servicio

Fecha Inclusión 30/04/2026

Revisión de Validez 31/03/2028

Descripción

Proactivanet es una solución integral para la gestión de servicios (ITSM) y activos de TI (ITAM), diseñada para ofrecer una visión unificada y control completo del entorno tecnológico. Con un enfoque sólido en ITSM alineado con ITIL, permite gestionar de forma eficiente incidencias, problemas, cambios y catálogo de servicios. A su vez, incorpora capacidades avanzadas de ITAM e inventario, con descubrimiento automático, gestión del ciclo de vida de activos y CMDB. Su principal valor reside en la integración nativa entre ITSM e ITAM, que permite relacionar servicios y activos en una única plataforma, mejorando la trazabilidad, la automatización y la toma de decisiones basada en datos fiables.

Observaciones

CCN-STIC 1007 Procedimiento de Empleo Seguro Proactivanet SaaS

Arexdata DSPM

Versión 24

Fabricante Arexdata

Familia Gobernanza y Planificación de la Seguridad

Tipo Producto

Fecha Inclusión 07/02/2025

Revisión de Validez 31/07/2027

Descripción

Arexdata DSPM es la Plataforma de Seguridad del Dato del fabricante español Arexdata, que Audita, Normaliza, Clasifica y Protege el dato de las organizaciones, además de proporcionar una Visibilidad y Trazabilidad end-to-end de manera Centralizada. Incluye la Auditoría, Gestión de Permisos y Clasificación de Datos Sensibles, en todos los repositorios de datos de las organizaciones, con independencia de su ubicación.

Observaciones

N/A

Wiz

Versión

Fabricante Wiz

Familia Gobernanza y Planificación de la Seguridad

Tipo Servicio

Fecha Inclusión 01/03/2026

Revisión de Validez 29/02/2028

Descripción

Wiz es una plataforma CNAPP (Cloud-Native Application Protection Platform) que protege todo lo que las organizaciones crean y ejecutan. La plataforma de seguridad de Wiz conecta el código, la nube y el tiempo de ejecución en un único contexto compartido, lo que permite a los equipos de seguridad e ingeniería comprender el riesgo real, solucionar problemas desde el origen y detener las amenazas a medida que surgen.
Diseñado para la era de la nube y la IA, Wiz permite un desarrollo seguro por defecto, una protección automatizada y una reducción continua del riesgo a lo largo de todo el ciclo de vida de las aplicaciones.
Wiz protege entornos en la nube, híbridos y on-premise, incluidos Amazon Web Services, Microsoft Azure, Google Cloud, Oracle Cloud, Openshift, VMware e IBM Cloud, entre otros.

Observaciones

N/A

Proactivanet - OnPremise	
Versión	10.25
Fabricante	Espiral Microsistemas
Familia	Gobernanza y Planificación de la Seguridad
Tipo	Producto
Fecha Inclusión	19/03/2026
Revisión de Validez	31/08/2028

Descripción

Proactivanet es una solución integral para la gestión de servicios (ITSM) y activos de TI (ITAM), diseñada para ofrecer una visión unificada y control completo del entorno tecnológico. Con un enfoque sólido en ITSM alineado con ITIL, permite gestionar de forma eficiente incidencias, problemas, cambios y catálogo de servicios. A su vez, incorpora capacidades avanzadas de ITAM e inventario, con descubrimiento automático, gestión del ciclo de vida de activos y CMDB. Su principal valor reside en la integración nativa entre ITSM e ITAM, que permite relacionar servicios y activos en una única plataforma, mejorando la trazabilidad, la automatización y la toma de decisiones basada en datos fiables.

Proactivanet está desarrollada por una empresa española fabricante de software con 28 años de experiencia en el mercado, especializada en soluciones para la gestión de TI. La compañía cuenta con presencia internacional y oficinas en varios países de Latinoamérica, lo que le permite ofrecer un servicio cercano y adaptado a distintos contextos. Dispone de una sólida trayectoria en la Administración Pública y una destacada implantación en el sector Defensa, donde su tecnología ha demostrado robustez, escalabilidad y adecuación a entornos con altos requisitos de seguridad y operatividad.

