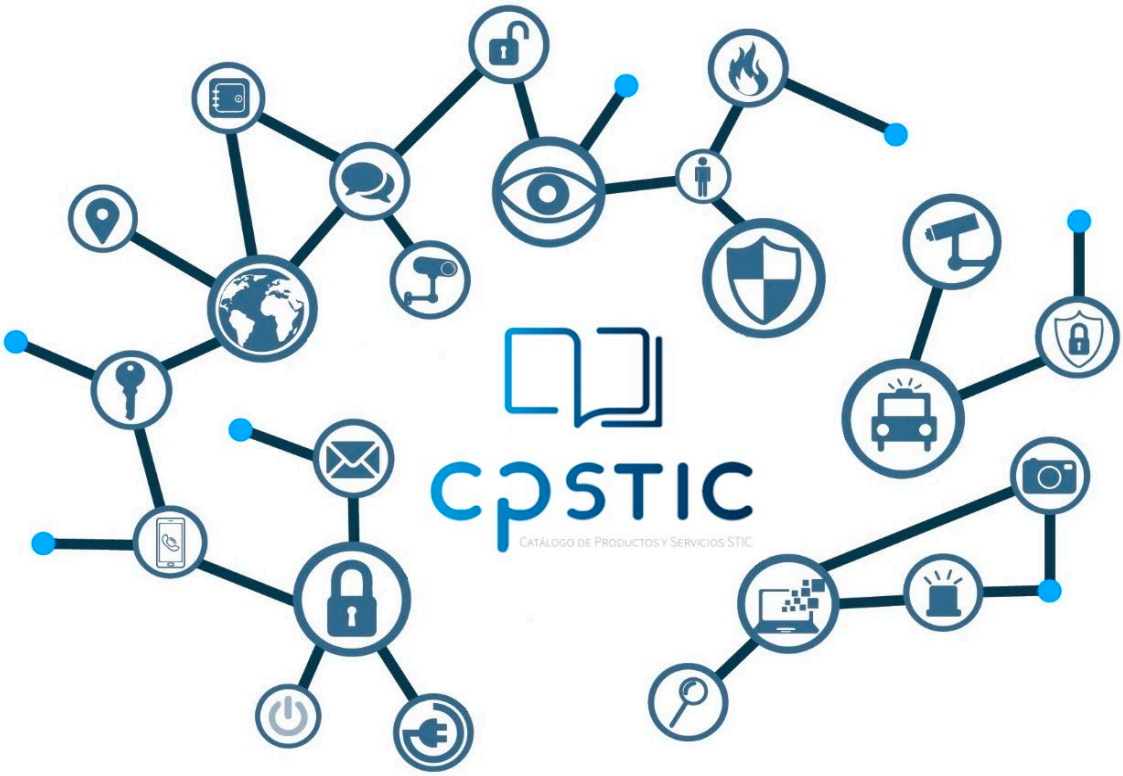
centro criptológico nacional

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



Noviembre de 2023

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO:083-23-034-4

Fecha de Edición: noviembre de 2023

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.11.24 10:23:31 +01'00'

ÍNDICE

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.

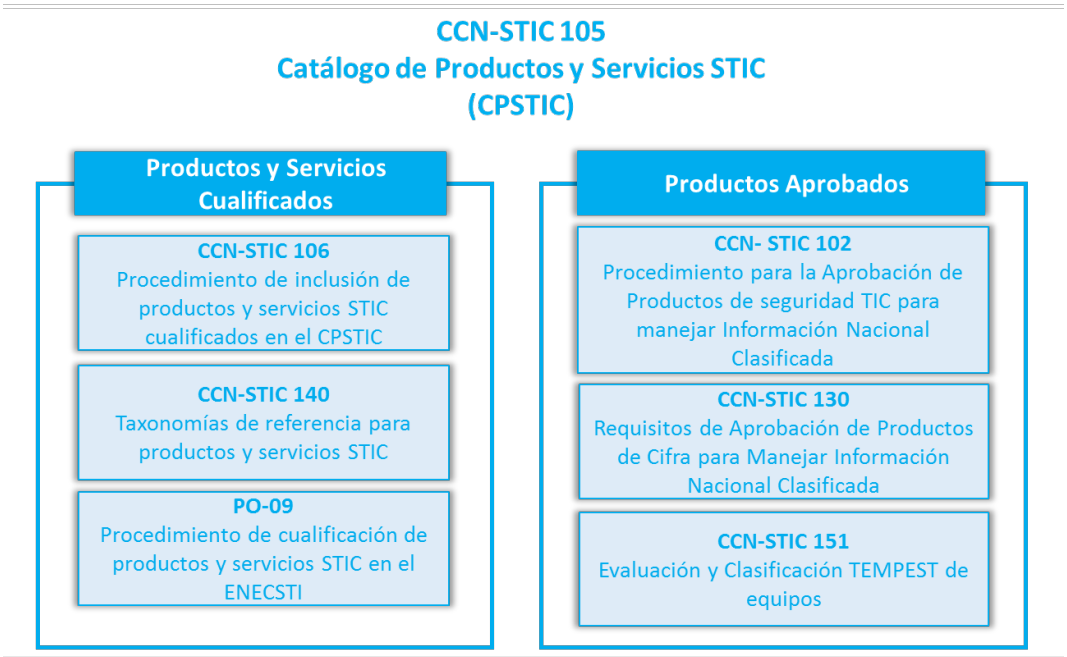


Figura 1. Inclusión de productos y servicios de seguridad en el CPSTIC

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 CUALIFICADOS

INFORMACIÓN IMPORTANTE

INFORMACIÓN IMPORTANTE

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

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

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

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

INFORMACIÓN IMPORTANTE

7.1 HERRAMIENTAS PARA EL DESARROLLO DE PRODUCTOS DE SEGURIDAD

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

Este módulo provee los servicios de cifrado y seguridad para garantizar la comunicación tanto con el servidor IMS como con los terminales remotos con un cifrado extremo a extremo.
Este módulo criptográfico está diseñado como una librería criptográfica e incorporado a aplicaciones de comunicaciones en entorno de movilidad debidamente aprobadas, e instaladas en plataformas confiables.

Observaciones

Procedimiento de empleo pendiente de publicación

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

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

Observaciones

No aplica

INFORMACIÓN IMPORTANTE

TRNG-P200 Physical True Random Number Generator

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

Descripción

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

Observaciones

No aplica

INFORMACIÓN IMPORTANTE

7.2 CONTROL DE ACCESO

7.2.1 CONTROL DE ACCESO A RED (NAC)

Forescout 8.3 (CT-R, CT-100, CT-1000, CT-2000, CT-4000, CT-10000, CEM-5, CEM-10, CEM-25, CEM-50, CEM-100, CEM-150, CEM-200, 4130, 5110, 5120, 5140, 5160)	
Versión	8.4
Fabricante	Forescout
Familia	Control de acceso a red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2023
Revisión de Validez	01/04/2025
Descripción	

La plataforma Forescout es una plataforma unificada de seguridad que permite a las empresas y organismos oficiales obtener información completa sobre el estado de sus entornos empresariales ampliados y orquestar medidas destinadas a reducir el riesgo operativo y de ciberseguridad. Se despliega de forma rápida y segura en entornos de campus, centros de datos, la nube y redes de OT. Ofrece descubrimiento, clasificación en tiempo real y evaluación continua de estado, sin necesidad de agentes. Para más información, véase: https://forescouttechnologies.es

Observaciones

CCN-STIC-1106 Procedimiento de empleo seguro Forescout

EMMA / OpenNac Enterprise	
Versión	1.2
Fabricante	OpenCloud Factory / CCN
Familia	Control de acceso a red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2020
Revisión de Validez	31/12/2023
Descripción	

EMMA es una solución de Visualización de activos en una red, su autenticación y segregación, así como la automatización de auditorías de seguridad de la infraestructura. El alcance de la cualificación abarca los siguientes módulos de EMMA: Visibilidad, Control / Respuesta, Segmentación, Cumplimiento, BYOD y Gestión de invitados. Se recoge el inventario y perfilado del equipo que se podrá utilizar en las políticas de acceso a la conexión remota. Adicionalmente, permite definir y aplicar políticas de acceso en función de una postura de seguridad basada en el nivel de bastionado, además de otros factores (horario de la conexión, características del equipo, role de usuario etc.). EMMA se integrará con soluciones del ecosistema CCN-CERT: ROCIO y ANA. https://www.ccn-cert.cni.es/pdf/documentos-publicos/4153-datasheet-emma/file.html

Observaciones

CCN-STIC-1105 Procedimiento de empleo seguro EMMA

INFORMACIÓN IMPORTANTE

7.2.2 SERVIDORES DE AUTENTICACIÓN

Location-Based Identity Platform	
Versión	N/A
Fabricante	Ironchip Telco, S.L.
Familia	Servidores de Autenticación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/04/2024

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

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.2.3 GESTIÓN DE ACCESO PRIVILEGIADO (PAM)

Safeguard for Priviledge Passwords	
Versión	6.7
Fabricante	One Identity
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023

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 Account Security Solution

Versión	10.10
Fabricante	CyberArk
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	24/06/2024

Descripción

CyberArk Core PAS es una solución de seguridad que permite proteger, controlar y monitorizar el acceso privilegiado a infraestructura locales, en la nube e híbridas. Permite a las organizaciones administrar y proteger las credenciales de las cuentas privilegiadas y los derechos de acceso, monitorizar y controlar la actividad de las cuentas privilegiadas, identificar las actividades sospechosas y responder a las amenazas. Permite:

- Asegurar y controlar centralmente el acceso a las credenciales privilegiadas basadas en políticas de seguridad definidas administrativamente
- Aislar y asegurar sesiones de usuarios privilegiados. Las capacidades de monitorización y grabación permiten a los equipos de seguridad ver sesiones privilegiadas en tiempo real, suspender automáticamente y terminar remotamente las sesiones sospechosas.
- Detectar, alertar y responder a actividades privilegiadas anómalas.
- Controlar el acceso de privilegios mínimos para * NIX y Windows. La solución permite a los usuarios con privilegios ejecutar comandos administrativos autorizados desde sus sesiones nativas de Unix o Linux, a la vez que se eliminan los privilegios de raíz innecesarios.
- Proteger los controladores de dominio de Windows.

No se incluye en la cualificación los conectores basados en Internet Explorer.

Observaciones

CCN-STIC-1108 PES CyberArk Privileged Account Security Solution PAS

INFORMACIÓN IMPORTANTE

7.2.4 GESTIÓN DE IDENTIDADES (IM)

AWS IAM Identity Center	
Versión	2022-07-26
Fabricante	AWS
Familia	Gestión de identidades (IM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023

Descripción

AWS IAM Identity Center (sucesor de AWS Single Sign-On) es un servicio en la nube que facilita la administración centralizada del acceso a varias cuentas de AWS y aplicaciones empresariales.
Con AWS IAM Identity Center, puede administrar fácilmente el acceso centralizado y los permisos de usuario para todas sus cuentas de AWS Organizations. AWS IAM Identity Center también incluye integraciones incorporadas con aplicaciones de AWS, y muchas aplicaciones empresariales, como Salesforce, Box y Microsoft Office 365. Además, mediante el asistente de configuración de aplicaciones de AWS IAM Identity Center, puede crear integraciones de Security Assertion Markup Language (SAML) 2.0 y ampliar el acceso SSO a cualquiera de sus aplicaciones compatibles con SAML.
Sus usuarios solo tienen que iniciar sesión en un portal de usuario con las credenciales que configuren en AWS IAM Identity Center o utilizando sus credenciales corporativas existentes para acceder a todas sus cuentas y aplicaciones asignadas desde un único lugar.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

SailPoint IdentityIQ

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

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

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

AWS Identity Access Management (IAM) + AWS STS	
Versión	n/a
Fabricante	AWS
Familia	Gestión de identidades (IM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/08/2022
Revisión de Validez	31/12/2023

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

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.3 SEGURIDAD EN LA EXPLOTACIÓN

7.3.1 ANTI-VIRUS / EPP (ENDPOINT PROTECTION PLATFORM)

Autonomous AI Endpoint Security Platform	
Versión	Console Tokyo#19, agent 23.1.1
Fabricante	SentinelOne
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2023
Revisión de Validez	31/12/2023
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

Procedimiento de Empleo Seguro pendiente de publicación

Deep Security (Manager y Agente/Relay Linux/Windows)	
Versión	11.0
Fabricante	Trend Micro
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024
Descripción	

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

Observaciones

CCN-STIC-1216 PES Trendmicro Deep Security

INFORMACIÓN IMPORTANTE

Cytomic EDR/EPDR	
Versión	4.2 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	31/12/2023

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-1211 Procedimiento de empleo seguro Cytomic EPDR

WatchGuard EPDR/Advanced EPDR	
Versión	4.2 (Protection Agent v8.0)
Fabricante	WatchGuard Technologies
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/03/2023
Revisión de Validez	31/12/2023

Descripción

WatchGuard EDR/EPP integra en una única solución un conjunto completo de tecnologías preventivas en el endpoint, con capacidades EDR y el Servicio Zero-Trust Application. Extiende las capacidades de prevención, detección y respuesta con una gama completa de capacidades de protección del endpoint necesarias para evitar que las amenazas lleguen a los dispositivos y servidores y reducir la superficie de ataque. Sus capacidades de protección avanzada cubren todas 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 servicios de Threat Hunting y Análisis Forense, que permite una enforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1213 PES Panda Adaptive Defense 360

INFORMACIÓN IMPORTANTE

Cortex XDR Agente Windows

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

Descripción

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

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

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

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

Observaciones

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

INFORMACIÓN IMPORTANTE

Kaspersky Endpoint Security for Windows	
Versión	11.6.0.395 AES256
Fabricante	KASPERSKY LAB, S.L.U.
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024

Descripción

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

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

Observaciones

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

ESET Endpoint Security

Versión	7.3
Fabricante	ESET
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/04/2020
Revisión de Validez	31/12/2023

Descripción

ESET Endpoint Security es una solución fácil de implementar y utilizar, administrable de forma centralizada, con protección multicapa que se basa en tres pilares básicos: primar el rendimiento del sistema, una detección eficaz y no importunar al usuario con falsos positivos. Este enfoque de protección multicapa permite a ESET detectar y/o bloquear diferentes tipos de amenazas, como ransomware, ataques sin archivos, botnets, ataques de red o exploits. Los componentes de protección que han sido analizados en el proceso de cualificación son: 1) Antivirus y antiespía: Elimina todo tipo de amenazas tales como virus, rootkits, gusanos y software espía. 2) Sistema avanzado de prevención de intrusiones (HIPS): Permite controlar los procesos, archivos y claves de registro a través de reglas. Protege frente a modificaciones no autorizadas y detecta las amenazas basándose en su comportamiento en el sistema. 3) Análisis avanzado de memoria: Monitoriza el comportamiento de todos los procesos y los analiza cuando se ejecutan en memoria. Esto permite una prevención más efectiva contra las infecciones, incluso en el caso de que estén especialmente diseñadas para evitar su detección. 4) Protección contra botnets: Evita que los equipos de tu empresa formen parte de una red de equipos controlados por cibercriminales para distribuir correo no deseado o lanzar ataques dirigidos.

Observaciones

CCN-STIC 1204 Procedimiento de empleo seguro ESET Endpoint Security 7

Falcon Sensor

Versión	6.49
Fabricante	CrowdStrike
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2022
Revisión de Validez	30/04/2024

Descripción

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

Observaciones

CCN-STIC-1217 PES FALCON SENSOR

INFORMACIÓN IMPORTANTE

Panda Adaptive Defense 360	
Versión	4.2 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	31/12/2023

Descripción

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

Observaciones

CCN-STIC-1213 PES Panda Adaptive Defense 360

INFORMACIÓN IMPORTANTE

7.3.2 EDR (ENDPOINT DETECTION AND RESPONSE)

Autonomous AI Endpoint Security Platform	
Versión	Console Tokyo#19, agent 23.1.1
Fabricante	SentinelOne
Familia	EDR (Endpoint Detection and Response)
Tipo	Servicio
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2023
Revisión de Validez	31/12/2023
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

Procedimiento de Empleo Seguro pendiente de publicación

Stormshield Endpoint Security Evolution	
Versión	2.2.2
Fabricante	Stormshield
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2022
Revisión de Validez	31/12/2023
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

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Deep Security (Manager y Agente/Relay Linux/Windows)	
Versión	11.0
Fabricante	Trend Micro
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024
Descripción	

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

Observaciones

CCN-STIC-1216 PES Trendmicro Deep Security

Cytomic EDR/EPDR	
Versión	4.2 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	31/12/2023
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-1211 Procedimiento de empleo seguro Cytomic EPDR

INFORMACIÓN IMPORTANTE

Microsoft Defender for Endpoint

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

Descripción

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

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

Observaciones

CCN-STIC-885E Guía de configuración segura para Microsoft Defender for Endpoint (Guía en proceso de adaptación)

WatchGuard EPDR/Advanced EPDR

Versión	4.2 (Protection Agent v8.0)
Fabricante	WatchGuard Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/03/2023
Revisión de Validez	31/12/2023

Descripción

WatchGuard EDR/EPP integra en una única solución un conjunto completo de tecnologías preventivas en el endpoint, con capacidades EDR y el Servicio Zero-Trust Application. Extiende las capacidades de prevención, detección y respuesta con una gama completa de capacidades de protección del endpoint necesarias para evitar que las amenazas lleguen a los dispositivos y servidores y reducir la superficie de ataque. Sus capacidades de protección avanzada cubren todas 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 servicios de Threat Hunting y Análisis Forense, que permite una enforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1213 PES Panda Adaptive Defense 360

INFORMACIÓN IMPORTANTE

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

Descripción

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

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

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

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

Observaciones

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

INFORMACIÓN IMPORTANTE

Kaspersky Endpoint Security for Windows	
Versión	11.6.0.395 AES256
Fabricante	KASPERSKY LAB, S.L.U.
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024

Descripción

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

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

Observaciones

Procedimiento de empleo seguro pendiente de publicación

Mobileiron Mobile Threat Defense – MTD	
Versión	11.1
Fabricante	Mobileiron
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024

Descripción

MobileIron Threat Defense permite supervisar, administrar y securizar los dispositivos móviles frente a ciberataques en dispositivos, redes y aplicaciones. Detecta las amenazas, tanto conocidas, como zero-day, incluso sin conectividad en red. Los cuatro pilares que definen esta funcionalidad de seguridad son la detección proactiva de amenazas y ataques, la corrección puntual, una mayor visibilidad de los dispositivos y de la red y una fácil administración.