Observaciones

CCN-STIC 1008 Procedimiento de Empleo Seguro Proactivanet OnPremise

9.2 NORMATIVA DE SEGURIDAD Y CONFORMIDAD

Wiz

Versión

Fabricante Wiz

Familia Normativa de Seguridad y Conformidad

Tipo Servicio

Fecha Inclusión 01/03/2026

Revisión de Validez 29/02/2028

Descripción

Wiz es una plataforma CNAPP (Cloud-Native Application Protection Platform) que protege todo lo que las organizaciones crean y ejecutan. La plataforma de seguridad de Wiz conecta el código, la nube y el tiempo de ejecución en un único contexto compartido, lo que permite a los equipos de seguridad e ingeniería comprender el riesgo real, solucionar problemas desde el origen y detener las amenazas a medida que surgen.
Diseñado para la era de la nube y la IA, Wiz permite un desarrollo seguro por defecto, una protección automatizada y una reducción continua del riesgo a lo largo de todo el ciclo de vida de las aplicaciones.
Wiz protege entornos en la nube, híbridos y on-premise, incluidos Amazon Web Services, Microsoft Azure, Google Cloud, Oracle Cloud, Openshift, VMware e IBM Cloud, entre otros.

Observaciones

N/A

Prowler

Versión 5.13.0

Fabricante Prowler

Familia Normativa de Seguridad y Conformidad

Tipo Servicio

Fecha Inclusión 01/11/2025

Revisión de Validez 31/10/2027

Descripción

(ES) Prowler es la plataforma de seguridad en la nube de código abierto más utilizada en el mundo, que automatiza la seguridad y el cumplimiento en cualquier entorno de nube. Con cientos de verificaciones de seguridad listas para usar, guías de remediación y marcos de cumplimiento, Prowler ofrece monitoreo e integraciones personalizables, fáciles de usar y potenciadas por IA, haciendo que la seguridad en la nube sea simple, escalable y rentable para organizaciones de cualquier tamaño.
(EN) Prowler is the world's most widely used open-source cloud security platform that automates security and compliance across any cloud environment. With hundreds of ready-to-use security checks, remediation guidance, and compliance frameworks, Prowler delivers AI-driven, customizable, and easy-to-use monitoring and integrations, making cloud security simple, scalable, and cost-effective for organizations of any size.

Observaciones

CCN-STIC 1011 Procedimiento de Empleo Seguro Prowler

9.3 ANÁLISIS Y GESTIÓN DE RIESGOS

GlobalSuite Solutions GRC SaaS	
Versión	7.6.0
Fabricante	GlobalSuite Solutions
Familia	Análisis y Gestión de Riesgos
Tipo	Servicio
Fecha Inclusión	01/09/2026
Revisión de Validez	31/08/2028

Descripción

GlobalSuite es una plataforma GRC (Gobierno, Riesgo y Cumplimiento) para el gobierno de la seguridad, la gestión del riesgo y la evaluación del cumplimiento normativo desde un único punto multinorma, en organizaciones públicas y privadas. Da soporte a la adecuación y mantenimiento del Esquema Nacional de Seguridad (ENS) e integra marcos como ISO/IEC 27001, 27017/27018, ISO 22301 (Continuidad de Negocio), ISO/IEC 20000-1, RGPD, NIS2, DORA, SOC 2, ISO/IEC 42001 y AI Act, y normativa propia del cliente, sobre un modelo de datos común con trazabilidad entre activos, riesgos, controles, tareas y evidencias. Incorpora inteligencia artificial que asiste la gestión normativa y de riesgos, y un módulo de automatizaciones del ciclo de cumplimiento. El módulo de riesgos admite cualquier metodología e incluye análisis cuantitativo por simulación de Montecarlo, con planes de tratamiento priorizados y trazables sobre activos esenciales y de soporte. Incluye gestión documental, auditorías internas y externas, declaración de aplicabilidad y cuadros de mando con visibilidad en tiempo real del riesgo y el cumplimiento para responsables y dirección. Se ofrece como servicio multitenant, en modo SaaS y On-Premise.