Observaciones

CCN-STIC-1219 Procedimiento de Empleo Seguro Mobile Threat Defense (MTD)

INFORMACIÓN IMPORTANTE

Falcon Sensor

Versión	6.49
Fabricante	CrowdStrike
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2022
Revisión de Validez	30/04/2024

Descripción

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

Observaciones

CCN-STIC-1217 PES FALCON SENSOR

Harmony Mobile

Versión	3
Fabricante	Check Point Software Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2023

Descripción

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

Observaciones

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

INFORMACIÓN IMPORTANTE

Harmony SandBlast Mobile (iOS)

Versión	versión 4.1
Fabricante	Check Point Software Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2023

Descripción

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

Observaciones

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

Panda Adaptive Defense 360

Versión	4.2 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	31/12/2023

Descripción

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

Observaciones

CCN-STIC-1213 PES Panda Adaptive Defense 360

INFORMACIÓN IMPORTANTE

7.3.3 HERRAMIENTAS DE FILTRADO DE NAVEGACIÓN

Cisco Web Security Appliance (S690, S690X, S695, S695F, S680, S390, S380, S395, S190, S195)	
Versión	AsyncOS 11.8
Fabricante	Cisco Systems
Familia	Herramientas de filtrado de navegación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	31/05/2025
Descripción	

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

Observaciones

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

INFORMACIÓN IMPORTANTE

7.3.4 SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM)

MONSE	
Versión	Probe 1.0, Agente 8.3.2
Fabricante	GRUPO CIES
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	31/12/2023
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

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

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

La plataforma XDR de Netwitness (an RSA Business), es la solución de SIEM evolucionado o XDR (eXtended Detection and Response), con capacidades de visibilidad completa gracias a su modelo de datos unificado pudiendo capturar logs, netflows, tráfico de red, actividad en los end points, además de información de inteligencia de seguridad, de forma integrada, bajo un único motor de análisis y correlación avanzada. Además, incluye funcionalidades necesarias por un SOC para hacer frente a amenazas complejas. Netwitness Platform XDR cuenta además con componentes adicionales como UEBA (User and Entity Behaviour 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

Gloria	
Versión	v5.8.1
Fabricante	S2 GRUPO / CCN
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2021
Revisión de Validez	30/06/2024
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

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	31/01/2024
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

Microsoft Sentinel

Versión	n/a
Fabricante	Microsoft Iberica SRL
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/11/2024

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-884E Guía de configuración segura para Azure Sentinel (Guía en proceso de adaptación)

INFORMACIÓN IMPORTANTE

ASIP (AIUKEN SECURITY INTELLIGENCE PLATFORM)

Versión	Delfos Linux Agent v0.8.10
Fabricante	AIUKEN SOLUTIONS
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Servicio
Categoría ENS	MEDIA
Fecha Inclusión	01/03/2023
Revisión de Validez	31/12/2023

Descripción

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

Integra a su vez, portal de servicio, gestión de casos y ticketing, motor de generación de paneles informativos y KPIs, Threat Intelligence propia y herramientas para Threat Hunting y detección temprana.

La automatización es otra de las ventajas de ASIP, orquestación y SOAR para el modelado de procesos autogestionado y generación de informes de servicio de forma automática, permitiendo a los técnicos enfocarse en las tareas importantes.

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

Observaciones

El componente Forwarder corre sobre un ubuntu 20.04, cuyo soporte finaliza en abril de 2025. El hipervisor que debe utilizar el usuario es ESXi 6.5.0 (EOL 15/11/2023), sobre el que se despliega la MV del forwarder. Se entiende que la misma máquina va a correr en versiones posteriores del hipervisor.

INFORMACIÓN IMPORTANTE

LogICA5 Next Generation SIEM

Versión	v7.1
Fabricante	Grupo ICA Sistemas y Seguridad
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2020
Revisión de Validez	30/06/2024

Descripción

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

Observaciones

CCN-STIC-1206 PES NGSIEM LogICA

INFORMACIÓN IMPORTANTE

7.3.5 DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS

EP543N	
Versión	V.1.7
Fabricante	Epicom
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2024
Descripción	

Centro de Gestión de cifradores IP EP430GN sobre ordenador seguro EP1140.

Observaciones

EP543X	
Versión	SW v 4.15
Fabricante	Epicom
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2024
Descripción	

Centro de Gestión sobre la plataforma EP1140, que da soporte a los cifradores de la familia EP430, incluidos los modelos EP430TX y EP430GX.

Observaciones

Utilización según PE-2012-49 Procedimiento de Empleo EP430GX v2

INFORMACIÓN IMPORTANTE

AWS Key Management Service (KMS)	
Versión	
Fabricante	AWS
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/12/2023
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

Google KMS with EKM solution

Versión	n/a
Fabricante	Google Cloud
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/05/2023
Revisión de Validez	31/12/2023

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

7.4 MONITORIZACIÓN DE LA SEGURIDAD

7.4.1 IDS, IPS Y ANTIDDOS

Cisco Firepower Threat Defense (FTD) en Firepower 1000 y 2100 Series (FP1010, FP1120, FP1140, FP2110, FP2120, FP2130, FP2140)	
Versión	FTD 6.4 y FMC/FCMv 6.4
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2024
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).
Compatible con:
-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
-FMCv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC-651B Seguridad en cortafuegos CISCO Firepower

Firepower 8000 Series Appliances: Firepower 8350, 8360, 8370, 8390	
Versión	6.4
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025
Descripción	

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

Observaciones

CCN-STIC-651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

FMC (Firepower Management Center) Appliances: FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9	
Versión	6.4.0.17
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025
Descripción	

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

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

Observaciones

CCN-STIC-651B Seguridad en Cortafuegos Cisco Firepower

FMCv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E180D	
Versión	6.4
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025
Descripción	

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

Observaciones

CCN-STIC-651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

NGIPSv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E18	
Versión	6.4
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025
Descripción	

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

Observaciones

CCN-STIC-651B Seguridad en Cortafuegos Cisco Firepower

Firepower AMP Appliances: AMP 8350, 8360, 8370, 8390	
Versión	6.4
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025
Descripción	

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

Observaciones

CCN-STIC-651B Seguridad en Cortafuegos Cisco Firepower

INFORMACIÓN IMPORTANTE

Cisco FTD (NGFW) 6.4 en Firepower Series 4100 y 9300 con FMC/FMCv	
Versión	6.4
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025
Descripción	

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

Observaciones

CCN-STIC-651B Seguridad en Cortafuegos Cisco Firepower

Cisco ASA 5500 Series (5508-X and 5516-X)	
Versión	7.0
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de publicación de Procedimiento de Empleo Seguro

INFORMACIÓN IMPORTANTE

FTDv running on ESXi 6.7 or 7.0 on Cisco Unified Computing System (UCS) - UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3 installed on ISR	
Versión	7.0
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de publicación de Procedimiento de Empleo Seguro

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 installed on ISR	
Versión	7.0
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de Publicación de Procedimiento de Empleo Seguro

INFORMACIÓN IMPORTANTE

FTDv running on NFVIS 4.4 on the ENCS 5406, 5408, and 5412	
Versión	7.0
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de Publicación de Procedimiento de empleo seguro

ISA 3000 (ISA 3000-4C and ISA 3000-2C2F)	
Versión	7.0
Fabricante	Cisco Systems
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de Publicación de Procedimiento de Empleo Seguro

INFORMACIÓN IMPORTANTE

Deep Discovery Inspector	
Versión	6.5.1129
Fabricante	Trend Micro
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	N/A
Revisión de Validez	30/04/2024

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

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

TippingPoint Threat Protection System

Versión	5.4.1
Fabricante	Trend Micro
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

Descripción

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

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

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

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

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

Observaciones

CCN-STIC-1220 PES TIPPING POINT TRENDMICRO

INFORMACIÓN IMPORTANTE

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	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2026
Descripción	

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

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

SonicWall SOHO Serie (250, 250W)	
Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024
Descripción	

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

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

SonicWall TZ Serie (300P, 350, 350W, 600P)	
Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024

Descripción

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

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

7.4.2 CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO

CARMEN	
Versión	Versión 7.16.1
Fabricante	S2 GRUPO / CCN
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2023
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 7.2.4

GigaVUE (GVS-HC301, GVS-HC302, GVS-HC2A1, GVS-HC2A2, GVS-HC101 y GVS-HC102)	
Versión	6.1
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	28/06/2023
Revisión de Validez	30/06/2024
Descripción	

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

Observaciones

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

INFORMACIÓN IMPORTANTE

GigaVUE (GVS-TAX21-HW, GVS-TAX22-HW, GVS-TAX21A-HW, GVS-TAX22A-HW, GVS-TAC21, GVS-TAC22, GTP-ATX21, GTP-ASF21)	
Versión	6.1
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	28/06/2023
Revisión de Validez	30/06/2024

Descripción

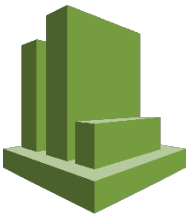
Network Packet Brokers HC Series. Network Packet Brokers de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1g/10g en cobre y funcionalidades de filtrado de trafico L2-3-4-7 con motor de DPI, generación de Netflow/IPFix/Metadatos, Cifrado/Descifrado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

Observaciones

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

INFORMACIÓN IMPORTANTE

CloudWatch



Versión	API Version 2010-08-01
Fabricante	AWS
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	31/12/2023

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

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.4.3 HERRAMIENTAS DE SANDBOX

Deep Discovery Inspector	
Versión	6.5.1129
Fabricante	Trend Micro
Familia	Herramientas de Sandbox
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	N/A
Revisión de Validez	30/04/2024

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

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.5 PROTECCIÓN DE LAS COMUNICACIONES

7.5.1 ENRUTADORES

Cisco Catalyst 9300L Series Switches (C9300L-24T|P-4G, C9300L-48T|P|PF-4G, C9300L-24T|P|UXG-4X, C9300L-48T|P|PF|UXG-4X, C9300L-24UXG-2Q, C9300L-48UXG-2Q)	
Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	14/11/2023
Revisión de Validez	30/04/2024
Descripción	

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

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

7950 (XRS-40, XRS-20, XRS-16C), 7750 (SR-12e, SR-12, SR-7, SR-c12, SR-c4), 7450 (ESS-1, ESS-6, ESS-6v, ESS-7, ESS-12)	
Versión	SR OSv12.0
Fabricante	NOKIA
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	01/01/2024
Descripción	

Pendiente

Observaciones

Procedimiento de empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

Aruba Switch 2930F, 2930M, 3810M y 5400R

Versión ArubaOS 16.08
Fabricante Aruba
Familia Enrutadores
Tipo Producto
Categoría ENS ALTA
Fecha Inclusión 01/12/2021
Revisión de Validez 31/05/2024

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-647C Seguridad en conmutadores HPE Aruba

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

Versión SAR OS v6.1
Fabricante NOKIA
Familia Enrutadores
Tipo Producto
Categoría ENS ALTA
Fecha Inclusión 01/01/2023
Revisión de Validez 01/01/2024

Descripción

Pendiente

Observaciones

Procedimiento de empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9600 Series Switches (C9606R, C9600-SUP-1 y C9600-LC-24C|48YL|48TX|24S)	
Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	13/11/2023
Revisión de Validez	30/04/2024
Descripción	

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

Observaciones

Cisco Catalyst 9500 Series Switches (C9500-12Q|24Q|40X|16X|32C|32QC|24Y4C|48Y4C) con los siguientes módulos de red (C9500-NM-8X y C9500-NM-2Q)	
Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	13/11/2023
Revisión de Validez	30/04/2024
Descripción	

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

Observaciones

INFORMACIÓN IMPORTANTE

Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800) y Cisco Catalyst 8300 Rugged Series Routers (IR8300)	
Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2023
Revisión de Validez	29/02/2024
Descripción	

Cisco Catalyst 8000V Edge (C8000V): C8000V virtual router deployed on one of the following compatible platforms:
- Cisco UCS C-Series M5 Servers with Intel Xeon Scalable 2nd Generation (Cascade Lake)
- General-purpose computing platforms with Intel Broadwell processors: Xeon D-1559
- General-purpose computing platforms with Intel Goldmont processors: Atom E3950
- General-purpose computing platforms with Intel Coffee Lake processors: Xeon E-2254ML

Cisco 1000 Series Integrated Services Routers (ISR1000):
- IR1821-K9
- IR1831-K9
- IR1833-K9
- IR1835-K9

Cisco Catalyst 1800 Rugged Series Routers (IR1800):
- C1131

Cisco Catalyst 8300 Rugged Series Routers (IR8300):
- IR8340-K9

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

Cisco Catalyst 9400 Series Switches (C9404R, C9407R, C9410R, C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y, C9400-LC-24S|48S|24XS|48P|48T|48U|48UX|48H)	
Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	13/11/2023
Revisión de Validez	30/04/2024
Descripción	

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

Observaciones

INFORMACIÓN IMPORTANTE

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

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

Descripción

La serie ATN 980C, 950D, 910C-G y 910D-A de Huawei son routers de acceso multiservicio que se han introducido en la transición a LTE y a la cobertura FMC de los operadores.
El objetivo de la serie ATN de Huawei es ofrecer soluciones de red de portadoras de IP de gama alta. Ofrece características ricas de segunda y tercera capa y cuenta con comodidades como el mantenimiento y la administración remotos, la ausencia de puesta en marcha in situ y la funcionalidad plug-and-play.
La serie ATN es compatible con el acceso virtual SDN y está pensada para satisfacer las necesidades de la capa de acceso, los dispositivos de despliegue a gran escala y el acceso a servicios integrados. Al ser un router de acceso multiservicio compacto de 2U de altura y 10GE, puede compartir un armario con la estación base, con una capacidad de conmutación de hasta 56G y soportar un acceso máximo de 8*10GE.

Observaciones

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

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

Versión	IOS-XE 17.9 (con fix 17.9.a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	14/11/2023
Revisión de Validez	30/04/2024

Descripción

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

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9200L Series Switches (C9200L-24P-4G|4X, C9200L-24T-4G|4X, C9200L-48P-4G|4X, C9200L-48T-4G|4X, C9200L-48PL-4G|4X, C9200L-24|48PXG-2Y y C9200L-24|48PXG-4X)	
Versión	IOS-XE 17.9 (con fix 17.9.a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	14/11/2023
Revisión de Validez	30/04/2024
Descripción	

Los equipos Cisco Catalyst 9200 y 9200L son switches de alto rendimiento y seguridad reforzada, ideales para empresas que requieren soluciones de red seguras y escalables. Con modelos que varían desde 24 hasta 48 puertos, proporciona una gran flexibilidad para adaptarse a cualquier tamaño de red. Ofrecen gestión avanzada y detección de amenazas mejorada.
Los Cisco Catalyst 9200L son la variante de la serie 9200, manteniendo las mismas características de seguridad y rendimiento. Son ideales para pequeñas y medianas empresas que buscan una red segura y escalable.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

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 España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	30/06/2024
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

ASR1000 (ASR1001-X, ASR1001-HX, ASR1002-HX, ASR1006-X, ASR1009-X, ASR1013, MACsec EPAs: ASR1000-MIP100, 18X1GE, 10X10GE, 1X100GE, CPAK-2X40GE, 1X100GE QSFP+, 2X40GE QSFP+, 1X40GE QSFP+)	
Versión	IOS-XE 17.3 (con fix 17.3.8a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2022
Revisión de Validez	31/12/2023
Descripción	

Los routers de Cisco permiten su despliege en redes WAN, LAN y la nube. Proporcionan una solución completa y probada a través de análisis avanzados, optimización de aplicaciones, aprovisionamiento automatizado y seguridad integrada.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Aggregation Services Router Cat8500 (C8500-12X4QC, C8500-12X)	
Versión	IOS-XE 17.3 (con fix 17.3.8a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2022
Revisión de Validez	31/12/2023
Descripción	

Los routers de Cisco permiten su despliege en redes WAN, LAN y la nube. Proporcionan una solución completa y probada a través de análisis avanzados, optimización de aplicaciones, aprovisionamiento automatizado y seguridad integrada.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Aggregation Services Router Cat8300 (C8300-1N1S-6T, C8300-1N1S-4T2X, C8300-2N2S-6T, C8300-2N2S-4T2X, NIMs: C-NIM-1X)	
Versión	IOS-XE 17.3 (con fix 17.3.8a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2022
Revisión de Validez	31/12/2023
Descripción	

Los routers de Cisco permiten su despliegue en redes WAN, LAN y la nube. Proporcionan una solución completa y probada a través de análisis avanzados, optimización de aplicaciones, aprovisionamiento automatizado y seguridad integrada.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ISR4000 (ISR4321, ISR4331, ISR4351, ISR4431, ISR4451-X, ISR4461, NIMs: NIM-1GE-CU-SFP, NIM-2GE-CU-SFP)	
Versión	IOS-XE 17.3 (con fix 17.3.8a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2022
Revisión de Validez	31/12/2023
Descripción	

Los routers de Cisco permiten su despliegue en redes WAN, LAN y la nube. Proporcionan una solución completa y probada a través de análisis avanzados, optimización de aplicaciones, aprovisionamiento automatizado y seguridad integrada.

Observaciones

N/A

INFORMACIÓN IMPORTANTE

Ruckus FastIron ICX8200 (ICX8200-C08PF, ICX8200-24, ICX8200-24P, ICX8200-48, ICX8200-48P, ICX8200-48PF y ICX8200-48PF2)	
Versión	10.0.00
Fabricante	CommScope Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/12/2023

Descripción

Nuestra familia RUCKUS ICX de conmutadores de nivel 2 y 3 está diseñada para simplificar la configuración y la gestión de la red, mejorar la seguridad, minimizar la resolución de problemas y facilitar las actualizaciones. Nuestra arquitectura de baja latencia sin bloqueo garantiza una capacidad y un rendimiento excelentes para las aplicaciones más exigentes.

La familia de conmutadores RUCKUS ICX dispone de una gama completa de modelos tanto para campus y redes empresariales de 2 y 3 niveles (acceso, agregación y Core) como para Data Center, con tecnologías avanzadas como Stacking a corta y larga distancia, PoE+ y PoE++, MultiGigabit, todo el rango de velocidades de puerto desde 1G hasta 100G, fuentes de alimentación modulares y reemplazables en caliente, nivel 2 y nivel 3 avanzado, MultiChassis Trunking, automatización, etc.

Tanto en el despliegue de un simple conmutador como de una gran red empresarial o un Data Center, obtendrá los beneficios del rendimiento, la flexibilidad y la protección de la inversión de CommScope.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

ACX5448-M

Versión	Junos OS 20.3R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	31/12/2024

Descripción

La línea Juniper Networks® ACX5000 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. La línea ACX5000 simplifica las arquitecturas de acceso y agregación al eliminar capas innecesarias y superposiciones de red, lo que reduce drásticamente CapEx y OpEx. Está basada en la simplificación de la arquitectura y en la reducción de costos, la línea ACX5000 brinda a los proveedores de servicios y empresas la capacidad de adoptar un verdadero paradigma de 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-M: El ACX5448-M tiene 44 puertos 1GbE/10GbE y 6 puertos 40GbE/100GbE, así como capacidades de seguridad avanzadas como such as Media Access Control Security (MACsec) on all 1GbE/10GbE ports.