Observaciones

N/A

Gconsulting Compliance

Versión	2.4
Fabricante	NUNSYS
Familia	Análisis y Gestión de Riesgos
Tipo	Producto
Fecha Inclusión	30/06/2026
Revisión de Validez	30/06/2028

Descripción

GConsulting Compliance es un software GRC multicliente (multitenant y multinorma) que actúa como vCISO automatizado para organizaciones y como plataforma de apoyo para oficinas de seguridad de consultoras. Integra cumplimiento normativo, plan director de seguridad y análisis de riesgos dinámico (recogiendo datos de SIEM/NIDS, IT y OT, y transformándolos con IA en un plan director accionable). Ofrece a organizaciones públicas y privadas visión centralizada y en tiempo real de riesgos, cumplimiento y operación de seguridad.
El módulo de Riesgos evalúa, documenta y mitiga riesgos en protección de datos y ciberseguridad, se integra con PILAR (INÉS, AMPARO) y ofrece cuestionarios guiados que generan un perfil de riesgo personalizado.
Cubre múltiples normativas (ENS, RGPD, ISO 27001, ISA 62443, NIS2, DORA, entre otras), identifica brechas y genera planes de acción priorizados y trazables, con automatización e IA que impulsan proactivamente las tareas y mantienen actualizados a consultor y cliente.
Incluye módulo de auditoría, gestor documental, y una API que enriquece cualquier SOC, con trazabilidad bidireccional entre activos y negocio, alertas/vulnerabilidades y riesgos, y acciones y controles, en entornos IT y OT.

Observaciones

N/A

PILAR

Versión	version web
Fabricante	CCN
Familia	Análisis y Gestión de Riesgos
Tipo	Servicio
Fecha Inclusión	10/02/2025
Revisión de Validez	31/01/2027

Descripción

PILAR versión web es una herramienta que implementa la metodología MAGERIT de análisis y gestión de riesgos en sistemas de información.
Su interfaz web facilita la colaboración entre usuarios y la rápida implementación de análisis de riesgo.
Llevando a cabo los siguientes pasos:
1. Identifica y valora información y servicios gestionados por el sistema
2. Identifica activos de soporte (equipamiento, comunicaciones, personas, instalaciones y servicios de terceros)
3. Establece las dependencias entre servicios y activos de soporte
4. Aplica un sistema experto de amenazas y vulnerabilidades ciber
5. Calcula el riesgo potencial inherente al sistema de información
6. Evalúa medidas de seguridad
7. Calcula el riesgo residual a lo largo del desarrollo del plan de tratamiento del riesgo

Observaciones

N/A

Continuous Exposure Management

Versión	Console/API v3.59.0.3724, Sensor v1.50.0
Fabricante	XM Cyber
Familia	Análisis y Gestión de Riesgos
Tipo	Servicio
Fecha Inclusión	01/05/2026
Revisión de Validez	30/04/2028

Descripción

XM Cyber es una solución de Gestión Continua de la Exposición de Amenazas (CTEM), diseñada para identificar, visualizar y priorizar de forma ininterrumpida los riesgos de seguridad en infraestructuras On-Premise, Cloud, híbridas y OT. La plataforma implementa el ciclo completo de exposición: alcance, descubrimiento, validación, priorización y movilización hacia la remediación. Mediante un motor de grafos y tecnología de "Gemelo Digital", XM Cyber visualiza de forma proactiva cómo las vulnerabilidades, las configuraciones erróneas y las debilidades de identidad se encadenan para permitir el movimiento lateral y la escalada de privilegios hacia activos críticos. Adicionalmente, permite la identificación de "Choke Points" o puntos de estrangulamiento: nodos críticos en los que la aplicación de una única medida correctiva interrumpe simultáneamente múltiples rutas de compromiso, optimizando la capacidad operativa de los equipos de seguridad.

La solución facilita el cumplimiento del ENS, NIS2, ISO27001, etc; al transformar datos técnicos complejos en métricas de riesgo de negocio y planes de remediación priorizados, alineándose con los objetivos de resiliencia. El cliente final debe seleccionar la región AWS EU para su tenant.

Observaciones

Sandas GRC

Versión 6.20

Fabricante Govertis Advisory Servicios

Familia Análisis y Gestión de Riesgos

Tipo Servicio

Fecha Inclusión 07/02/2025

Revisión de Validez 31/01/2027

Descripción

Sandas GRC es una plataforma que permite dar respuesta a las necesidades de Gobierno de la Seguridad, Gestión del Riesgo y Evaluación del Cumplimiento Normativo (GRC), a través de la trazabilidad (proceso de seguridad) de las normas ENS, ISO/IEC 27001 (Seguridad de la Información), junto con otros marcos normativos y buenas prácticas internacionales (Continuidad de Negocio, PCI-DSS) o normativa propia del cliente. Permite dar visibilidad a responsables y niveles de dirección del riesgo tecnológico y del grado de cumplimiento de las normas.Integración de multinorma (ENS, Privacidad, ISO, Continuidad de Negocio, PCI-DSS, DORA, Seguridad IoT, GSMA,..) con la capa operativa (monitorización, gestión de vulnerabilidades, ..) y proporciona inteligencia directa y accionable sobre seguridad tanto en IT como en OT.Diseña cuadros de mando dinámicos a partir de indicadores pudiendo obtener su información de datos disponibles en la propia plataforma, y de sistemas externos.Permite su uso en las distintas fases de la adecuación y el mantenimiento de las normas como sistema centralizador de los modelos (Arquitectura. Empresarial, Gestión del Riesgo, Marco de Controles y Gestión de Tareas) y la documentación generada, garantizando su coherencia.

Observaciones

CCN-STIC 1705. Procedimiento de Empleo Seguro Sandas GRC

Wiz

Versión

Fabricante Wiz

Familia Análisis y Gestión de Riesgos

Tipo Servicio

Fecha Inclusión 01/03/2026

Revisión de Validez 29/02/2028

Descripción

Wiz es una plataforma CNAPP (Cloud-Native Application Protection Platform) que protege todo lo que las organizaciones crean y ejecutan. La plataforma de seguridad de Wiz conecta el código, la nube y el tiempo de ejecución en un único contexto compartido, lo que permite a los equipos de seguridad e ingeniería comprender el riesgo real, solucionar problemas desde el origen y detener las amenazas a medida que surgen.
Diseñado para la era de la nube y la IA, Wiz permite un desarrollo seguro por defecto, una protección automatizada y una reducción continua del riesgo a lo largo de todo el ciclo de vida de las aplicaciones.
Wiz protege entornos en la nube, híbridos y on-premise, incluidos Amazon Web Services, Microsoft Azure, Google Cloud, Oracle Cloud, Openshift, VMware e IBM Cloud, entre otros.

Observaciones

N/A

Forescout REM (Risk and Exposure Management)

Versión	24.2
Fabricante	Forescout Technologies
Familia	Análisis y Gestión de Riesgos
Tipo	Servicio
Fecha Inclusión	20/08/2025
Revisión de Validez	30/07/2027

Descripción

La solución REM (Risk and Exposure Management) de Forescout, es un componente de plataforma de Forescout que proporciona una visión de la postura de ciberseguridad, y de su evolución, de todos los todos los dispositivos IT, OT, IoT y IoMT de la organización, cuantificando su riesgo, en base a su exposición, a sus comunicaciones, a los servicios que están ofreciendo y a sus vulnerabilidades, permitiendo mitigar los riesgos en tiempo real. En entornos médicos, además de cuantificar el riesgo de los dispositivos, también indica cuáles tratan información personal, cuáles tienen "Recalls" por parte del fabricante, muestra en un cronograma el tiempo de uso y el tipo de pruebas médicas que realizan, proporcionando además su información MDS2.