Observaciones

CCN-STIC-1445 PES Router_Juniper_ACX5448-M_JunOS 20.3R1

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

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2024

Descripción

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

Observaciones

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

INFORMACIÓN IMPORTANTE

Cisco Nexus 3500 Series Switches (3524-X/XL, 3548-X/XL)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2024
Descripción	

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

Observaciones

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

Cisco Nexus 3200 Series Switches (3232C, 3264C-E)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2024
Descripción	

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

Observaciones

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

Cisco Nexus 3600 Series Switches (36180YC-R, 3636C-R)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2024
Descripción	

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

Observaciones

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

INFORMACIÓN IMPORTANTE

NE40E 8000 Series Routers running VRP software	
Versión	V800R012C00SPC300
Fabricante	Huawei Technologies España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	31/12/2024

Descripción

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

Observaciones

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

Cisco Catalyst 9300 Series Switches (C9300-24T|P|U|AUX|S|H, C9300-48T|P|U|UXM|UN|S|H, C9300D-24UB|UXB, C9300D-48UB) con los siguientes módulos de red (C9300-NM-4G|8X|2Q|4M|2Y)	
Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/11/2023
Revisión de Validez	30/04/2024

Descripción

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

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

RouterTeldat-M1 Series	
Versión	11.01.09
Fabricante	TELDAT, S.A.
Familia	Enrutadores
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2023
Revisión de Validez	31/10/2025

Descripción

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

Observaciones

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

INFORMACIÓN IMPORTANTE

Ruckus FastIron ICX7250 (24G y 48P)	
Versión	09.0.10
Fabricante	CommScope Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/12/2023

Descripción

Nuestra familia RUCKUS ICX de conmutadores de nivel 2 y 3 está diseñada para simplificar la configuración y la gestión de la red, mejorar la seguridad, minimizar la resolución de problemas y facilitar las actualizaciones. Nuestra arquitectura de baja latencia sin bloqueo garantiza una capacidad y un rendimiento excelentes para las aplicaciones más exigentes.

La familia de conmutadores RUCKUS ICX dispone de una gama completa de modelos tanto para campus y redes empresariales de 2 y 3 niveles (acceso, agregación y Core) como para Data Center, con tecnologías avanzadas como Stacking a corta y larga distancia, PoE+ y PoE++, MultiGigabit, todo el rango de velocidades de puerto desde 1G hasta 100G, fuentes de alimentación modulares y reemplazables en caliente, nivel 2 y nivel 3 avanzado, MultiChassis Trunking, automatización, etc.

Tanto en el despliegue de un simple conmutador como de una gran red empresarial o un Data Center, obtendrá los beneficios del rendimiento, la flexibilidad y la protección de la inversión de CommScope.

Observaciones

Procedimiento de empleo pendiente de publicación

Cisco ASR9000 Series y NCS4200 Series (ASR902, ASR903, ASR907, ASR920 y NCS4201, NCS4202, NCS4206, NCS4216)	
Versión	IOS-XE 16.9
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	30/04/2025

Descripción

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

Observaciones

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

INFORMACIÓN IMPORTANTE

Ruckus FastIron ICX7150 (C12P-2X10GR-A, 24-4X10GR-A, 24P-4X10GR-A, 48-4X10GR-A, 48P-4X10GR-A , 48PF-4X10GR-A y 48ZP-8X10GR2-A)	
Versión	09.0.10
Fabricante	CommScope Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/12/2023

Descripción

Nuestra familia RUCKUS ICX de conmutadores de nivel 2 y 3 está diseñada para simplificar la configuración y la gestión de la red, mejorar la seguridad, minimizar la resolución de problemas y facilitar las actualizaciones. Nuestra arquitectura de baja latencia sin bloqueo garantiza una capacidad y un rendimiento excelentes para las aplicaciones más exigentes.

La familia de conmutadores RUCKUS ICX dispone de una gama completa de modelos tanto para campus y redes empresariales de 2 y 3 niveles (acceso, agregación y Core) como para Data Center, con tecnologías avanzadas como Stacking a corta y larga distancia, PoE+ y PoE++, MultiGigabit, todo el rango de velocidades de puerto desde 1G hasta 100G, fuentes de alimentación modulares y reemplazables en caliente, nivel 2 y nivel 3 avanzado, MultiChassis Trunking, automatización, etc.

Tanto en el despliegue de un simple conmutador como de una gran red empresarial o un Data Center, obtendrá los beneficios del rendimiento, la flexibilidad y la protección de la inversión de CommScope.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

Ruckus FastIron ICX7450 (24P, 48P y 48F)

Versión	09.0.10
Fabricante	CommScope Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/12/2023

Descripción

Nuestra familia RUCKUS ICX de conmutadores de nivel 2 y 3 está diseñada para simplificar la configuración y la gestión de la red, mejorar la seguridad, minimizar la resolución de problemas y facilitar las actualizaciones. Nuestra arquitectura de baja latencia sin bloqueo garantiza una capacidad y un rendimiento excelentes para las aplicaciones más exigentes.

La familia de conmutadores RUCKUS ICX dispone de una gama completa de modelos tanto para campus y redes empresariales de 2 y 3 niveles (acceso, agregación y Core) como para Data Center, con tecnologías avanzadas como Stacking a corta y larga distancia, PoE+ y PoE++, MultiGigabit, todo el rango de velocidades de puerto desde 1G hasta 100G, fuentes de alimentación modulares y reemplazables en caliente, nivel 2 y nivel 3 avanzado, MultiChassis Trunking, automatización, etc.

Tanto en el despliegue de un simple conmutador como de una gran red empresarial o un Data Center, obtendrá los beneficios del rendimiento, la flexibilidad y la protección de la inversión de CommScope.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

Ruckus FastIron ICX Series Switch/Router with MACsec (ICX 7550|7650 SKUS with ICX7600-4X10GF Module, ICX 7650-48F y ICX 7850-48FS)	
Versión	09.0.10
Fabricante	CommScope Technologies
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/12/2023
Descripción	

Nuestra familia RUCKUS ICX de conmutadores de nivel 2 y 3 está diseñada para simplificar la configuración y la gestión de la red, mejorar la seguridad, minimizar la resolución de problemas y facilitar las actualizaciones. Nuestra arquitectura de baja latencia sin bloqueo garantiza una capacidad y un rendimiento excelentes para las aplicaciones más exigentes.

La familia de conmutadores RUCKUS ICX dispone de una gama completa de modelos tanto para campus y redes empresariales de 2 y 3 niveles (acceso, agregación y Core) como para Data Center, con tecnologías avanzadas como Stacking a corta y larga distancia, PoE+ y PoE++, MultiGigabit, todo el rango de velocidades de puerto desde 1G hasta 100G, fuentes de alimentación modulares y reemplazables en caliente, nivel 2 y nivel 3 avanzado, MultiChassis Trunking, automatización, etc.

Tanto en el despliegue de un simple conmutador como de una gran red empresarial o un Data Center, obtendrá los beneficios del rendimiento, la flexibilidad y la protección de la inversión de CommScope.

Observaciones

Procedimiento de empleo pendiente de publicación

Cisco Nexus 9500 Series Switches (9504, 9508, 9516, Supervisor 9500-Sup-A , Supervisor 9500-Sup-A +, Supervisor 9500-Sup-B , Supervisor 9500-Sup-B, System Controller N9k-SC-A)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	04/10/2025
Descripción	

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

Observaciones

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

INFORMACIÓN IMPORTANTE

- Cisco Nexus 9200 Series Switches (92348GC-X, 92160YC-X, 92300YC, 9272Q)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	10/04/2025
Descripción	
Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.	
Observaciones	
CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9	

Cisco Nexus 9300 Series Switches (93108TC-EX, 93108TC-FX, 9348GC-FXP, 93216TC-FX2, 93180LC-EX, 93180YC-EX, 93180YC-FX, 93240YC-FX2, 93360YC-FX2, 9364C, 9332C, 9336C-FX2, 9364C-GX, 9316D-GX, 93600CD-GX	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	04/10/2025
Descripción	
Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.	
Observaciones	
CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9	

INFORMACIÓN IMPORTANTE

Dell EMC Networking SmartFabric OS10.5.4en Switches de las series N, S y Z (N3248TE, S41xx, S52xx, S54xx, Z91xx, Z92xx, Z93xx, Z94xx, Z96xx)	
Versión	OS10.5.4
Fabricante	DELL COMPUTER, S.A.
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/03/2024

Descripción

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

Observaciones

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Dell EMC Networking SmartFabric (Modelos: S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, MX5108n, S4248FB-ON, S4248FBL-ON, S6010-ON, Z9100-ON, MX9116n, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9264F-ON y Z9332F-ON)	
Versión	OS 10 Build: 10.5.1.3.
Fabricante	Dell Computer
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	31/08/2024

Descripción

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

Observaciones

CCN-STIC-1429 PES DELL EMC Networking

INFORMACIÓN IMPORTANTE

MX10003	
Versión	Junos OS 22.2R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
Descripción	

Las plataformas de enrutamiento universal MX10000 brindan un rendimiento de gran escalabilidad y un factor de forma optimizado para la nube y las economías de coste por puerto o bit más exigentes. Se pueden utilizar tanto en redes de tipo operador como nodo de borde PE en una red MPLS, como en entornos de movilidad convergente, IoT, empresarial y también en arquitecturas de Core convergente y de borde multiservicio. También soporta el uso como enrutador de conmutación de etiquetas (LSR), provider Edge, equipo de intercambio de Internet y red troncal para implementaciones en redes de carácter metropolitanas, regionales o nacionales. La serie MX admite un amplio conjunto de funcionalidades IPoDWDM, L2, L3, IP/MPLS, SR, SRv6 para permitir redes de transporte a gran escala con operaciones y aprovisionamiento de servicios simplificados, manteniendo simplicidad en la red. Gracias al tipo de chipsets implementados, tienen una capacidad de programación de plano de datos casi infinita, lo que le brinda la libertad de implementar nuevas innovaciones de red.
Con tecnología de silicio TRIO, la familia MX10000 es altamente escalable desde los 2.4Tbps en 3U, pasando por 38,4 Tbps en 7 slots y hasta un rendimiento de 76,8 Tbps en 13 slots.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

Huawei S Series Ethernet Switches S5732 (H24S6Q, H24UM2CC, H48S6Q, H48UM2CC, H48XUM2CC, H24S6Q-K, H24UM2C-K, H48S6Q-K, H48UM2C-K)	
Versión	V200R022C00SPC500
Fabricante	Huawei Technologies España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
Descripción	

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

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

Huawei S Series Ethernet Switches S5735 (L12P4S-A, L12T4S-A, L24P4S-A, L24P4S-A1, L24P4X-A, L24P4X-A1, L24T4S-A, L24T4S-A1, L24T4S-QA1, L24T4X-A, L24T4X-A1, L24T4X-QA1, L32ST4X-A, L32ST4X-A1, L48P4S-A1, L48P4X-A, L48P4X-A1, L48T4S-A, L48T4S-A1, L48T4X-A, L48T4X-A1, L8P4S-A1, L8P4S-QA1, L8P4X-A1, L8T4S-A1, L8T4S-QA1, L8T4X-A1, S24P4X, S24T4X, S24T4X-I, S32ST4X, S48P4X, S48S4X, S48T4X, L24T4X-D,L24T4X-D1, L24T4X-IA1, L32ST4X-D, L32ST4X-D1, L8P4X-IA1, L8T4X-IA1)	
Versión	V200R022C00SPC500
Fabricante	Huawei Technologies España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	N/A
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
Descripción	
Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.	
Observaciones	
Procedimiento de empleo seguro pendiente de publicación	

Huawei S Series Ethernet Switches S5736 (S24UM4XC, S48S4X-A, S24S4XC, S24T4XC, S24U4XC, S48S4XC, S48S4X-D, S48T4XC, S48U4XC)	
Versión	V200R022C00SPC500
Fabricante	Huawei Technologies España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	N/A
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
Descripción	
Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.	
Observaciones	
Procedimiento de empleo seguro pendiente de publicación	

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 España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
Descripción	

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

Observaciones

Procedimiento de empleo seguro pendiente de publicación

Huawei S Series Ethernet Switches S6735 (S6735-S24X6C y S6735-S48X6C)	
Versión	V200R022C00SPC500
Fabricante	Huawei Technologies España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
Descripción	

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

Observaciones

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 España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	N/A
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024

Descripción

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

Observaciones

Procedimiento de empleo seguro pendiente de publicación

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

Versión	V200R022C00SPC500
Fabricante	Huawei Technologies España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024

Descripción

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

Observaciones

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Huawei CloudEngine 16800 (CE16804, CE16808 y CE16816), Huawei CloudEngine 12800 (CE12804, CE12808 y CE12816), Huawei CloudEngine 8800 (CE8861-4C-EI y CE8850-64CQ-EI), Huawei CloudEngine 6800 (CE6863-48S6CQ, CE6881-48S6CQ, CE6820-48S6CQ, CE6863E-48S6CQ, CE6870-48S6CQ-EI, CE6870-48S6CQ-EI-A), CE5882-48T4S, CE9860-4C-EI Y CE9860-4C-EI-A	
Versión	V200R022C00SPC500
Fabricante	Huawei Technologies España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
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

Procedimiento de empleo seguro pendiente de publicación

Aruba 6200F, 6300M, 6300F, 6405, 6410, 8320, 8325, 8360, and 8400	
Versión	Aruba OS-CX version 10.06
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	29/02/2024
Descripción	

La familia Aruba CX implementan soluciones de switching y routing para redes de sucursales, campus y datacenter. Los equipos 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.

Observaciones

CCN-STIC-1432 Procedimiento de empleo seguro ARUBA OS-CX

INFORMACIÓN IMPORTANTE

SLX Product Series (SLX 9740 y SLX 9540)	
Versión	20.2.1
Fabricante	Extreme Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	29/02/2024

Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack. El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados

Observaciones

CCN-STIC-1430 PES Switches Extreme Networks SLXOS

INFORMACIÓN IMPORTANTE

7.5.2 SWITCHES

Cisco Catalyst 9300L Series Switches (C9300L-24T|P-4G, C9300L-48T|P|PF-4G, C9300L-24T|P|UXG-4X, C9300L-48T|P|PF|UXG-4X, C9300L-24UXG-2Q, C9300L-48UXG-2Q)	
Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	14/11/2023
Revisión de Validez	30/04/2024
Descripción	

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

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Aruba Switch 2930F, 2930M, 3810M y 5400R	
Versión	ArubaOS 16.08
Fabricante	Aruba
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024
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-647C Seguridad en conmutadores HPE Aruba

INFORMACIÓN IMPORTANTE

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

Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	13/11/2023
Revisión de Validez	30/04/2024

Descripción

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

Observaciones

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

Versión	OS 20.2R1-S1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2022
Revisión de Validez	31/12/2024

Descripción

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

Estos switches para centros de datos son dispositivos de red que soportan la definición, y cumplimiento, de políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión segura.
Como switch de nivel 2 en la capa OSI, realiza el análisis de paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario.
Como switch de nivel 3 en la capa OSI, admite el enrutamiento del tráfico, basado en tablas, identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar el camino más adecuado para cada paquete.

Observaciones

CCN-STIC-1440 Juniper QFX-EX JunOS 20.2

INFORMACIÓN IMPORTANTE

Virtual Services Platform (VSP) Series Switches (VSP4900, VSP7400, VSP8400 y XA-1400)	
Versión	8.3
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/09/2025
Descripción	

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

Observaciones

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

Cisco Catalyst 9500 Series Switches (C9500-12Q|24Q|40X|16X|32C|32QC|24Y4C|48Y4C) con los siguientes módulos de red (C9500-NM-8X y C9500-NM-2Q)	
Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	13/11/2023
Revisión de Validez	30/04/2024
Descripción	

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

Observaciones

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9400 Series Switches (C9404R, C9407R, C9410R, C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y, C9400-LC-24S|48S|24XS|48P|48T|48U|48UX|48H)	
Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	13/11/2023
Revisión de Validez	30/04/2024
Descripción	

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

Observaciones

Cisco Catalyst 9200 Series Switches (C9200-24T, C9200-48T, C9200-24P, C9200-48P, C9200-24PB, C9200-48PB, C9200-48PL, C9200-24PXG, C9200-48PXG) con los módulos de red (C9200-NM-4G|4X|2Y|2Q)	
Versión	IOS-XE 17.9 (con fix 17.9.a)
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	14/11/2023
Revisión de Validez	30/04/2024
Descripción	

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

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9200L Series Switches (C9200L-24P-4G|4X, C9200L-24T-4G|4X, C9200L-48P-4G|4X, C9200L-48T-4G|4X, C9200L-48PL-4G|4X, C9200L-24|48PXG-2Y y C9200L-24|48PXG-4X)	
Versión	IOS-XE 17.9 (con fix 17.9.a)
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	14/11/2023
Revisión de Validez	30/04/2024
Descripción	

Los equipos Cisco Catalyst 9200 y 9200L son switches de alto rendimiento y seguridad reforzada, ideales para empresas que requieren soluciones de red seguras y escalables. Con modelos que varían desde 24 hasta 48 puertos, proporciona una gran flexibilidad para adaptarse a cualquier tamaño de red. Ofrecen gestión avanzada y detección de amenazas mejorada.
Los Cisco Catalyst 9200L son la variante de la serie 9200, manteniendo las mismas características de seguridad y rendimiento. Son ideales para pequeñas y medianas empresas que buscan una red segura y escalable.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Switches EXOS: x440-G2, x460-G2, x465, x435, x695, 5520, 5420	
Versión	EXOS 31.3.100
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	31/05/2025
Descripción	

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

Observaciones

CCN-STIC-1446 PES Switches EXoS

INFORMACIÓN IMPORTANTE

Alcatel-Lucent Enterprise OmniSwitch Serie 6360 (OS6360-10, OS6360-P10, OS6360-24, OS6360-P24, OS6360-PH24, OS6360-P24X, OS6360-48, OS6360-P48, OS6360-P48X, OS6360-PH48)	
Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2022
Revisión de Validez	28/02/2026
Descripción	

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches	
Versión	IOS-XE 17.3 (con fix 17.3.8a)
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	31/03/2025
Descripción	

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

Observaciones

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

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9200 Series Switches (C9200-24T, C9200-48T, C9200-24P, C9200-48P, C9200-24PB, C9200-48PB, C9200-48PL, C9200-24PXG, C9200-48PXG) con los módulos de red (C9200-NM-4G,C9200-NM-4X,C9200-NM)	
Versión	IOS-XE 17.6.6a
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/06/2025
Descripción	
Cisco Catalyst 9200 Series Switches	
Observaciones	
CCN-STIC-1450 Procedimiento de empleo Seguro de Catalyst 9000 y Catalyst IE3000. La versión inicial cualificada fue la 17.6 pero tras la publicación de la vulnerabilidad pública [CVE-2023-20198], CISCO ha publicado una nueva versión con el fix (17.6.6a).	

Cisco Catalyst 9200L Series Switches (C9200L-24P-4G|4X, C9200L-24T-4G|4X, C9200L-48P-4G|4X, C9200L-48T-4G|4X, C9200L-48PL-4G|4X, C9200L-24|48PXG-2Yy C9200L-24|48PXG-4X)	
Versión	IOS-XE 17.6.6a
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/06/2025
Descripción	
Series Cisco Catalyst 9200L.	
Observaciones	
CCN-STIC-1450 Procedimiento de empleo Seguro de Catalyst 9000 y Catalyst IE3000 La versión inicial cualificada fue la 17.6 pero tras la publicación de la vulnerabilidad pública [CVE-2023-20198], CISCO ha publicado una nueva versión con el fix (17.6.6a).	

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9300 Series Switches (C9300-24T|P|U|UX|S|UB|UXB|H y C9300-48T|P|U|UXM|UN|S|UB|H) con los siguientes módulos de red (C9300-NM-4G, C9300-NM-8X, C9300-NM-2Q, C9300-NM-4M, C9300-NM-2Y)	
Versión	IOS-XE 17.6.6a
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/06/2025
Descripción	
Cisco Catalyst 9300 Series Switches	
Observaciones	
CCN-STIC-1450 Procedimiento de empleo Seguro de Catalyst 9000 y Catalyst IE3000. La versión inicial cualificada fue la 17.6 pero tras la publicación de la vulnerabilidad pública [CVE-2023-20198], CISCO ha publicado una nueva versión con el fix (17.6.6a).	

Cisco Catalyst 9500 Series Switches (C9500-12Q C9500-24Q, C9500-40X, C9500-16X, C9500-32C, C9500-32QC, C9500-24Y4C, C9500-48Y4C) con los siguientes módulos de red (C9500-NM-8X y C9500-NM-2Q)	
Versión	IOS-XE 17.6.6a
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/06/2025
Descripción	
Cisco Catalyst 9500 Series Switches	
Observaciones	
CCN-STIC-1450 Procedimiento de empleo Seguro de Catalyst 9000 y Catalyst IE3000. La versión inicial cualificada fue la 17.6 pero tras la publicación de la vulnerabilidad pública [CVE-2023-20198], CISCO ha publicado una nueva versión con el fix (17.6.6a).	

INFORMACIÓN IMPORTANTE

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

Versión	IOS-XE 17.6.6a
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/12/2025

Descripción

Cisco Catalyst 9300L Series Switches

Observaciones

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

Ruckus FastIron ICX8200 (ICX8200-C08PF, ICX8200-24, ICX8200-24P, ICX8200-48, ICX8200-48P, ICX8200-48PF y ICX8200-48PF2)

Versión	10.0.00
Fabricante	CommScope Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/12/2023

Descripción

Nuestra familia RUCKUS ICX de conmutadores de nivel 2 y 3 está diseñada para simplificar la configuración y la gestión de la red, mejorar la seguridad, minimizar la resolución de problemas y facilitar las actualizaciones. Nuestra arquitectura de baja latencia sin bloqueo garantiza una capacidad y un rendimiento excelentes para las aplicaciones más exigentes.

La familia de conmutadores RUCKUS ICX dispone de una gama completa de modelos tanto para campus y redes empresariales de 2 y 3 niveles (acceso, agregación y Core) como para Data Center, con tecnologías avanzadas como Stacking a corta y larga distancia, PoE+ y PoE++, MultiGigabit, todo el rango de velocidades de puerto desde 1G hasta 100G, fuentes de alimentación modulares y reemplazables en caliente, nivel 2 y nivel 3 avanzado, MultiChassis Trunking, automatización, etc.

Tanto en el despliegue de un simple conmutador como de una gran red empresarial o un Data Center, obtendrá los beneficios del rendimiento, la flexibilidad y la protección de la inversión de CommScope.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9400 Series Switches (C9404R, C9407R, C9410R, C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y, C9400-LC-24S|48S|24XS|48P|48T|48U|48UX|48H)	
Versión	IOS-XE 17.6.6a
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/12/2025
Descripción	

Cisco Catalyst 9400 Series Switches

Observaciones

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

Cisco Catalyst 9600 Series Switches (C9606R, C9600-SUP-1 y C9600-LC-24C|48YL|48TX|24S)	
Versión	IOS-XE 17.6.6a
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/06/2025
Descripción	

Cisco Catalyst 9600 Series Switches

Observaciones

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

INFORMACIÓN IMPORTANTE

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

Versión	H3C Comware Software 7.1.070
Fabricante	New H3C Technologies Co., Ltd
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/04/2024

Descripción

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

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

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Huawei Cloud Engine 6800 (6881-48T6CQ)

Versión	V200R020C00SPC600 Patch V200R020SPH100T
Fabricante	Huawei Technologies España
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2024

Descripción

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

Observaciones

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

INFORMACIÓN IMPORTANTE

Cisco Nexus 3400 Series Switches (34180-YC, 3464C, 3432D-S, 3408-S)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2024
Descripción	

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

Observaciones

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

Cisco Nexus 3500 Series Switches (3524-X/XL, 3548-X/XL)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2024
Descripción	

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

Observaciones

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

Cisco Nexus 3200 Series Switches (3232C, 3264C-E)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2024
Descripción	

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

Observaciones

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

INFORMACIÓN IMPORTANTE

Cisco Nexus 3600 Series Switches (36180YC-R, 3636C-R)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2024
Descripción	

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

Observaciones

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

Cisco Catalyst 9300 Series Switches (C9300-24T|P|U|AUX|S|H, C9300-48T|P|U|UXM|UN|S|H, C9300D-24UB|UXB, C9300D-48UB) con los siguientes módulos de red (C9300-NM-4G|8X|2Q|4M|2Y)	
Versión	IOS-XE 17.9 (con fix 17.9.4a)
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	10/11/2023
Revisión de Validez	30/04/2024
Descripción	

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

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Nokia 1830 Photonic Service Switch (PSS)	
Versión	9.1
Fabricante	NOKIA
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2022
Revisión de Validez	31/08/2024

Descripción

El conmutador de servicio fotónico Nokia 1830PSS es una plataforma que ofrece conectividad multiservicio de multiplexación óptica por división de longitud de onda densa de gran capacidad. Incluye cifrado, baja latencia y detección de intrusiones ópticas, lo que garantiza la confidencialidad e integridad de los datos, así como el soporte de comunicaciones.
La familia 1830PSS consta de diferentes plataformas que se han optimizado para su aplicabilidad en diversos entornos de despliegue de redes ópticas, desde la interconexión de CPD hasta el escalado de grandes redes ópticas multiservicio, multicapa, regionales y de larga distancia. Estos equipos aprovechan el software, el hardware, la gestión y el control comunes, para ofrecer operaciones fluidas en toda la cartera de posibilidades que ofrece la familia 1830PSS.
Son compatibles con múltiples aplicaciones de red de transporte, que incluyen: transporte y agregación metro multiservicio, implementaciones de larga distancia/núcleo óptico, configuraciones de conmutación fotónica con enrutamiento colorless, directionless y contentionless con Flexgrid, agregación/conmutación en capa L1, medidas reflextométricas OTDR de las fibras ópticas, y otros mecanismos de protección.

Observaciones

CCN-STIC-1463 Procedimiento de empleo seguro Nokia 1830 Photon Service Switch (PSS) v.9.1

INFORMACIÓN IMPORTANTE

RouterTeldat-M1 Series	
Versión	11.01.09
Fabricante	TELDAT, S.A.
Familia	Switches
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2023
Revisión de Validez	31/10/2025

Descripción

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

Observaciones

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

INFORMACIÓN IMPORTANTE

Ruckus FastIron ICX7250 (24G y 48P)

Versión	09.0.10
Fabricante	CommScope Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/12/2023

Descripción

Nuestra familia RUCKUS ICX de conmutadores de nivel 2 y 3 está diseñada para simplificar la configuración y la gestión de la red, mejorar la seguridad, minimizar la resolución de problemas y facilitar las actualizaciones. Nuestra arquitectura de baja latencia sin bloqueo garantiza una capacidad y un rendimiento excelentes para las aplicaciones más exigentes.

La familia de conmutadores RUCKUS ICX dispone de una gama completa de modelos tanto para campus y redes empresariales de 2 y 3 niveles (acceso, agregación y Core) como para Data Center, con tecnologías avanzadas como Stacking a corta y larga distancia, PoE+ y PoE++, MultiGigabit, todo el rango de velocidades de puerto desde 1G hasta 100G, fuentes de alimentación modulares y reemplazables en caliente, nivel 2 y nivel 3 avanzado, MultiChassis Trunking, automatización, etc.

Tanto en el despliegue de un simple conmutador como de una gran red empresarial o un Data Center, obtendrá los beneficios del rendimiento, la flexibilidad y la protección de la inversión de CommScope.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

Ruckus FastIron ICX7150 (C12P-2X10GR-A, 24-4X10GR-A, 24P-4X10GR-A, 48-4X10GR-A, 48P-4X10GR-A , 48PF-4X10GR-A y 48ZP-8X10GR2-A)	
Versión	09.0.10
Fabricante	CommScope Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/12/2023

Descripción

Nuestra familia RUCKUS ICX de conmutadores de nivel 2 y 3 está diseñada para simplificar la configuración y la gestión de la red, mejorar la seguridad, minimizar la resolución de problemas y facilitar las actualizaciones. Nuestra arquitectura de baja latencia sin bloqueo garantiza una capacidad y un rendimiento excelentes para las aplicaciones más exigentes.

La familia de conmutadores RUCKUS ICX dispone de una gama completa de modelos tanto para campus y redes empresariales de 2 y 3 niveles (acceso, agregación y Core) como para Data Center, con tecnologías avanzadas como Stacking a corta y larga distancia, PoE+ y PoE++, MultiGigabit, todo el rango de velocidades de puerto desde 1G hasta 100G, fuentes de alimentación modulares y reemplazables en caliente, nivel 2 y nivel 3 avanzado, MultiChassis Trunking, automatización, etc.

Tanto en el despliegue de un simple conmutador como de una gran red empresarial o un Data Center, obtendrá los beneficios del rendimiento, la flexibilidad y la protección de la inversión de CommScope.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

Ruckus FastIron ICX7450 (24P, 48P y 48F)

Versión	09.0.10
Fabricante	CommScope Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/12/2023

Descripción

Nuestra familia RUCKUS ICX de conmutadores de nivel 2 y 3 está diseñada para simplificar la configuración y la gestión de la red, mejorar la seguridad, minimizar la resolución de problemas y facilitar las actualizaciones. Nuestra arquitectura de baja latencia sin bloqueo garantiza una capacidad y un rendimiento excelentes para las aplicaciones más exigentes.

La familia de conmutadores RUCKUS ICX dispone de una gama completa de modelos tanto para campus y redes empresariales de 2 y 3 niveles (acceso, agregación y Core) como para Data Center, con tecnologías avanzadas como Stacking a corta y larga distancia, PoE+ y PoE++, MultiGigabit, todo el rango de velocidades de puerto desde 1G hasta 100G, fuentes de alimentación modulares y reemplazables en caliente, nivel 2 y nivel 3 avanzado, MultiChassis Trunking, automatización, etc.

Tanto en el despliegue de un simple conmutador como de una gran red empresarial o un Data Center, obtendrá los beneficios del rendimiento, la flexibilidad y la protección de la inversión de CommScope.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

Ruckus FastIron ICX Series Switch/Router with MACsec (ICX 7550|7650 SKUS with ICX7600-4X10GF Module, ICX 7650-48F y ICX 7850-48FS)	
Versión	09.0.10
Fabricante	CommScope Technologies
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/12/2023
Descripción	

Nuestra familia RUCKUS ICX de conmutadores de nivel 2 y 3 está diseñada para simplificar la configuración y la gestión de la red, mejorar la seguridad, minimizar la resolución de problemas y facilitar las actualizaciones. Nuestra arquitectura de baja latencia sin bloqueo garantiza una capacidad y un rendimiento excelentes para las aplicaciones más exigentes.

La familia de conmutadores RUCKUS ICX dispone de una gama completa de modelos tanto para campus y redes empresariales de 2 y 3 niveles (acceso, agregación y Core) como para Data Center, con tecnologías avanzadas como Stacking a corta y larga distancia, PoE+ y PoE++, MultiGigabit, todo el rango de velocidades de puerto desde 1G hasta 100G, fuentes de alimentación modulares y reemplazables en caliente, nivel 2 y nivel 3 avanzado, MultiChassis Trunking, automatización, etc.

Tanto en el despliegue de un simple conmutador como de una gran red empresarial o un Data Center, obtendrá los beneficios del rendimiento, la flexibilidad y la protección de la inversión de CommScope.

Observaciones

Procedimiento de empleo pendiente de publicación

Series AlliedWare Plus x550 (X550-18XTQ, X550-18XSQ, X550-18XSPQm) y x530-x530L (X530-28GPXm, X530-28GPXm, X530-52GTXm, X530-52GPXm, X530L-28GTX, X530L-28GPX, X530L-52GTX, X530L-52GPX)	
Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2019
Revisión de Validez	31/12/2023
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+) versión 5.5.0-0.6

INFORMACIÓN IMPORTANTE

EX4300-48MP

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

Descripción

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

Los switches EX4300 son dispositivos de red que soportan la definición, y cumplimiento, de políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión segura.
Como switch de nivel 2 en la capa OSI, realiza el análisis de paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario.
Como switch de nivel 3 en la capa OSI, admite el enrutamiento del tráfico, basado en tablas, identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar el camino más adecuado para cada paquete.

Observaciones

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

INFORMACIÓN IMPORTANTE

Huawei CE Series Switches (CE6820H-48S6CQ , CE6860-HAM, CE6860-SAN, CE6863H-48S6CQ, CE6866-48S8CQ-P, CE6881H-48S6CQ, CE6881H-48T6CQ, CE8850-HAM, CE8850-SAN, CE8851-32CQ8DQ-P y CE16804)	
Versión	V300R022C00SPC200
Fabricante	Huawei Technologies Co., Ltd.
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/03/2024
Descripción	

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

Observaciones

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

Cisco Nexus 9500 Series Switches (9504, 9508, 9516, Supervisor 9500-Sup-A , Supervisor 9500-Sup-A +, Supervisor 9500-Sup-B , Supervisor 9500-Sup-B, System Controller N9k-SC-A)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	04/10/2025
Descripción	

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

Observaciones

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

INFORMACIÓN IMPORTANTE

- Cisco Nexus 9200 Series Switches (92348GC-X, 92160YC-X, 92300YC, 9272Q)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	10/04/2025
Descripción	

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

Observaciones

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

Cisco Nexus 9300 Series Switches (93108TC-EX, 93108TC-FX, 9348GC-FXP, 93216TC-FX2, 93180LC-EX, 93180YC-EX, 93180YC-FX, 93240YC-FX2, 93360YC-FX2, 9364C, 9332C, 9336C-FX2, 9364C-GX, 9316D-GX, 93600CD-GX	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	04/10/2025
Descripción	

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

Observaciones

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

INFORMACIÓN IMPORTANTE

Dell EMC Networking SmartFabric OS10.5.4en Switches de las series N, S y Z (N3248TE, S41xx, S52xx, S54xx, Z91xx, Z92xx, Z93xx, Z94xx, Z96xx)	
Versión	OS10.5.4
Fabricante	DELL COMPUTER, S.A.
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/03/2024

Descripción

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

Observaciones

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Dell EMC Networking SmartFabric (Modelos: S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, MX5108n, S4248FB-ON, S4248FBL-ON, S6010-ON, Z9100-ON, MX9116n, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9264F-ON y Z9332F-ON)	
Versión	OS 10 Build: 10.5.1.3.
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	31/08/2024

Descripción

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

Observaciones

CCN-STIC-1429 PES DELL EMC Networking

INFORMACIÓN IMPORTANTE

Huawei S Series Switches (S3710, S5732, S5735I, S5735, S6730, S16700-4, S16700-8, S8700-10, S8700-4 y S8700-6)	
Versión	V600R022C10SPC500
Fabricante	Huawei Technologies Co., Ltd.
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/03/2024

Descripción

Los modelos cualificados son: S3710-H24P4S-A, S3710-H24T4S-A, S3710-H48LP4S-A,S3710-H48T4S-A, S5732-H24S4X6QZ-TV2, S5732-H24S4X6QZ-V2, S5732-H24UM4Y2CZ-TV2, S5732-H24UM4Y2CZ-V2, S5732-H44S4X6QZ-TV2, S5732-H44S4X6QZ-V2, S5732-H48UM4Y2CZ-TV2, S5732-H48UM4Y2CZ-V2, S5735I-L10T4X-A-V2, S5735I-L10T4X-A-V2, S5735I-L8P4X-A-V2, S5735I-S24T4XE-V2, S5735I-S24U4XE-V2, S5735I-S8T4SN-V2, S5735I-S8T4XN-V2, S5735I-S8U4XN-V2, S5735-L10T4X-A-V2, S5735-L16T4S-A-V2, S5735-L16T4X-QA-V2, S5735-L24P4S-A-V2, S5735-L24P4XE-A-V2, S5735-L24T4S-A-V2, S5735-L24T4XE-A-V2, S5735-L24T4XE-D-V2, S5735-L24T4X-QA-V2, S5735-L48LP4S-A-V2, S5735-L48LP4XE-A-V2, S5735-L48P4XE-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, S5735-S24P4XE-V2, S5735-S24T4XE-V2, S5735-S24U4XE-V2, S5735-S48P4XE-V2, S5735-S48T4XE-V2, S5735-S48U4XE-V2, S6730-H24X6C-TV2, S6730-H24X6C-V2, S6730-H28X6CZ-TV2, S6730-H28X6CZ-V2, S6730-H48X6C-TV2, S6730-H48X6C-V2, S6730-H48X6CZ-TV2, S6730-H48X6CZ-V2, S6730-H48Y6C-TV2, S6730-H48Y6C-V2, S16700-4, S16700-8, S8700-10, S8700-4 y S8700-6.