Observaciones

Tenable One

Versión

Fabricante Tenable

Familia Análisis y Gestión de Riesgos

Tipo Servicio

Fecha Inclusión 01/09/2026

Revisión de Validez 31/08/2028

Descripción

Tenable.one es la plataforma de gestión de riesgo y exposición que unifica datos de toda la superficie de ataque (IT, nube, identidades, aplicaciones, OT/IoT e IA) para priorizar y remediar los riesgos con mayor impacto en el negocio. Módulos incluidos:

Vulnerability Management: prioriza vulnerabilidades en infraestructura IT tradicional. Capacidad nativa análisis de bastionado y cumplimiento normativo.
Web App Scanning: detecta fallos de seguridad en aplicaciones web.
Cloud Security (CNAPP/CIEM): protege cargas de trabajo, contenedores e identidades en la nube.
Identity Exposure: descubre riesgos en Active Directory y Entra ID.
OT/IoT Security: asegura entornos operativos e industriales convergentes con IT.
Attack Surface Management: mapea activos expuestos a internet.
AI Exposure: visibiliza y protege el uso de IA en la organización.
Application Security: contextualiza riesgos de código en la exposición global.
Conectores: integra datos de más de 300 herramientas externas en una vista única.

Su licenciamiento también permite integrar entornos on-premises gestionados con Tenable Security Center, incorporando esos datos al mismo modelo unificado de riesgo.

Capacidad de integración vía API con herramientas CCN Cert.

Correlaciona todo mediante puntuación de exposición y mapas de rutas de ataque.

Observaciones

N/A

GlobalSuite Solutions GRC - On-premises

Versión	7.6.0
Fabricante	GlobalSuite Solutions
Familia	Análisis y Gestión de Riesgos
Tipo	Producto
Fecha Inclusión	01/09/2026
Revisión de Validez	28/02/2029

Descripción

GlobalSuite es una plataforma GRC (Gobierno, Riesgo y Cumplimiento) para el gobierno de la seguridad, la gestión del riesgo y la evaluación del cumplimiento normativo desde un único punto multinorma, en organizaciones públicas y privadas. Da soporte a la adecuación y mantenimiento del Esquema Nacional de Seguridad (ENS) e integra marcos como ISO/IEC 27001, 27017/27018, ISO 22301 (Continuidad de Negocio), ISO/IEC 20000-1, RGPD, NIS2, DORA, SOC 2, ISO/IEC 42001 y AI Act, y normativa propia del cliente, sobre un modelo de datos común con trazabilidad entre activos, riesgos, controles, tareas y evidencias. Incorpora inteligencia artificial que asiste la gestión normativa y de riesgos, y un módulo de automatizaciones del ciclo de cumplimiento. El módulo de riesgos admite cualquier metodología e incluye análisis cuantitativo por simulación de Montecarlo, con planes de tratamiento priorizados y trazables sobre activos esenciales y de soporte. Incluye gestión documental, auditorías internas y externas, declaración de aplicabilidad y cuadros de mando con visibilidad en tiempo real del riesgo y el cumplimiento para responsables y dirección. Se ofrece como servicio multitenant, en modo SaaS y On-Premise.

Observaciones

N/A

9.4 NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES

Hexagon Connnect	
Versión	2024.09.08
Fabricante	Intergraph Corporation
Familia	Notificación y Gestión de Ciberincidentes
Tipo	Servicio
Fecha Inclusión	14/10/2025
Revisión de Validez	30/09/2027

Descripción

HxGN Connect permite a las organizaciones compartir y actuar fácilmente sobre los datos en un entorno seguro para impulsar los centros de operaciones, incidentes y delitos en tiempo real.
HxGN Connect reúne los datos y las personas en una vista unificada para compartir información, colaborar y actuar.
Se trata de un centro de incidentes en tiempo real nativo de la nube como servicio que le permite compartir información de forma segura y coordinar acciones basadas en diferentes tipos de datos, incluidos activos, eventos e incidentes, unidades, cámaras, alarmas y mucho más.
HxGN Connect complementa los sistemas existentes de las organizaciones, proporcionando una vista más rica y unificada de la información con mensajería y asignación de tareas integradas para permitir tanto la participación ad hoc no planificada como la colaboración estructurada diaria y continua.
Conecte y actualice fácilmente los datos, envíe mensajes y asigne tareas a los usuarios, y rompa las barreras entre departamentos, organizaciones, ciudades y regiones.