Observaciones

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

INFORMACIÓN IMPORTANTE

Alcatel-Lucent Enterprise OmniSwitch Serie 6900 (OS6900-X20, OS6900-X40, OS6900-T20, OS6900-T40, OS6900-X72, OS6900-Q32, OS6900-V72, OS6900-C32,OS6900-C32E, OS6900-X48C6, OS6900-T48C6, OS6900-X48C4E, OS6900-V48C8, OS6900-X24C2, OS6900-T24C2)	
Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026
Descripción	

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6865 (OS6865-P16X, OS6865-U12X y OS6865-U28X)	
Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026
Descripción	

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

INFORMACIÓN IMPORTANTE

Alcatel-Lucent Enterprise OmniSwitch Serie 6860 (OS6860E-24, OS6860E-P24, OS6860E-48, OS6860E-P48, OS6860E-U28, OS6860E-P24Z8, TA6860E-P48, OS6860N-U28, OS6860N-P48Z, OS6860N-P48M, O6860N-P24M, OS6860N-P24Z)	
Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026
Descripción	

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 9900 (OS9907-CFM, OS99-CMM, OS99-XNI-48, OS99-XNI-U48, OS99-GNI-48, OS99-GNI-P48, OS99-CNI-U8, OS99-XNI-P24Z8, OS99-XNI-P48Z16, OS99-XNI-U12Q, OS99-XNI-U24, OS99-XNI-U48, OS99-GNI-U48, y OS99-XNI-UP24Q2)	
Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026
Descripción	

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

INFORMACIÓN IMPORTANTE

Alcatel-Lucent Enterprise OmniSwitch Serie 6560 (OS6560-P24Z8, OS6560-P24Z24, OS6560-P48Z16, OS6560-24Z8, OS6560-24Z24, OS6560-24X4, OS6560-P24X4, OS6560-48X4, OS6560-P48X4 y OS6560-X10)	
Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026
Descripción	

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Series AlliedWare Plus SBX81CFC960 (SBx81CFC960, SBx81GP24, SBx81GT24, SBx81GS24a, SBx81GC40, SBx81XLEM) y SBX908 GEN2 (XEM2-8XSTm, XEM2-12XTm, XEM2-12XT, XEM2-12XS, XEM2-4QS, XEM2-1CQ)	
Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2019
Revisión de Validez	31/12/2023
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+) versión 5.5.0-0.6

INFORMACIÓN IMPORTANTE

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

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

Descripción

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Dell Networking C-Series (C9010 y C1048P)

Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	31/12/2023

Descripción

Este switch ofrece una plataforma de conmutación modular, de varias velocidades. Puede admitir redes de grandes empresas, medianas empresas y campus. Su plataforma de 8U cuenta con ranuras para hasta 10 módulos de tarjetas de línea, 2 módulos de procesadores de ruta, 3 módulos de ventiladores y 4 módulos de fuente de alimentación. El chasis viene equipado con un plano posterior integrado y compatible con varias velocidades 100GbE. El C1048 incluye 48 puertos 10/100/1000Base-T POE+ para el acceso de usuario y 2 puertos uplink SFP+ para la conectividad con el C9010

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

INFORMACIÓN IMPORTANTE

Dell Networking Z-Series (Z9100-ON)

Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	31/12/2023

Descripción

Este switch Open Networking de formato fijo y preparado para redes definidas por software (SDN) se ha diseñado para centros de datos y ofrece las siguientes prestaciones: - Switch multivelocidad con opciones 10/25/40/50/100GbE. - Alta densidad con hasta 32 puertos 100GbE en 1U. - Selección de los principales sistemas operativos de red. - Vía de acceso fácil a las SDN para una parte o la totalidad de su entorno de producción.

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

Dell Networking S-Series 25/40/50/100GbE (S6010-ON, S6100-ON)

Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	31/12/2023

Descripción

Los Swtiches Serie S ofrecen una solución preparada para redes definidas por software, con las siguientes pestaciones: - Alta densidad para las implementaciones basadas en 25/40/50/100GbE para la parte superior del rack, en medio de la fila o al final de la fila. - Selección de switches 40GbE S5048F-ON, S6000-ON y S6010-ON, además del switch modular 10/25/40/50/100GbE S6100-ON. - Módulos S6100-ON que incluyen: 16 puertos 14GbE, 8 puertos 100GbE, módulo combinado de 4 puertos 100GbE CXP y 4 puertos 100GbE

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

INFORMACIÓN IMPORTANTE

Dell Networking S-Series 1GbE (S3124, S3124P, S3124F, S3148, S3148P, S3048-ON)

Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	31/12/2023

Descripción

Estos switches 1GbE ofrecen las siguientes prestaciones: - Proporcionan baja latencia y alta densidad con redundancia de hardware y software.. - Ofrecen diseños de Active Fabric con el uso de switches principales de la serie S o Z para crear una arquitectura de red de centro de datos 1/10/40GbE de dos niveles.

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

Dell Networking S-Series 10GbE (S5048F, S4048-ON, S4048T-ON)

Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	31/12/2023

Descripción

Estos switches 10GbE flexibles ofrecen las siguientes prestaciones: - S4048-ON es un switch de baja latencia y alta densidad para la parte superior del rack con 48 puertos 10GbE SFP+ y 6 puertos 40 GbE (o 72 puertos 10 GbE en modo de transición), así como un rendimiento de 720 Gb/s máscimo. Es compatible con el entorno Open Network Install Environment (ONIE). - S5000 ofrece un diseño modular que permite añadir módulos Ethernet y Fibre Channel. El módulo Fibre Channel es compatible con el modo NPG los servicios completos de estructura Fibre Channel. Admite 4 módulos.

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

INFORMACIÓN IMPORTANTE

Series AlliedWare Plus x510 (X510-28GSX)	
Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2019
Revisión de Validez	31/12/2023

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+) versión 5.5.0-0.6

Series AlliedWare Plus x230 (X230-10GP, X230-10GT, X230-18GP, X230-18GT, X230-28GP, X230-28GT, X230L-17GT, X230L-26GT) y x200 (X220-28GS, X220-52GP, X220-52GT)	
Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2019
Revisión de Validez	31/12/2023

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+) versión 5.5.0-0.6E

INFORMACIÓN IMPORTANTE

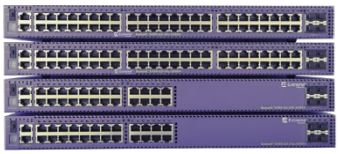
Series AlliedWare Plus x930 (x930-28GTX, x930-28GPX, x930-28GSTX, x930-52GTX, x930-52GPX) y x950 (x950-28XSQ y x950-28XTQm)	
Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2019
Revisión de Validez	31/12/2023
Descripción	

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+) versión 5.5.0-0.6

Summit x450-G2 Series: X450-G2-24t-GE4, X450-G2-24p-GE4, X450-G2-48t-GE4, X450-G2-48p-GE4, X450-G2-24t-10GE4, X450-G2-24p-10GE4, X450-G2-48t-10GE4, X450-G2-48p-10GE4, X450-G2-24p-10GE4-FB-715-TAA, X450-G2-48p-10GE4-FB-1100-TAA,X450-G2-24t-GE4-FB-TAA, X450-G2-24p-GE4-FB-715-TAA	
Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023
Descripción	



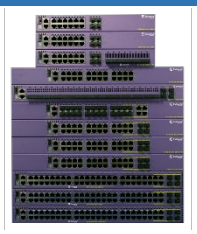
Conmutador apilable de alto rendimiento, posicionado como equipo de acceso de altas prestaciones. Proporciona conmutación avanzada de Nivel 2 y routing de Nivel 3, con interfaces 10/100/1000 Mbps, así como 10Gb. Existen versiones PoE y no PoE, y puede apilarse con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

INFORMACIÓN IMPORTANTE

Summit X440-G2 Series: X440-G2-12t-10GE4, X440-G2-12p-10GE4, X440-G2-24t-10GE4 X440-G2-24p-10GE4, X440-G2-48t-10GE4, X440-G2-48p-10GE4, X440-G2-24t-10GE4-DC, X440-G2-48t-10GE4-DC, X440-G2-24x-10GE4, X440-G2-24fx-GE4, X440-G2-12t8fx-GE4, X440-G2-24t-GE4	
Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023
Descripción	



Conmutador apilable de alto rendimiento, posicionado como equipo de acceso. Proporciona conmutación inteligente de Nivel 2 y routing básico de Nivel 3, con interfaces 10/100/1000 Mbps así como 10 Gb. Existen versiones PoE y no PoE y de puertos de fibra óptica y puede apilarse también con otras familias de switches Extreme Networks

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit X690 Series: (X690-48x-2q-4c, X690-48t-2q-4c)	
Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023
Descripción	

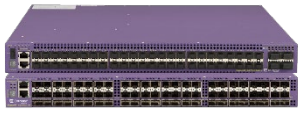
La familia de productos x690 proporciona servicios avanzados de switching y routing, pudiendo utilizarse como equipo concentrador o bien como una solución Top of Rack para una granja de servidores, gracias a su baja latencia y capacidades avanzadas. Se soportan interfaces 10Gb, 25Gb, 40Gb, 50 Gb y 100Gb. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

INFORMACIÓN IMPORTANTE

Summit x670-G2 Series: X670-G2-72x, X670-G2-48x-4q, X670-G2-48x-4q-FB-AC-TAA	
Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023
Descripción	



La familia de productos x670-G2 proporciona servicios avanzados de switching y routing, pudiendo utilizarse como equipo concentrador o bien como una solución Top of Rack para una granja de servidores, gracias a su baja latencia y capacidades avanzadas. Se soportan interfaces 10Gb y 40Gb. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit X620 Series: X620–16x, X620–16t, X620–10x, X620–8t-2x	
Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023
Descripción	

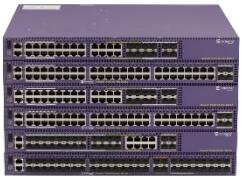
Conmutador apilable de alto rendimiento, proporcionando servicios avanzados de switching y enrutamiento básico. Destinado como concentrador de redes pequeñas y también para conexión de servidores. Soporta interfaces 100Mb, 1Gb y 10Gb. Asimismo puede proporcionar PoE. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

INFORMACIÓN IMPORTANTE

Summit X460-G2 Series: X460-G2-24t-10GE4, X460-G2-48t-10GE4, X460-G2-24p-10GE4, X460-G2-48p-10GE4, X460-G2-24x-10GE4, X460-G2-48x-10GE4, X460-G2-24t-GE4, X460-G2-48t-GE4, X460-G2-24p-GE4, X460-G2-48p-GE4	
Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023
Descripción	



Conmutador apilable de alta rendimiento, posicionado como equipo de acceso de altas prestaciones y backbone de redes medias. Proporciona conmutación avanzada de Nivel 2 y de Nivel 3, con soporte de protocolos de alta complejidad (BGP, MPLS, etc). con interfaces 10/100/1000 Mbps, así como 10Gb y 40 Gb. Existen versiones PoE y no PoE, y puede apilarse con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Aruba 6200F, 6300M, 6300F, 6405, 6410, 8320, 8325, 8360, and 8400	
Versión	Aruba OS-CX version 10.06
Fabricante	Aruba
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	29/02/2024
Descripción	

La familia Aruba CX implementan soluciones de switching y routing para redes de sucursales, campus y datacenter. Los equipos 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.

Observaciones

CCN-STIC-1432 Procedimiento de empleo seguro ARUBA OS-CX

INFORMACIÓN IMPORTANTE

Huawei CloudEngine 16800 (CE16804, CE16808 y CE16816), Huawei CloudEngine 12800 (CE12804, CE12808 y CE12816), Huawei CloudEngine 8800 (CE8861-4C-EI y CE8850-64CQ-EI) y Huawei CloudEngine 6800 (CE6863-48S6CQ, CE6881-48S6CQ y CE6820-48S6CQ)	
Versión	V200R019C10SPC800 Patch V200R019SPH008T
Fabricante	Huawei Technologies España
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2023
Descripción	

Huawei CloudEngine 16800, Huawei CloudEngine 12800, Huawei CloudEngine 8800 and Huawei CloudEngine 6800 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

Summit X870 Series: (X870-32c, X870-96x-8c)	
Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023
Descripción	

La familia de productos x870 proporciona servicios de switching y de routing. Soporta velocidades de 10 Gb, 25Gb, 40GB, 50Gby 100GB en un formato compacto de 1U. La conmutación directa de baja latencia y un conjunto de características avanzadas lo hacen ideal para centros de datos de alto rendimiento. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

INFORMACIÓN IMPORTANTE

7.5.3 CORTAFUEGOS

Check Point Security Gateway Serie 7000 (CPAP-SG7000)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

Servidores de Gestión Smart-1 (CPAP-NGSM-405, CPAP-NGSM-410, CPAP-NGSM-625, CPAP-NGSM-5050, CPAP-NGSM-5150)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

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	31/07/2025
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

Check Point Security Gateway Serie 23000 (CPAP-SG23500, CPAP-SG23800, CPAP-SG23900)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Check Point Security Gateway Serie 16000 (CPAP-SG16000, CPAP-SG16200, CPAP-SG16600HS)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

CloudGuard Network (VMware ESXi/NSX)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Sonicwall TZ Serie (300, 300W, 400, 400W, 500, 500W, 600), NSa (2650, 3600, 3650, 4600, 4650, 5600, 5650, 6600, 6650, 9250, 9450 y 9650), SM (9200, 9400, 9600 y 9800)	
Versión	6.5.4.4-44n-federal-12n
Fabricante	SONICWALL
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024

Descripción

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

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

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

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

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

Cisco Firepower Threat Defense (FTD) en Firepower 1000 y 2100 Series (FP1010, FP1120, FP1140, FP2110, FP2120, FP2130, FP2140)	
Versión	FTD 6.4 y FMC/FCMv 6.4
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2024
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).
Compatible con:
-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
-FMCv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC-651B Seguridad en cortafuegos CISCO Firepower

Check Point Security Threat Emulation/Extraction (CPAP-SBTE100XN, CPAP-SBTE250XN, CPAP-SBTE2000XN-28VM)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Check Point Security Gateway Serie 26000 y 28000 (CPAP-SG26000, CPAP-SG2800, CPAP-SG28600)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025

Descripción

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

PA-400 Series (PA-410, PA-440, PA-450, PA-460)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023

Descripción

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

Check Point Security Gateway Serie 3000 (CPAP-SG3100, CPAP-SG3200, CPAP-SG3600, CPAP-SG3800)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

PA-800 Series (PA-820, A-850)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

Check Point Security Gateway Serie 6000 (CPAP-SG6200, CPAP-SG6400, CPAP-SG6600, CPAP-SG6700, CPAP-SG6900)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

Check Point Maestro Hyperscale Appliances (CPAP-MHO-140, CPAP-MHO-175-xC)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

PA-3400 Series (PA-3410, PA-3420, PA-3430, PA-3440)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

PA-5400 Series (PA-5410, PA-5420, PA-5430, PA-5450)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

Forcepoint NGFW 3400 series (N3401, N3405, N3410)	
Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2024
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 Virtual Appliance (ESXi)	
Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2024
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 N120 series (N120, N120W, N120WL) y N60	
Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2024
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

Check Point Security Gateway serie 15000 (CPAP-SG15400, CPAP-SG15600)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Forcepoint NGFW 2200 series (N2201, N2205, N2210)	
Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2024
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 Threat Emulation/Extraction (CPAP-SBTE100X-4VM, CPAP-SBTE250X-8VM, CPAP-SBTE1000X-A-28VM, CPAP-SBTE2000X)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

OPNsense Business Edition	
Versión	23.10
Fabricante	Deciso B.V
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2022
Revisión de Validez	31/08/2024
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.

Observaciones

CCN-STIC-1453 Procedimiento de Empleo Seguro Cortafuegos OPNSense

Checkpoint Security Gateway y Maestro Hyperscale Appliances (140, 154**, 156**, 175, 3600, 3800, 6200, 6400, 6600, 6700, 7000, 16000, 16200, 16600HS, 26000, 28000, 6600, 6700, 6900, 7000, 16600, 28600, 28600HS, Smart-1 525, Smart-1 660-S, Smart-1 660-M, Smart-1 6000-L, Smart-1 6000-XL, ESXi (HPE D360 G10))	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2022
Revisión de Validez	30/11/2024
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Servidores de Gestión Smart-1 600 and 6000 series (CPAP-NGSM600S-X, CPAP-NGSM600M-X, CPAP-NGSM6000L-X, CPAP-NGSM6000XL-X)	
Versión	R.81
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025
Descripción	

Son dispositivos dedicados que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
Para más información: https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

WatchGuard Fireware on Firebox NGFWs (T35, T40, T80, T55, M270, M370, M470, M570, M670, M4600 y M5600)	
Versión	FirewareOS 12.6
Fabricante	WatchGuard Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2023
Descripción	

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

Observaciones

CCN-STIC-1421 Procedimiento de empleo seguro WatchGuard Fireware OS v12.6.2

INFORMACIÓN IMPORTANTE

PA-220 Series (PA-220, PA-220R)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

PA-3200 Series (PA-3220, PA-3250, PA-3260)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

PA-7000 Series (PA-7050, PA-7080)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

VM-Series (VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000-HV	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

PA-5200 Series (PA-5220, PA-5250, PA-5260, PA-5280)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

Eudemon1000EN USG6510E, USG6530E, USG6525E, USG555E, USG6565E, USG6575E-B, USG6610E, USG6620E, USG6650E, USG6605E-B, USG6712E y USG6716E.	
Versión	V600R007C20SPC300 + V600R007C20SPH315T
Fabricante	Huawei Technologies España
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024
Descripción	

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

Observaciones

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

INFORMACIÓN IMPORTANTE

Cisco ASA 5500 Series (5508-X and 5516-X)	
Versión	7.0
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de publicación de Procedimiento de Empleo Seguro

FTDv running on ESXi 6.7 or 7.0 on Cisco Unified Computing System (UCS) - UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3 installed on ISR	
Versión	7.0
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de publicación de Procedimiento de Empleo Seguro

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 installed on ISR	
Versión	7.0
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024

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

Pendiente de Publicación de Procedimiento de Empleo Seguro

Aruba Mobility Controller (9004, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280) y puntos de acceso.	
Versión	ArubaOS 8.6
Fabricante	Aruba
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2023

Descripción

Las familias Aruba Mobility Controllers 7000´s, 7200´s, 9000s y las Virtual Mobility Controller (appliance virtual) junto con los puntos de acceso de las familias 500s, 300s y 200s permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Con esta versión se soporta también WPA3 y Wifi-6/802.11ax (con las familias 500s) así como WiFi-5/802.1ac y Wifi-4/802.11n. Se implementan avanzadas características de seguridad, en el control de acceso a la red, así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro. Los Puntos de Acceso en modo pueden trabajar en modo Campus (CAP) y modo Remoto (RAP), lo que permite conectar de forma segura puntos de acceso que cruzan redes ajenas como internet). Se implementan mejoras en actualizaciones de software sin pérdida de servicio. Aruba Multizona permite a un Punto de Acceso dar servicio a varias Mobility Controllers de diferentes dominios o entornos de seguridad. Los Mobility Controllers puede actuar como servidores de túneles IPSEC/SSL para el cliente Aruba VIA.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS 8.6. Controladoras y Puntos de Acceso

INFORMACIÓN IMPORTANTE

FTDv running on NFVIS 4.4 on the ENCS 5406, 5408, and 5412	
Versión	7.0
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de Publicación de Procedimiento de empleo seguro

ISA 3000 (ISA 3000-4C and ISA 3000-2C2F)	
Versión	7.0
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de Publicación de Procedimiento de Empleo Seguro

INFORMACIÓN IMPORTANTE

SRX1500, SRX4100, SRX4200, SRX4600	
Versión	Junos OS 19.2R1
Fabricante	Juniper Networks
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	31/12/2024

Descripción

El firewall SRX4600 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 el usuario y la aplicación. experiencia.
Al integrar redes y seguridad en una sola plataforma, el SRX4600 cuenta con 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.
El SRX4600 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, el SRX4600 actúa como un concentrador de VPN y finaliza las conexiones superpuestas seguras/VPN en varias topologías SD-WAN.

Observaciones

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

SMB Firewall Quantum Spark series. Family 1500 and models 1600 and 1800	
Versión	R80.20
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2022
Revisión de Validez	31/12/2023

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

OPNSense	
Versión	21.7
Fabricante	Deciso B.V
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/03/2022
Revisión de Validez	31/08/2024
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.

Observaciones

CCN-STIC-1453 Procedimiento de Empleo Seguro Cortafuegos OPNSense

FortiGate NGFW Appliances (FG-61E, FG-61F, FWF-61E, FWF-61F, FG-81E, FG-81E-PoE, FG-81F, FG-81F-2R, FG-81F-2R-3G4G-PoE, FG-81F-2R-PoE, FG-81F-PoE, FG-90E, FG-91E)	
Versión	FortiOS 6.4
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025
Descripción	

Firewalls de Nueva Generación 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, etc. Más información en: https://docs.fortinet.com/product/fortigate/6.4

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

INFORMACIÓN IMPORTANTE

FortiGate NGFW Appliances (FG-100F, FG-101E, FG-101F, FG-201E, FG-201F, FG-301E, FG400F, FG-401E, FG401F, FG-501E, FG-600F, FG-601E, FG-601F)	
Versión	FortiOS 6.4
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025
Descripción	

Firewalls de Nueva Generación 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, etc. Más información en: https://docs.fortinet.com/product/fortigate/6.4

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

FortiGate NGFW Appliances (FG-1101E, FG-1801F, FG-1801F-DC, FG-2000E, FG-2201E, FG-2500E, FG-2601F, FG-2601F-DC, FG-3301E, FG-3401E, FG-3401E-DC, FG-3601E, FG-4201F, FG-4201F-DC, FG-4401F, FG-4401F-DC, FG-5001E1, FG-6300F, FG-6301F, FG-6500F, FG-6501F)	
Versión	FortiOS 6.4
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025
Descripción	

Firewalls de Nueva Generación 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, etc. Más información en: https://docs.fortinet.com/product/fortigate/6.4

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

INFORMACIÓN IMPORTANTE

FortiGate NGFW VM64	
Versión	FortiOS 6.4
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025

Descripción

Firewalls de Nueva Generación 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, etc. Más información en: https://docs.fortinet.com/product/fortigate/6.4

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

Next-Generation Firewall with PAN-OS PA-200 Series (PA-220, PA220R), PA-400, PA-800 Series (PA-820, PA850), PA-3200 Series (PA-3220, PA3250, PA3260), PA-5200 Series (PA-5220, PA5250, PA5260, PA5280), PA-5450, PA-7000 Series (PA-7050, PA7080), VM-Series (VM-50, VM-100, VM-300, VM-500, VM-700, VM-1000HV)	
Versión	10.1
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2022
Revisión de Validez	31/03/2025

Descripción

Firewalls de Nueva Generación orientado a grandes empresas y datacenters, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado.
Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido. Soportan hipervisores: vmware ESXi, Citrix SDX, Microsoft Hyper-V, KVM, vmware vCloud Air, Microsoft Azure y Amazon AWS.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

Cortafuegos SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC y SRX380	
Versión	Junos OS 20.4R1
Fabricante	Juniper Networks
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	30/11/2025

Descripción

La línea SRX300 de firewalls proporciona capacidades de seguridad, redes y SD-WAN de próxima generación para satisfacer las necesidades cambiantes de su red empresarial basada en la IA y habilitada para la nube. La gestión del SRX300 a través de la arquitectura en la nube Juniper Mist simplifica las operaciones de sus sucursales. Tanto si está añadiendo nuevas aplicaciones en varias ubicaciones, conectándose a la nube o esforzándose por mejorar la eficiencia operativa, el SRX300 puede ayudarle con una conectividad escalable, segura y fácil de gestionar.

El SRX300 admite funciones de firewall de nueva generación como prevención de intrusiones, visibilidad y control de aplicaciones y funciones de seguridad de contenidos que incluyen antivirus, antispam y filtrado Web mejorado.Advanced Threat Prevention proporciona una defensa integral frente a amenazas con detección dinámica de malware, fuentes de amenazas de SecIntel, Juniper Encrypted Traffic Insights y Juniper Adaptive Threat Profiling.

Observaciones

CCN-STIC-1442 PES Cortafuegos Juniper SRX

INFORMACIÓN IMPORTANTE

OpnSense Business Edition

Versión	23.4
Fabricante	Deciso B.V
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2022
Revisión de Validez	31/08/2024

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

Aruba Mobility Controller (9004, 9012, 9240, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) y Aruba Virtual Mobility Controllers (MC-VA-50, MC-VA-250 y MC-VA-1k)

Versión	ArubaOS 8.10
Fabricante	HPE Aruba Networking
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/03/2024

Descripción

Los Aruba Mobility Controllers permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan avanzadas características de seguridad, en el control de acceso a la red, así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro.

Observaciones

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

INFORMACIÓN IMPORTANTE

LTM+AFM (Bourne 1035v-F, Shuttle i5000 (i5600, i5800, i5820-DF), Shuttle i7000 (i7600, i7800, i7820-DF), Shuttle i10000 (i10600, i10800), Shuttle i11000 (i11600-DS, i11800-DS), Shuttle i15000 (i15800, i15600-DS), VIPRION B2250 y VIPRION B4450)	
Versión	14.1
Fabricante	F5 Networks Iberia
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2023
Descripción	

F5 BIG-IP, en su configuración de firewall, es una solución de seguridad perimetral de red para los centros de datos. Dota de mecanismos de seguridad de las capas 3 y 4 basados en políticas y una protección frente a ataques de denegación de servicio distribuidos. Con BIG-IP los ataques serán mitigados antes de llegar a los recursos críticos del centro de datos. Mediante una interfaz de gestión de políticas intuitiva, la generación de reportes y analíticas, BIG-IP proporciona una visión completa del estado de seguridad del perímetro de la red.

BIG-IP es un dispositivo full-proxy capaz de inspeccionar, gestionar y proporcionar visibilidad del tráfico entrante y saliente de las aplicaciones corporativas. Proporciona funcionalidades desde balanceo de carga a las decisiones de gestión de tráfico más complejas basadas en el cliente, las condiciones del servidor o el estado de la aplicación. Permite la gestión integral de las conexiones para la distribución de usuarios de forma inteligente hacia los servidores. BIG-IP es totalmente programable y granular, para cubrir cualquier necesidad existente o futura del control de tráfico de las aplicaciones. Mejora el tiempo de respuesta de las mismas optimizando la experiencia de los usuarios.

Observaciones

CCN-STIC-1613 PES BIG-IP LTM+AFM

Stormshield Network Security UTM/NG-Firewall (Appliances desde SN200 a SN6100 en 4 compilaciones distintas: S, M, L y XL).	
Versión	3.11.LTSB
Fabricante	Stormshield SAS
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	30/06/2024
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 Cortafuegos UTMNG Stormshield

INFORMACIÓN IMPORTANTE

SonicWall SOHO Serie (250, 250W)	
Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024
Descripción	

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

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

SonicWall TZ Serie (300P, 350, 350W, 600P)	
Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024
Descripción	

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

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

7.5.4 PROXIES

Fortinet FortiProxy	
Versión	2.0
Fabricante	Fortinet
Familia	Proxies
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	30/04/2024

Descripción

A medida que las ciber amenazas se van haciendo más sofisticadas, las compañías necesitan cada vez más una aproximación integral para proteger a los usuarios del trafico web malicioso, los websites peligrosos y aquel contenido que pueda suponer una amenaza para ellos y sus organizaciones. El Secure Web Gateway (SWG) de Fortinet (FortiProxy) aborda esta situación con un único producto que incluye filtrado de URL, protección contra amenazas avanzadas y malware, filtrado de DNS, DLP, IPS…. La protección de los usuarios contra amenazas procedentes de Internet facilita el cumplimiento de las políticas corporativas tanto normativas como de seguridad.

Observaciones

CCN-STIC-1425 PES FortiProxy

INFORMACIÓN IMPORTANTE

Zscaler Work from Anywhere

Versión	ZIA Agent 4.2.0.178
Fabricante	Zscaler Spain, S.L
Familia	Proxies
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/01/2023
Revisión de Validez	31/12/2023

Descripción

Zscaler es una plataforma de seguridad en la nube que proporciona un proxy web seguro para proteger a las empresas de las amenazas en línea. El proxy de Zscaler se ejecuta en la nube y se conecta a través de un túnel cifrado a los dispositivos de los usuarios, lo que permite a las empresas proteger sus dispositivos y datos mientras los usuarios acceden a Internet.

El proxy de Zscaler ofrece varias características de seguridad, incluyendo filtrado de contenido, detección de amenazas, prevención de intrusiones y cumplimiento normativo. El filtrado de contenido ayuda a evitar el acceso a sitios web maliciosos o inapropiados, mientras que la detección de amenazas utiliza técnicas avanzadas de aprendizaje automático para identificar y bloquear las amenazas en tiempo real. La prevención de intrusiones ayuda a proteger contra ataques de red y la violación de datos, mientras que el cumplimiento normativo ayuda a las empresas a cumplir con las regulaciones y estándares de seguridad.

Además, el proxy de Zscaler también ofrece características adicionales, como la capacidad de controlar el acceso a aplicaciones y servicios en la nube, la protección contra el robo de identidad y el filtrado de correo electrónico. También proporciona una visibilidad detallada y un control granular de las actividades en línea de los usuarios, lo que permite a las empresas detectar y abordar rápidamente cualquier actividad sospechosa.

Además, Zscaler ofrece una integración con otras soluciones de seguridad, como firewalls, sistemas de detección de intrusos y sistemas de gestión de amenazas, lo que permite una protección más completa y una respuesta más rápida a las amenazas.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

7.5.5 DISPOSITIVOS DE RED INALÁMBRICOS

Access Controllers (AC6508, AC6605, AC6805, ACU2, AC6800V, AC6507S, AirEngine 9700-M, AirEngine 9700-M1 y AirEngine 9700S-S) con Access Points (AP6050DN, AP6150DN, AP4050DE-M, AP7060DN y AirEngine 5760, 5761, 6760, 6761, 6761 Series)	
Versión	AC V200R021C00SPC100 + V200R021C00SPH301
Fabricante	Huawei Technologies España
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	30/06/2024

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.

Puntos de accesos V200R021C00SPC200 + V200R021C00SPH301T cualificados:
• AP6050DN, AP6150DN, AP4050DE-M, AP7060DN
• AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD,
• AirEngine5761-11, AirEngine5761S-11, AirEngine5761-11W, AirEngine5761S-11W, AirEngine5761-11WD, AirEngine5761S-21, AirEngine5761-21, AirEngine5761-12W, AirEngine 5761R-11, AirEngine 5761R-11E, AirEngine 5761R-11, AirEngine 5761R-11E, AirEngine 5761S-13, AirEngine 5761S-12, AirEngine 5761-10W, AirEngine 5761S-10W
• AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 6760R-51, AirEngine 6760-X1E, AirEngine 6760R-X1, AirEngine 6760-51EI
• AirEngine6761-21, AirEngine6761-21E, AirEngine 6761-21E, AirEngine 6761S-21
• AirEngine 8760R-X1, AirEngine 8760-X1-PRO y AirEngine 8760R-X1

Observaciones

CCN-STIC-1426 Procedimiento de empleo seguro Huawei AirEngine Series

INFORMACIÓN IMPORTANTE

Cisco 9800-80-K9 Wireless Controller, 9800-40-K9 Wireless Controller, 9800-L Wireless Controller (C9800-L-F-K9 y C9800-L-C-K9), C9800-CL-K9 Wireless Controller for Private Cloud.	
Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
Descripción	

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

Procedimiento de Empleo Seguro Pendiente de Publicación

Cisco 9130 Series Wi-Fi 6 Access Points (C9130AXI-x, C9130AXE-x, C9130AXE-STA-x)	
Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
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 Aironet 4800 Access Point (AIR-AP4800-x-K9 y AIR-AP4800-x-K9)C	
Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
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 9115 Series Wi-Fi 6 Access Points (C9115AXI-x y C9115AXE-x)	
Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
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 Aironet 2800 Series Access Points (AIR-AP2802I-x-K9, AIR-AP2802I-x-K9C, AIR-AP2802E-x-K9 y AIR-AP2802E-x-K9C)	
Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
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

N/A

Cisco Aironet 3800 Series Access Points (AIR-AP3802I-x-K9, AIR-AP3802I-x-K9C, AIR-AP3802e-x-K9, AIR-AP3802E-x-K9C, AIR-AP3802p-x-K9 y AIR-AP3802p-x-K9C)	
Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
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

Aruba Mobility Controller (9004, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280) y puntos de acceso.	
Versión	ArubaOS 8.6
Fabricante	Aruba
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2023
Descripción	

Las familias Aruba Mobility Controllers 7000´s, 7200´s, 9000s y las Virtual Mobility Controller (appliance virtual) junto con los puntos de acceso de las familias 500s, 300s y 200s permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Con esta versión se soporta también WPA3 y Wifi-6/802.11ax (con las familias 500s) así como WiFi-5/802.1ac y Wifi-4/802.11n. Se implementan avanzadas características de seguridad, en el control de acceso a la red, así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro. Los Puntos de Acceso en modo pueden trabajar en modo Campus (CAP) y modo Remoto (RAP), lo que permite conectar de forma segura puntos de acceso que cruzan redes ajenas como internet). Se implementan mejoras en actualizaciones de software sin pérdida de servicio. Aruba Multizona permite a un Punto de Acceso dar servicio a varias Mobility Controllers de diferentes dominios o entornos de seguridad. Los Mobility Controllers puede actuar como servidores de túneles IPSEC/SSL para el cliente Aruba VIA.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS 8.6. Controladoras y Puntos de Acceso

Cisco 9800-80, 9800-40, 9800-L Wireless Controller con Cisco Aironet 1560, 2800, 4800, 3800 Series Access Points	
Versión	IOS-XE 16.12
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2024
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.
Puntos de acceso cualificados:

- Cisco Aironet 1560 Series Access Points: Cisco Aironet 1562i, Cisco Aironet 1562e, Cisco Aironet 1562d,
- Cisco Aironet 2800 Series Access Points: Cisco Aironet 2802i, Cisco Aironet 2802e,
- Cisco Aironet 3800 Series Access Points: Cisco Aironet 3802i, Cisco Aironet 3802e, Cisco Aironet 3802p,
- Cisco Aironet 4800 Access Point

Observaciones

Procedimiento de Empleo Seguro Controladoras Inalámbricas CISCO WLC 9800

INFORMACIÓN IMPORTANTE

Ruckus SmartZone WLAN Controllers (Smart Zone 100, Smart Zone 300, Ruckus Virtual Smartzone, Ruckus virtual SmartZone - Data plane) & Access Points (R610, R650, T610/T710, R720, R750, R850)

Versión	R5.2.1.3
Fabricante	CommScope Technologies
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2022
Revisión de Validez	31/12/2023

Descripción

Los puntos de acceso RUCKUS cuentan con antenas adaptativas inteligentes con diagramas de radiación dinámicos capaces de adaptarse a cualquier escenario, incluso a los más complicados. Tanto si se enfrentan a una densidad de usuarios masiva, como a materiales de construcción perjudiciales para el Wi-Fi o a escenarios de alta complejidad radioeléctrica con arquitecturas propensas a las interferencias, los puntos de acceso RUCKUS brindan un acceso seguro y fiable de altas prestaciones garantizando una excelente experiencia de usuario en cualquier entorno.

Los controladores RUCKUS SmartZone, además de simplificar la configuración, mejorar la seguridad y facilitar la resolución de problemas, pueden separar el plano de control del plano de datos permitiendo adaptarse a cualquier arquitectura. Tanto para redes complejas de múltiples ubicaciones como para servicios gestionados de red de múltiples niveles, los controladores RUCKUS SmartZone ofrecen la escalabilidad, fiabilidad, seguridad y flexibilidad necesarias para adaptarse a los escenarios más sofisticados.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

Aruba Mobility Controller (9004, 9012, 9240, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) y Aruba Virtual Mobility Controllers (MC-VA-50, MC-VA-250 y MC-VA-1k)

Versión	ArubaOS 8.10
Fabricante	HPE Aruba Networking
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/03/2024

Descripción

Los Aruba Mobility Controllers permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan avanzadas características de seguridad, en el control de acceso a la red, así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro.

Observaciones

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

INFORMACIÓN IMPORTANTE

Huawei AirEngine (5760-22W, 5760-51,5761-10W, 5761-11,5761-11W, 5761-12W, 5761-21,5761R-11, 5761R-11E, 5761S-10W, 5761S-11, 5761S-11W, 5761S-12, 5761S-13, 5761S-21, 6760-51EI, 6760R-51,6760-X1,6760-X1E, 6761-21,6761-21E, 6761S-21, 8760R-X1, 8760-X1-PRO, 5761-10WD, 5761-11EI, 5761-12, 5761RS-11, 5762-12, 5762-12SW, 5762-13W, 5762-15HW, 5762-16W, 5762S-11, 5762S-11SW, 5762S-12, 5762S-12SW, 5762S-13W, 6760R-51E, 6761-21T, 6761-22T, 6761S-21T, 8760R-X1E) y WLAN AC (AC6508, AC6805, AirEngine 9700-M1)	
Versión	V200R022C00SPC100 + V200R022C00SPH301T
Fabricante	Huawei Technologies España
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
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

Procedimiento de empleo seguro pendiente de publicación

Cisco 9105 Series Wi-Fi 6 Access Points (C9105AXI-x, C9105AXW-x, C9105AXIT-x y C9105AXWT-x)	
Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
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 9120 Series Wi-Fi 6 Access Points (C9120AXI-x, C9120AXE-x, C9120AXP-x)	
Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
Descripción	

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

Cisco Aironet 1560 Series Access Points (AIR-AP1562I-x-K9, AIR-AP1562E-x-K9 y AIR-AP1562D-x-K9)	
Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
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 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
Descripción	

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

Cisco IW6300 Series Access Points (IW-6300H-AC-X-K9, IW-6300H-DC-X–K9 y W-6300H-DCW-X–K9)	
Versión	IOS-XE 17.6
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2023
Revisión de Validez	31/01/2024
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

Access Controllers (AC6508, AC6605, AC6805, ACU2, AC6800V, AC6507S, AirEngine 9700-M, AirEngine 9700-M1 y AirEngine 9700S-S) con Access Points (AP6050DN, AP6150DN, AP4050DE-M, AP7060DN y AirEngine 5760, 5761, 6760, 6761, 6761 Series)	
Versión	V200R020C00SPC300 + V200R020C00SPH301T
Fabricante	Huawei Technologies España
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2023

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.