Observaciones

N/A

9.5 INTERCAMBIO DE CIBERINTELIGENCIA

CryptoTrack

Versión

Fabricante TREE TECHNOLOGY

Familia Intercambio de Ciberinteligencia

Tipo Servicio

Fecha Inclusión 11/03/2026

Revisión de Validez 29/02/2028

Descripción

CRYPTOTRACK es una solución en la nube diseñada para ayudar a organizaciones a detectar, analizar y prevenir actividades ilícitas en el entorno digital, con foco en la ciberdelincuencia y el uso fraudulento de criptoactivos. La plataforma integra análisis de fuentes abiertas, procesamiento de información mediante inteligencia artificial y análisis avanzado de transacciones en redes blockchain, proporcionando una visión completa y accionable del riesgo.

Permite identificar y clasificar comportamientos sospechosos, automatizar la detección de patrones anómalos mediante modelos de IA, realizar el seguimiento de flujos económicos, correlacionar información procedente de la surface y la dark web, y evaluar el riesgo asociado a direcciones y entidades cripto. Incorpora capacidades de generación de alertas, definición de perfiles de riesgo y elaboración de informes unificados, facilitando la detección temprana de amenazas y apoyando la toma de decisiones.

Con un enfoque modular y escalable, alineado con las normativas y regulaciones europeas desde el diseño, CRYPTOTRACK ha sido desarrollada en colaboración con usuarios finales e incorpora estándares de seguridad y privacidad, incluyendo mecanismos de control de modelos de IA.

Observaciones

N/A

9.6 FORMACIÓN Y CONCIENCIACIÓN

Trend Micro Vision One Email and Collaboration Security

Versión	
Fabricante	Trend Micro
Familia	Formación y Concienciación
Tipo	Servicio
Fecha Inclusión	01/04/2026
Revisión de Validez	30/06/2027

Descripción

Vision One – Email and Collaboration Security, es la propuesta de Trend Micro para proteger Entornos de Correo electrónico y colaborativos independientemente de su ubicación (nube/Onpremise) o tecnología empleada.
Forma parte de la plataforma de Ciberseguridad Empresarial Trend Vision One y brinda en 2 capas complementarias de seguridad:
Transporte MTA:
Donde se integra en el flujo de correo SMTP entrante y/o saliente del cliente proporcionando seguridad robusta a nivel de conexión, transporte, contenido y comportamiento antes de que el correo sea entregado en su destino.
Integración API:
La cual se integra a nivel de API con distintos productos y servicios de correo y colaborativos: Microsoft 365 (Exchange Online (modo Inline/Online), SharePoint, OneDrive, Teams), Microsoft Exchange, Google Workspace (Modo Inline/Online), Box y Dropbox. Permitiendo un análisis y protección del correo entrante, saliente y correo interno así como los distintos flujos de información asociados a los entornos colaborativos.
Todo lo anterior proporcionado de manera activa o en modo monitorización y alimentando la telemetría XDR y de gestión del riesgo proporcionadas por Trend Vision One

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Kaspersky Automated Security Awareness Platform

Versión

Fabricante KASPERSKY LAB

Familia Formación y Concienciación

Tipo Servicio

Fecha Inclusión 07/01/2026

Revisión de Validez 31/12/2027

Descripción

Kaspersky Automated Security Awareness Platform (KASAP) automatiza el ciclo completo de concienciación (evaluación, educación, simulación, medición) mediante motor adaptativo que personaliza itinerarios según perfil de riesgo, comportamiento y evolución de competencias del usuario. Gestiona formación unificada en ciberamenazas y normativas organizacionales, eliminando carga administrativa.

Características Principales:

• Motor Adaptativo: Planes de estudios por nivel inicial/progreso usuario, cubriendo Deepfakes(IA), cadena suministro, ciberseguridad Industrial(ICS/OT) y Whaling.
• Soporte SCORM: Importa/despliega cursos propios para unificar ciberformación con políticas internas, cumplimiento legal y trazabilidad completa.
• Simulación Phishing: Campañas email personalizables con refuerzo inmediato y botón reporte incidentes vía complemento correo.
• Integración/Métricas: APIs nativas, SIEM(KUMA), Kaspersky XDR para correlacionar factor humano-detección técnica; métricas NIS2 Art.21 y ENS personal.”