Puntos de accesos cualificados:
- AP6050DN, AP6150DN, AP4050DE-M, AP7060DN
- AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD,
- AirEngine5761-11, AirEngine5761S-11, AirEngine5761-11W, AirEngine5761S-11W, AirEngine5761-11WD, AirEngine5761S-21, AirEngine5761-21, AirEngine5761-12W, AirEngine 5761R-11, AirEngine 5761R-11E, AirEngine 5761R-11, AirEngine 5761R-11E, AirEngine 5761S-13, AirEngine 5761S-12, AirEngine 5761-10W, AirEngine 5761S-10W
- AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 6760R-51, AirEngine 6760-X1E, AirEngine 6760R-X1, AirEngine 6760-51EI
- AirEngine6761-21, AirEngine6761-21E, AirEngine 6761-21E, AirEngine 6761S-21
- AirEngine 8760R-X1, AirEngine 8760-X1-PRO y AirEngine 8760R-X1

Observaciones

CCN-STIC-1426 Procedimiento de empleo seguro Huawei AirEngine Series

INFORMACIÓN IMPORTANTE

7.5.6 PASARELAS SEGURAS DE INTERCAMBIO DE DATOS

PSTfile	
Versión	v4.4.2
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2023
Descripción	

PSTfile es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de ficheros entre dominios de seguridad. Se establece una correspondencia entre carpetas, en servidores de ficheros de ambas redes y PSTfile, automáticamente, mueve o copia los ficheros del origen al destino. Soporta los protocolos FTP, FTPS, SFTP y SMB. La transferencia de ficheros desde el dominio de alta seguridad al de baja requiere autorización mediante firma digital.

Observaciones

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

PSTmail	
Versión	v3.0.5
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2023
Descripción	

PSTmail es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de correo electrónico entre dominios de seguridad. Posibilita el empleo de direcciones de correo de redes externas, desde una red interna, más segura. Soporta las versiones seguras de los protocolos de correo. Los mensajes de salida requieren autorización mediante firma digital (S/MIME).

Observaciones

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

INFORMACIÓN IMPORTANTE

7.5.7 DIODOS DE DATOS

PSTdiode	
Versión	v1.3.1-A
Fabricante	Autek Ingeniería
Familia	Diodos de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2019
Revisión de Validez	31/08/2024

Descripción

El diodo de datos hardware PSTdiode es un dispositivo de protección de perímetro que permite la transferencia de información en un único sentido entre dos dominios de seguridad con garantía física de transmisión unidireccional. Su aplicación principal es la introducción de información en una red aislada en entornos clasificados. También se puede aplicar para extraer información de una red de control industrial en entornos de infraestructuras críticas. En ambos casos se garantiza que no existe tráfico en el sentido inverso. Existen modelos de transferencia de ficheros y tráfico UDP.

Observaciones

Procedimeinto de empleo seguro: CCN-STIC 1408 Procedimiento de empleo seguro Diodo Autek Ingeniería

INFORMACIÓN IMPORTANTE

7.5.8 REDES PRIVADAS VIRTUALES: IPSEC

Cisco Firepower Threat Defense (FTD) en Firepower 1000 y 2100 Series (FP1010, FP1120, FP1140, FP2110, FP2120, FP2130, FP2140)	
Versión	FTD 6.4 y FMC/FCMv 6.4
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2024
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).
Compatible con:
-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
-FMCv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

CCN-STIC-651B Seguridad en cortafuegos CISCO Firepower

PA-400 Series (PA-410, PA-440, PA-450, PA-460)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

PA-800 Series (PA-820, A-850)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

PA-3400 Series (PA-3410, PA-3420, PA-3430, PA-3440)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

PA-5400 Series (PA-5410, PA-5420, PA-5430, PA-5450)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

EMMA VPN	
Versión	CMI/CMIX 1.6.0-23.7153 | Core 1.2.2-0.11643
Fabricante	OpenCloud Factory
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	28/02/2024
Descripción	

El módulo de concentración de VPNs de EMMA actúa como frontend para la finalización de túneles VPN, mediante un agente. EMMA realiza la autenticación, autorización y auditoría contra el gestor de identidad corporativas del Organismo y permite añadir un segundo factor de autenticación, para minimizar el riesgo de suplantación de identidad. Permite definir y aplicar políticas de acceso en función de una postura de seguridad basada en el nivel de bastionado deseado, además de otros factores, como el horario de la conexión, características del equipo, role de usuario, etc...

Observaciones

CCN-STIC-1105 Procedimiento de empleo seguro EMMA

INFORMACIÓN IMPORTANTE

WatchGuard Fireware on Firebox NGFWs (T35, T40, T80, T55, M270, M370, M470, M570, M670, M4600 y M5600)	
Versión	FirewareOS 12.6
Fabricante	WatchGuard Technologies
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2023
Descripción	

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

Observaciones

CCN-STIC-1421 Procedimiento de empleo seguro WatchGuard Fireware OS v12.6.2

PA-220 Series (PA-220, PA-220R)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

PA-3200 Series (PA-3220, PA-3250, PA-3260)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

PA-7000 Series (PA-7050, PA-7080)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

VM-Series (VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000-HV	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

PA-5200 Series (PA-5220, PA-5250, PA-5260, PA-5280)	
Versión	PAN-OS v10.2
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

Firewalls de Nueva Generación para entornos virtuales, con capacidad de identificar la aplicación, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

Cisco ASA 5500 Series (5508-X and 5516-X)	
Versión	7.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de publicación de Procedimiento de Empleo Seguro

FTDv running on ESXi 6.7 or 7.0 on Cisco Unified Computing System (UCS) - UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3 installed on ISR	
Versión	7.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de publicación de Procedimiento de Empleo Seguro

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 installed on ISR	
Versión	7.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de Publicación de Procedimiento de Empleo Seguro

Aruba Mobility Controller (9004, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280) y puntos de acceso.	
Versión	ArubaOS 8.6
Fabricante	Aruba
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2023
Descripción	

Las familias Aruba Mobility Controllers 7000´s, 7200´s, 9000s y las Virtual Mobility Controller (appliance virtual) junto con los puntos de acceso de las familias 500s, 300s y 200s permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Con esta versión se soporta también WPA3 y Wifi-6/802.11ax (con las familias 500s) así como WiFi-5/802.1ac y Wifi-4/802.11n. Se implementan avanzadas características de seguridad, en el control de acceso a la red, así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro. Los Puntos de Acceso en modo pueden trabajar en modo Campus (CAP) y modo Remoto (RAP), lo que permite conectar de forma segura puntos de acceso que cruzan redes ajenas como internet). Se implementan mejoras en actualizaciones de software sin pérdida de servicio. Aruba Multizona permite a un Punto de Acceso dar servicio a varias Mobility Controllers de diferentes dominios o entornos de seguridad. Los Mobility Controllers puede actuar como servidores de túneles IPSEC/SSL para el cliente Aruba VIA.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS 8.6. Controladoras y Puntos de Acceso

INFORMACIÓN IMPORTANTE

FTDv running on NFVIS 4.4 on the ENCS 5406, 5408, and 5412	
Versión	7.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de Publicación de Procedimiento de empleo seguro

ISA 3000 (ISA 3000-4C and ISA 3000-2C2F)	
Versión	7.0
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	19/10/2023
Revisión de Validez	31/03/2024
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

Pendiente de Publicación de Procedimiento de Empleo Seguro

INFORMACIÓN IMPORTANTE

FortiGate NGFW Appliances (FG-61E, FG-61F, FWF-61E, FWF-61F, FG-81E, FG-81E-PoE, FG-81F, FG-81F-2R, FG-81F-2R-3G4G-PoE, FG-81F-2R-PoE, FG-81F-PoE, FG-90E, FG-91E)	
Versión	FortiOS 6.4
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025
Descripción	

Firewalls de Nueva Generación 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, etc. Más información en: https://docs.fortinet.com/product/fortigate/6.4

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

FortiGate NGFW Appliances (FG-100F, FG-101E, FG-101F, FG-201E, FG-201F, FG-301E, FG400F, FG-401E, FG401F, FG-501E, FG-600F, FG-601E, FG-601F)	
Versión	FortiOS 6.4
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025
Descripción	

Firewalls de Nueva Generación 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, etc. Más información en: https://docs.fortinet.com/product/fortigate/6.4

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

INFORMACIÓN IMPORTANTE

FortiGate NGFW Appliances (FG-1101E, FG-1801F, FG-1801F-DC, FG-2000E, FG-2201E, FG-2500E, FG-2601F, FG-2601F-DC, FG-3301E, FG-3401E, FG-3401E-DC, FG-3601E, FG-4201F, FG-4201F-DC, FG-4401F, FG-4401F-DC, FG-5001E1, FG-6300F, FG-6301F, FG-6500F, FG-6501F)	
Versión	FortiOS 6.4
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025
Descripción	

Firewalls de Nueva Generación 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, etc. Más información en: https://docs.fortinet.com/product/fortigate/6.4

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

FortiGate NGFW VM64	
Versión	FortiOS 6.4
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	30/09/2025
Descripción	

Firewalls de Nueva Generación 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, etc. Más información en: https://docs.fortinet.com/product/fortigate/6.4

Observaciones

CCN-STIC 1406 Procedimiento de empleo seguro Cortafuegos FortiGate

INFORMACIÓN IMPORTANTE

Next-Generation Firewall with PAN-OS PA-200 Series (PA-220, PA220R), PA-400, PA-800 Series (PA-820, PA850), PA-3200 Series (PA-3220, PA3250, PA3260), PA-5200 Series (PA-5220, PA5250, PA5260, PA5280), PA-5450, PA-7000 Series (PA-7050, PA7080), VM-Series (VM-50, VM-100, VM-300, VM-500, VM-700, VM-1000HV)	
Versión	10.1
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2022
Revisión de Validez	31/03/2025
Descripción	

Firewalls de Nueva Generación orientado a grandes empresas y datacenters, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado.
Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido. Soportan hipervisores: vmware ESXi, Citrix SDX, Microsoft Hyper-V, KVM, vmware vCloud Air, Microsoft Azure y Amazon AWS.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

Aruba Mobility Controller (9004, 9012, 9240, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) y Aruba Virtual Mobility Controllers (MC-VA-50, MC-VA-250 y MC-VA-1k)	
Versión	ArubaOS 8.10
Fabricante	HPE Aruba Networking
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/03/2024
Descripción	

Los Aruba Mobility Controllers permiten desplegar redes inalámbricas de máxima seguridad y rendimiento. Se implementan avanzadas características de seguridad, en el control de acceso a la red, así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro.

Observaciones

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

INFORMACIÓN IMPORTANTE

Aruba Virtual Intranet Access (VIA) Client

Versión	4.3
Fabricante	Aruba
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	30/06/2025

Descripción

Aruba Virtual Intranet Access (VIA) es un servicio VPN seguro para usuarios que necesitan conectividad corporativa remota desde el hogar, ubicaciones temporales o mientras están en movimiento. Se encuentra disponible como una descarga de software para Google Android, Apple iOS, MacOS, Linux y Windows, pudiéndose integrar con plataformas de múltiple factor de autenticación (MFA, 2FA).
La función cualificada del VIA es la de cliente VPN IPSEC que evalúa y selecciona automáticamente la mejor conexión segura para efectuar la conexión VPN con la organización. A diferencia de las VPN tradicionales que requieren hardware dedicado (terminadores de túneles), Aruba integra servicios VPN directamente en la infraestructura segura existente de Aruba (Mobility Controllers) para simplificar la arquitectura y la administración.

Observaciones

CCN-STIC 1431 Procedimiento de Empleo Seguro ArubaOS 8.6. Controladoras y Puntos de Acceso

IS101

Versión	1.01
Fabricante	ISTRIA SOLUCIONES DE CRIPTOGRAFIA
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2018
Revisión de Validez	31/12/2025

Descripción

El equipo IS101 es un cifrador de altas prestaciones que, sobre una plataforma hardware segura con un FW/SW específico, implementa protocolo IPSec en modo túnel. (con encapsulado ESP y protocolo IKEv2), lo que permite establecer, de forma sencilla y eficiente, redes privadas virtuales (VPN) sobre una red IP no confiable (ya sea pública o privada). Diseñado para sistemas en entornos críticos que manejan información sensible. Velocidad de transferencia de 2Gbps agregados.

Observaciones

CCN-STIC-1405 Procedimiento de empleo seguro IS101

INFORMACIÓN IMPORTANTE

SonicWall SOHO Serie (250, 250W)

Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024

Descripción

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

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

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

Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024

Descripción

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

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

7.5.9 REDES PRIVADAS VIRTUALES: SSL

EMMA VPN	
Versión	CMI/CMIX 1.6.0-23.7153 | Core 1.2.2-0.11643
Fabricante	OpenCloud Factory
Familia	Redes privadas virtuales: SSL
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	28/02/2024
Descripción	

El módulo de concentración de VPNs de EMMA actúa como frontend para la finalización de túneles VPN, mediante un agente. EMMA realiza la autenticación, autorización y auditoría contra el gestor de identidad corporativas del Organismo y permite añadir un segundo factor de autenticación, para minimizar el riesgo de suplantación de identidad. Permite definir y aplicar políticas de acceso en función de una postura de seguridad basada en el nivel de bastionado deseado, además de otros factores, como el horario de la conexión, características del equipo, role de usuario, etc...

Observaciones

CCN-STIC-1105 Procedimiento de empleo seguro EMMA

Cisco AnyConnect Secure Mobility Client for Android 11	
Versión	4.10
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: SSL
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	31/12/2023
Descripción	

El Cisco AnyConnect Secure Mobility Client v4.10 for Android 11 es un cliente VPN, que permite a los usuarios de una organización, con dispositivos Android, trabajar de manera remota de forma completamente segura como si estuvieran conectados directamente a su red privada.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

Cisco AnyConnect Secure Mobility Client for iOS 13

Versión	4.9
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: SSL
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	31/12/2023

Descripción

El Cisco AnyConnect Secure Mobility Client v4.9 for IOS 13 es un cliente VPN, que permite a los usuarios de una organización, con dispositivos IOS, trabajar de manera remota de forma completamente segura como si estuvieran conectados directamente a su red privada.

Observaciones

Procedimiento de empleo pendiente de publicación

Cisco AnyConnect Secure Mobility Client for Windows 10

Versión	4.10
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: SSL
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	31/12/2023

Descripción

El Cisco AnyConnect Secure Mobility Client v4.10 for Windows 10 es un cliente VPN, que permite a los usuarios de una organización, con dispositivos Windows, trabajar de manera remota de forma completamente segura como si estuvieran conectados directamente a su red privada.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

7.5.10 HERRAMIENTAS PARA COMUNICACIONES MÓVILES SEGURAS

Cisco IM and Presence Service (C220 M5 y C240 M5)	
Versión	12.5 y 14 (con Centos 7.7)
Fabricante	Cisco Systems
Familia	Herramientas para comunicaciones móviles seguras
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2023
Revisión de Validez	31/12/2023
Descripción	

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

Observaciones

Procedimiento de empleo seguro pendiente de publicación

Cisco Unified Communications Manager (C220 M5 y C240 M5)	
Versión	12.5 y 14 (con Centos 7.7)
Fabricante	Cisco Systems
Familia	Herramientas para comunicaciones móviles seguras
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2023
Revisión de Validez	31/12/2023
Descripción	

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

Observaciones

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

COMSec

Versión	v4.2
Fabricante	Indra
Familia	Herramientas para comunicaciones móviles seguras
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2018
Revisión de Validez	31/12/2023

Descripción

COMSec es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con su alto nivel de seguridad, gran calidad de audio y facilidad de uso protege de forma eficaz cualquier información sensible de la organización. Las llamadas y los datos intercambiados por COMSec son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: comsec.indracompany.com

Observaciones

CCN-STIC-1407 Procedimiento de Empleo Seguro de COMSec

INFORMACIÓN IMPORTANTE

7.5.11 HERRAMIENTAS DE VIDEOCONFERENCIA

PEXIP Infinity	
Versión	v.25.4 (Build 59565.0.0); Client software v1.6.2
Fabricante	PEXIP
Familia	Herramientas de videoconferencia
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/03/2022
Revisión de Validez	31/08/2024

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

7.5.12 CIFRADORES IP

EP430TX	
Versión	1.04
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2024
Descripción	

Cifrador de comunicaciones IP hasta 200 Mbps, interoperable con el resto de cifradores de la familia EP430.

Observaciones

Utilización según PE-2016-28 Procedimiento de empleo EP430TX.

EP430GX	
Versión	v.1.08
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2024
Descripción	

Cifrador de redes IP a 2 Gbps (agregados), interoperable con el resto de cifradores de la familia EP430.

Observaciones

Utilización según PE-2012-49 Procedimiento de Empleo EP430GX.

INFORMACIÓN IMPORTANTE

EP430GN	
Versión	v2.04
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	31/12/2024
Descripción	

Cifrador de redes IP a 2 Gbps (agregados).

Observaciones

Este modelo no es compatible con el resto de la familia de cifradores EP430 de EPICOM. Utilización según P029-PE-2011-33 Operational doctrine EP430GN v2.

EP960	
Versión	1.09.17
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	31/12/2025
Descripción	

Cifrador personal de tamaño reducido (120x80x25mm) para la protección de las comunicaciones. Cuenta con varios interfaces negros (interfaces no seguros donde la información ya está cifrada) : Ethernet, WiFi y 3G/4G. Ofrece un nivel medio de seguridad y proporciona una solución de WiFi seguro.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

EP430GN

Versión	1.08.29
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2024

Descripción

Cifrador de redes IP a 2 Gbps (agregados).

Observaciones

Este modelo no es compatible con el resto de la familia de cifradores EP430 de EPICOM. Utilización según P029-PE-2011-33 Operational doctrine EP430GN v2.