Observaciones

N/A

Cyber Guru s.r.l

Versión 2.0

Fabricante Cyber Guru

Familia Formación y Concienciación

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

SMARTFENSE

Versión

Fabricante Defense Balance

Familia Formación y Concienciación

Tipo Servicio

Fecha Inclusión 27/03/2025

Revisión de Validez 28/02/2027

Descripción

La plataforma SMARTFENSE transforma la concienciación en ciberseguridad en una estrategia de defensa activa frente al riesgo humano: •A través de una amplia gama de contenidos 100% personalizables, con catálogos diseñados para distintos niveles de complejidad y sectores industriales críticos. •Con marca blanca, adaptándose a la identidad única de una organización y cumpliendo con las normativas vigentes. •Una vasta cantidad de componentes innovadores, como módulos interactivos, newsletters, videos, videojuegos, cómics, momentos educativos, nudges y muchos más. •Ejercicios realistas con simulaciones de phishing y ransomware, con la opción de insertar el mensaje directamente en la bandeja de entrada de los usuarios destinatarios para una entrega efectiva. •Concienciación al usuario en el momento justo si realiza un comportamiento de riesgo. •Detección precisa de falsos positivos, que permite evaluar y optimizar la efectividad de las acciones, asegurando resultados confiables y una respuesta proactiva y medible ante amenazas. •La oportunidad de administrar de manera centralizada diversas entidades. •Integraciones estratégicas: se conecta sin esfuerzo con Microsoft Entra ID, Google Workspace, Slack y SAP SuccessFactors, entre otras.

Observaciones

No aplica la publicación de procedimiento de empleo seguro.

EVE Intelligence

Versión	
Fabricante	TICSMART TECHHEROX SOFT COM INFORMATICA UTE
Familia	Formación y Concienciación
Tipo	Servicio
Fecha Inclusión	01/04/2026
Revisión de Validez	31/03/2028

Descripción

EVE Intelligence es una solución de ciberseguridad orientada a la identificación y gestión del riesgo asociado al factor humano en las organizaciones. El sistema analiza variables de personalidad y comportamiento, junto con factores contextuales y tecnológicos, para predecir niveles de vulnerabilidad frente a ciberataques a nivel individual y agregado, basado en su inédito algoritmo ético.
La solución permite realizar evaluaciones iniciales y un seguimiento continuo del riesgo, así como la ejecución de simulaciones de amenazas adaptadas a distintos perfiles de usuario, de acuerdo a su personalidad. Asimismo, facilita acciones de mitigación mediante contenidos personalizados dirigidos al autoconocimiento y corrección de sesgos cognitivos detectados.
Los resultados se presentan en un panel de control con métricas, segmentación por colectivos, trazabilidad y plan de acción, adicionalmente la solución dispone de capacidades de integración con herramientas corporativas de seguridad.

Observaciones

N/A

ATTACK Simulator

Versión	1.0.0
Fabricante	Attack Simulator
Familia	Formación y Concienciación
Tipo	Servicio
Fecha Inclusión	21/10/2024
Revisión de Validez	31/10/2026

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

TIER8

Versión

Fabricante Tier8 Solutions

Familia Formación y Concienciación

Tipo Servicio

Fecha Inclusión 13/11/2025

Revisión de Validez 31/10/2027

Descripción

TIER8 es la solución inmersiva de concienciación y formación que compromete y entrena culturas de ciberseguridad con escenarios, simulaciones y datos para prevenir y responder amenazas, sin las consecuencias de experimentar un incidente real.

Observaciones

N/A

Ángeles

Versión 1.0

Fabricante CSA / CCN

Familia Formación y Concienciación

Tipo Servicio

Fecha Inclusión 01/09/2023

Revisión de Validez 31/01/2027

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

SoSafe Concienciación y Formación en Ciberseguridad

Versión

Fabricante SoSafe SE

Familia Formación y Concienciación

Tipo Servicio

Fecha Inclusión 30/04/2026

Revisión de Validez 31/03/2028

Descripción

SoSafe es una plataforma de gestión adaptativa del riesgo humano que permite identificar, medir y reducir el riesgo asociado al comportamiento de los usuarios en ciberseguridad. La solución combina formación adaptativa, simulaciones de ataques y capacidades de reporte y gestión de incidentes, permitiendo evaluar y mejorar la respuesta frente a amenazas de ingeniería social como phishing, smishing, vishing y ataques multicanal. La plataforma genera simulaciones basadas en amenazas reales mediante un motor de recreación de ataques, distribuyéndolas de forma segmentada según el perfil y comportamiento de cada usuario. Incluye un sistema de aprendizaje personalizado, con microcontenidos y rutas formativas dinámicas que se ajustan automáticamente al desempeño del usuario.
Asimismo, incorpora funcionalidades de reporte de amenazas en un clic, integradas en herramientas de correo electrónico y colaboración, así como un entorno centralizado para la gestión y análisis de los eventos reportados. Los incidentes pueden convertirse en nuevas acciones formativas, cerrando el ciclo entre detección y prevención. Permite monitorizar la evolución del riesgo y generar reportes para auditoría mediante indicadores cuantitativos y modelos de scoring.

Observaciones

N/A

Zepo

Versión

Fabricante Zepo Intelligence

Familia Formación y Concienciación

Tipo Servicio

Fecha Inclusión 01/03/2026

Revisión de Validez 29/02/2028

Descripción

Zepo Intelligence es la primera plataforma de inteligencia social agéntica para la seguridad del espacio de trabajo. A diferencia de las soluciones tradicionales, la plataforma de Zepo lleva la formación y las simulaciones al siguiente nivel al integrar la gestión del riesgo humano con la detección de amenazas en tiempo real. Esto permite la protección holística de los empleados a través de múltiples canales del espacio de trabajo digital, creando una capa de defensa unificada y proactiva.

Observaciones

N/A

PSAT-Proofpoint Security Awareness Training

Versión

Fabricante Proofpoint

Familia Formación y Concienciación

Tipo Servicio

Fecha Inclusión 01/03/2022

Revisión de Validez 14/07/2027

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

Kymatio

Versión

Fabricante Kymatio

Familia Formación y Concienciación

Tipo Servicio

Fecha Inclusión 01/02/2024

Revisión de Validez 01/02/2028

Descripción

Kymatio® es la plataforma SaaS de gestión del ciberriesgo humano que permite a las organizaciones identificar, medir, reducir y evidenciar el riesgo asociado al comportamiento digital de las personas.

La solución combina evaluación y concienciación individualizada, simulaciones multivector de ingeniería social, monitorización de credenciales expuestas, análisis de exposición humana, métricas de evolución y planes de acción priorizados. Entre sus capacidades de simulación y preparación frente a amenazas se incluyen escenarios de phishing, QR phishing, smishing, malware e ingeniería social y ataques basados de vishing con IA.

De este modo, Kymatio® proporciona a los equipos de seguridad, cumplimiento, recursos humanos y dirección una visión operativa y ejecutiva del riesgo humano dentro de la organización.

Kymatio® permite alcanzar visibilidad sobre la exposición de la plantilla a incidentes de seguridad de la información y activar medidas de mitigación adaptadas a usuarios y áreas de riesgo. La plataforma cubre ámbitos clave como puesto de trabajo, cumplimiento, protección de datos, comunicaciones, malware, gestión de contraseñas, ingeniería social, exposición de credenciales y simulaciones de ataque.

Kymatio® facilita el seguimiento continuo de la evolución del riesgo humano, la identificación de colectivos vulnerables, la priorización de acciones y la generación de evidencias útiles para programas de gobierno de la seguridad, cumplimiento normativo y mejora continua bajo marcos como ENS, NIS2, DORA, ISO 27001 y políticas internas de ciberseguridad.

Observaciones

CCN-STIC 1703. Procedimiento de Empleo Seguro Kymatio

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	*Common Criteria*
CCN	*Centro Criptológico Nacional*
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación*
EDR	*Endpoint Detection and Response*
ENECSTI	*Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información*
ENS	*Esquema Nacional de Seguridad.*
EPP	*Endpoint Protection Platform*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
PES	*Procedimiento de Empleo Seguro*
RFS	*Requisitos Fundamentales de Seguridad*
STIC	*Seguridad de las Tecnologías de la Información y la Comunicación*
TIC	*Tecnologías de la Información y la Comunicación*

PUBLICACIONES DE DEFENSA

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