IS101

Versión	1.01
Fabricante	ISTRIA SOLUCIONES DE CRIPTOGRAFIA
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2018
Revisión de Validez	31/12/2025

Descripción

El equipo IS101 es un cifrador de altas prestaciones que, sobre una plataforma hardware segura con un FW/SW específico, implementa protocolo IPSec en modo túnel. (con encapsulado ESP y protocolo IKEv2), lo que permite establecer, de forma sencilla y eficiente, redes privadas virtuales (VPN) sobre una red IP no confiable (ya sea pública o privada). Diseñado para sistemas en entornos críticos que manejan información sensible. Velocidad de transferencia de 2Gbps agregados.

Observaciones

CCN-STIC-1405 Procedimiento de empleo seguro IS101

INFORMACIÓN IMPORTANTE

7.6 PROTECCIÓN DE LA INFORMACIÓN Y LOS SOPORTES DE LA INFORMACIÓN

7.6.1 ALMACENAMIENTO CIFRADO DE DATOS

ZONE CENTRAL	
Versión	Q.2021.1
Fabricante	PRIMX
Familia	Almacenamiento cifrado de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2023
Revisión de Validez	31/12/2023

Descripción

ZONECENTRAL es un software de cifrado de datos cuyo objetivo es asegurar la confidencialidad de todos los archivos de una organización (locales, en la red y compartidos) incluyendo los perfiles de usuario.

ZONECENTRAL facilita la gestión de "la necesidad de conocer", protegiendo el acceso a los datos sensibles y segmentando la información entre los diferentes perfiles de usuarios. Solo los usuarios autorizados pueden entender el contenido de un determinado fichero.

ZONECENTRAL se instala en los puestos de trabajo como cualquier otro software de seguridad informática, integrándose con otras soluciones del tipo PKI, tarjetas inteligentes, token, etc.. y aplica de forma automática las políticas de seguridad de la empresa.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

CRYHOD	
Versión	Q.2021.2
Fabricante	PRIMX
Familia	Almacenamiento cifrado de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2023
Revisión de Validez	31/12/2023

Descripción

Cryhod es un programa de cifrado moderno que asegura el cifrado completo de los discos duros de las estaciones de trabajo portátiles de la organización. Cryhod implementa mecanismo de autenticación fuerte (doble factor) mediante la tarjeta SmartCard de la FNMT en el Pre-Boot del equipo lo que permite identificar unívocamente a los usuarios del sistema y protegerlo frente a ataques en caso de pérdida o robo.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.6.2 CIFRADO Y COMPARTICIÓN SEGURA DE INFORMACIÓN

SMiD Cloud	
Versión	2.1
Fabricante	ENCIFRA
Familia	Cifrado y compartición segura de información
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2024

Descripción

SMiD cloud es un dispositivo hardware Plu&Play que se integra en una red local SMB de Microsoft y que se encarga del almacenamiento cifrado de los ficheros que se almacenen en él. El uso de SMiD cloud NO requiere la instalación de ningún tipo de software o agente en los equipos que lo utilizan. Los ficheros cifrados pueden almacenarse en local y/o en uno o varios proveedores de almacenamiento en la nube.
Los dispositivos SMiD cloud sólo mantienen copias en claro de los ficheros que están siendo utilizados y retornan cualquier fichero a su estado cifrado cuando se dejan de utilizar.
El arranque de todo dispositivo SMiD cloud requiere la presencia en el arranque de una llave física USB de arranque sin la cual el dispositivo no arranca. Si se configura explícitamente para ello, los dispositivos SMiD cloud pueden ser clonados en el caso de que el original se deteriore, sea sustraído o destruido.
SMiD cloud es compatible con Directorio Activo y con cualquier o sistema operativo que opere en la red local SMB. El uso de diferentes dispositivos permite la compartimentalización automática del riesgo y de los sistemas de almacenamiento. La estructura del sistema de ficheros no sale del dispositivo SMiD cloud que los creó y no son deducibles desde el exterior.
SMiD cloud protege confidencialidad e integridad de la información que se le entrega frente a ataques en la nube o en almacenamiento local. Cualquier ataque de ransomware no pone en peligro las copias cifradas en local o en la nube ya que son inaccesibles incluso para los usuarios autorizados o para el administrador del dispositivo.
Cada fichero se cifra con una clave distinta, realmente aleatoria y de 256 bits de longitud, mediante el cifrador AES-256. La integridad de cada fichero está controlada con el valor SHA-256 del mismo.

Observaciones

Sin Procedimiento de Empleo Seguro

INFORMACIÓN IMPORTANTE

EP852

Versión	3.05
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2025

Descripción

El EP852 es un cifrador de ficheros fuera de línea que permite el cifrado y descifrado de ficheros y el transporte de información cifrada en el dispositivo. Mejora las prestaciones en cuanto a almacenamiento y velocidad de las versiones anteriores de los Token USB así como la puesta en marcha del dispositivo, carga y distribución de claves.

Observaciones

Utilización según el PE-2020-4 -Procedimiento de Empleo Seguro EP852 -(ESP)

GuardedBox

Versión	10.5
Fabricante	DinoSec
Familia	Cifrado y compartición segura de información
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	31/05/2025

Descripción

GuardedBox es una solución para almacenamiento, compartición y control seguros de información, con cifrado E2E, disponible para despliegues on-premise y en nube pública o privada, tanto autogestionados como en modalidad SaaS.
La información almacenada (denominada "secretos") y sus metadatos se guardan cifrados en el servidor mediante claves AES-256 bits, y se cifran y descifran en el lado cliente mediante criptografía asimétrica de curva elíptica reconocida para ENS en categoría ALTA y complementada con sofisticados controles de acceso.
Funcionalidades:
- Intercambio en tiempo real: individual o de grupo, disponible tanto para usuarios registrados como externos, con filtros por dominio y mecanismos de control para conocer los estados actuales y pasados de compartición.
- Notificaciones: avisa a los usuarios (por email y en el interfaz) de los eventos que afectan a los elementos de su ámbito.
- Auditoría: implementada como blockchain, registra todos los eventos sin desvelar el contenido de la información.
- Recordatorios: para definir avisos sobre acciones necesarias.
- Diseño APIficado: admite integración con otras soluciones del entorno (SSO, logging, etc.).
- Personalizaciones a medida.
- Panel de administración.

Observaciones

CCN-STIC 1509 Procedimiento de empleo seguro Guardedbox

INFORMACIÓN IMPORTANTE

EP880

Versión	V2.08.36 y V2.09.35
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2026

Descripción

El EP880 es una aplicación software que se ejecuta sobre ordenador con sistema operativo Windows y que permite realizar, en origen, el cifrado y firma de ficheros de datos “off-line” almacenados en el disco duro del ordenador o dispositivos de almacenamiento externos conectados al ordenador, para su posterior almacenamiento y/o envío de forma segura desde el correo electrónico u otro medio y, en destino, el descifrado y verificación de la integridad de los datos.

Observaciones

CCN-STIC-1506 Procedimiento de Empleo Seguro EP880

EP852

Versión	3.04
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2025

Descripción

El EP852 es un cifrador de ficheros fuera de línea que permite el cifrado y descifrado de ficheros y el transporte de información cifrada en el dispositivo. Mejora las prestaciones en cuanto a almacenamiento y velocidad de las versiones anteriores de los Token USB así como la puesta en marcha del dispositivo, carga y distribución de claves.

Observaciones

Utilización según el PE-2020-4 -Procedimiento de Empleo Seguro EP852 -(ESP)

INFORMACIÓN IMPORTANTE

7.6.3 HERRAMIENTAS DE BORRADO SEGURO

Blancco Drive Eraser	
Versión	7.6
Fabricante	Blancco
Familia	Herramientas de borrado seguro
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2020
Revisión de Validez	31/01/2024
Descripción	

Software de borrado seguro de datos para discos duros HDD y estado sólido SSD en computadoras de escritorio, laptops y almacenamiento masivo con adaptadores IDE, SATA, SAS, SCSI, FIBRA CANAL FC, SSD y Emmc. Ofrece un borrado seguro del 100% del disco duroo por particiones físicas al realizar una sobre escritura en la totalidad de los sectores contenidos en el disco duro. Permite un borrado automatizado, monitorización de las actividades de borrado e informa de todas las actividades de borrado facilitandoel cumplimiento de las Políticas de Seguridad y Retención de Información. El borrado realizado es conforme a los criterios de los órganos normativos gracias a su reporte certificado de auditoría y en cumplimiento con RGPD. Dispone de una instalación flexible y sencilla.

Observaciones

CCN-STIC 1504 Procedimiento de empleo seguro de Blancco Drive Eraser

INFORMACIÓN IMPORTANTE

OLVIDO Windows

Versión	1.0.6
Fabricante	authUSB
Familia	Herramientas de borrado seguro
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	29/02/2024

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

Blancco File Eraser	
Versión	v8.5.2
Fabricante	Blancco
Familia	Herramientas de borrado seguro
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/01/2024

Descripción

La solución de borrado de archivos Blancco File Eraser permite administrar y automatizar rutinas de borrado de datos en ordenadores de sobremesa, portátiles y servidores. BENEFICIOS PRINCIPALES 1. Borrado seguro de datos en ficheros. 2. Borrado automatizado. 3. Monitoriza e informa de todas las actividades de borrado. 4. Borrado conforme a los criterios de los órganos normativos gracias a su reporte certificado de auditoría y en cumplimiento con RGPD. 5. Sencilla instalación. Más información: espana@deletetecnology.com - 91 761 23 70.

Observaciones

CCN-STIC 1502 Procedimiento de empleo seguro de Blancco File Eraser

INFORMACIÓN IMPORTANTE

7.6.4 HERRAMIENTAS PARA FIRMA ELECTRÓNICA

Ascertia ADSS Server Signature Activation Module (SAM)	
Versión	7.0
Fabricante	Ascertia Limited
Familia	Herramientas para firma electrónica
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2022
Revisión de Validez	31/10/2024

Descripción

El ADSS SAM v.7.0.2 es el nuevo rQSCD/rQSealCD de Ascertia certificado Common Criteria EAL4+ EN 419 241-2 (SCAL2).

El ADSS SAM v.7.0.2 cumple con los estándares FIPS 140-2 Level 3, EN 419 241-1 & 2 (SCAL1 & SCAL2), EN 419 221-5, TS 119 431-1, TS 119 431-2, TS 119 432 y Cloud Signature Consortium (CSC).

Este nuevo rQSCD/rQSealCD da respuesta a las necesidades más exigentes de seguridad y confianza que necesitan los Proveedores de Servicios de Confianza Cualificados, proporcionando un alto rendimiento y una alta disponibilidad para la emisión de sellos de tiempo cualificados, de firma digital remota cualificada (reconocida) y de sello electrónico corporativo cualificado. El ADSS SAM v.7 también está disponible en modo “software only” para satisfacer los requerimientos de los Proveedores de Servicios de Confianza Avanzados.

El ADSS SAM v.7.0.2 destaca por su gran flexibilidad, resiliencia y escalabilidad; todo ello combinado con una seguridad interna bien diseñada que facilita su administración, su auditoría y la generación de informes que cumplen con los requerimientos ETSI/CEN para sistemas de Alta Confianza. Es compatible su uso con HSMs de red externos de los 3 principales fabricantes que hayan sido certificados EN 419 221-5.

Observaciones

N/A

INFORMACIÓN IMPORTANTE

SIAVAL Safecert Server Signing Sistema

Versión	v.3
Fabricante	Sistemas Informáticos Abiertos
Familia	Herramientas para firma electrónica
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	28/02/2024

Descripción

Solución de firma centralizada de la familia SIAVAL orientada a facilitar la gestión y el uso de las claves privadas y públicas de los usuarios finales, también identificados como titulares o firmantes. Está diseñado para funcionar como un dispositivo remoto de creación de firma rQSCD, según los requisitos especificados en el Reglamento (UE) nº 910/2014 del Parlamento Europeo (eIDAS: Anexo II), haciendo posible la generación de firmas electrónicas avanzadas (AdES) y de firmas electrónicas cualificadas o reconocidas (QES) en un servidor remoto.

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

7.6.5 HARDWARE SECURITY MODULE (HSM)

nShield Solo XC Hardware Security Module	
Versión	v12.60.15
Fabricante	Entrust Solutions
Familia	Hardware Security Module (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2021
Revisión de Validez	30/04/2024

Descripción

Los módulos de seguridad hardware (HSM) nShield XC son dispositivos físicos con certificación FIPS 140-2 nivel 3 y Common Criteria EAL4+ (EN 419 221-5) que permiten realizar operaciones criptográficas de forma segura. A su vez, el diseño de estos equipos, ofrece una serie de funcionalidades que facilita la gestión de material criptográfico: - Protección prácticamente ilimitada de claves privadas. - Flexibilidad en la creación de copias de seguridad de las claves al no necesitar equipos adicionales ni acceso directo a los HSM. - Capacidad de ejecutar código dentro del HSM mediante CodeSafe. Desde un punto de vista funcional, los HSM nShield XC son plataformas resistentes a la manipulación (tamper resistant) que realizan de forma segura funciones de generación y protección de claves y firma digital para una gran variedad de aplicaciones, como: - Autoridades de certificación - Procesos de negocio - Firma de código - Servicios en la nube - Blockchain privadas y públicas - Establecimiento de comunicaciones seguras

Observaciones

Solicitar al fabricante la guía de configuración utilizada en la certificación Common Criteria. Configurar el producto para la utilización de funciones, algoritmos y protocolos aprobados por el Centro Criptológico Nacional, según la guía CCN-STIC-807 Criptología de empleo en el ENS

INFORMACIÓN IMPORTANTE

CryptoServer CP5

Versión	5.1.0.0
Fabricante	UTIMACO
Familia	Hardware Security Module (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	29/02/2024

Descripción

Los Módulos de Seguridad Hardware (HSM) UTIMACO constituyen la raíz de confianza ideal para proteger activos sensibles críticos para la seguridad en empresas y administraciones públicas, con casos de uso en finanzas, automoción, IoT, infraestructuras críticas, telecomunicaciones y proveedores de servicios.

CryptoServer CP5 es el HSM certificado para la generación y almacenamiento de Certificados Cualificados para firmas y sellos electrónicos que cuenta con la Certificación Common Criteria acorde al Protection Profile eIDAS EN 419221-5 “Módulo Criptográfico para Servicios de Confianza”.

CryptoServer CP5 dispone de funcionalidades de autorización de clave para creación de firmas cualificadas y firmas remotas compatibles con eIDAS. Otras áreas de aplicación incluyen la emisión de certificados cualificados OCSP y sellado de tiempo.

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

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Thales Luna K7 Cryptographic Module (808-000048-002, 808-000073-001, 808-000066-001, 808-000069-001 y 808-000070-001)	
Versión	7.7.0 (bootloader versions 1.1.1, 1.1.2 y 1.1.4)
Fabricante	Thales
Familia	Hardware Security Module (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	28/02/2024

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

7.6.6 GESTIÓN DE METADATOS

metaOLVIDO Endpoint y metaOLVIDO Server	
Versión	2.2.6
Fabricante	Adarsus Technologies S.L
Familia	Gestión de metadatos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/04/2024
Descripción	
N/A	
Observaciones	
Procedimiento de empleo seguro pendiente de publicación	

metaOLVIDO Dashboard (modalidad on-premise)	
Versión	1.1.0
Fabricante	Adarsus Technologies S.L
Familia	Gestión de metadatos
Tipo	Producto
Categoría ENS	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	30/04/2024
Descripción	
N/A	
Observaciones	
Procedimiento de empleo seguro pendiente de publicación	

INFORMACIÓN IMPORTANTE

7.7 PROTECCIÓN DE EQUIPOS Y SERVICIOS

7.7.1 DISPOSITIVOS MÓVILES

Samsung Galaxy S22 5G (SM-S901B), S22+ 5G (SM-S906B), S22 Ultra 5G (SM-S908B)	
Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	21/01/2027

Descripción

La familia de dispositivos de la gama Galaxy S22 son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basado en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Fecha Fin de Soporte prevista:
Samsung Galaxy S22 5G SM-S901B 21/01/2027
Samsung Galaxy S22+ 5G SM-S906B 21/01/2027
Samsung Galaxy S22 Ultra 5G SM-S908B 21/01/2027

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

INFORMACIÓN IMPORTANTE

Samsung Galaxy Tab S8 5G (SM-X706B), Tab S8+ 5G (SM-X806B), Tab S8 Ultra 5G (SM-X906B), S8 5G (SM-X700B), Tab S8+ 5G (SM-X800B), Tab S8 Ultra 5G (SM-X900B)	
Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	01/02/2027

Descripción

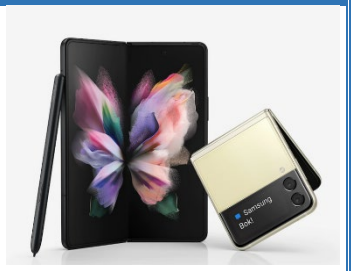
La familia de dispositivos de la gama TAB S8 son tabletas empresariales basada en Android que incorpora la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basados en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Fecha Fin de Soporte prevista:
Samsung Galaxy Tab S8 5G SM-X706B 12/01/2027
Galaxy Tab S8+ 5G SM-X806B 12/01/2027
Galaxy Tab S8 Ultra 5G SM-X906B 14/01/2027

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

Samsung Galaxy Z Flip3 5G (SM-F711F)	
Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	13/08/2026



Descripción

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

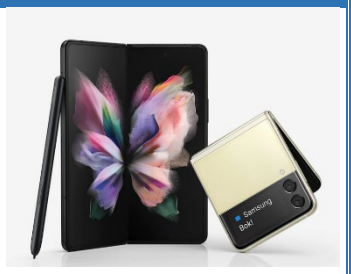
Fecha Fin de Soporte prevista:
Samsung Galaxy Z Flip3 5G SM-F711B 27/07/2026

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

INFORMACIÓN IMPORTANTE

Samsung Galaxy Z Fold3 5G (SM-F926B)



Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2022
Revisión de Validez	16/08/2026

Descripción

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

Fecha Fin de Soporte prevista:
Samsung Galaxy Z Fold3 5G SM-F926B 16/07/2026

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

Samsung Galaxy Z Flip (SM-F700F / SM-F707B)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	28/03/2024

Descripción

Galaxy Z Flip es un teléfono móvil basado en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Fecha Fin de Soporte prevista:
SM-F700F: 28/01/2024
SM-F707B: 08/07/2024

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

INFORMACIÓN IMPORTANTE

Samsung Galaxy A53 5G (SM-A536B)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	01/03/2027

Descripción

Galaxy A53 5G son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basado en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Versión de Sistema Operativo soportado actualmente: Android 12

Fecha Fin de Soporte prevista:
Samsung Galaxy A53 5G (SM-A536B): 01/02/2027

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

Samsung Galaxy Tab Active4 Pro (SM-T636 / SM-T630)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	01/09/2027

Descripción

Galaxy Tab Active 4 Pro 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.

Versión de Sistema Operativo soportado actualmente: Android 12

Fecha Fin de Soporte prevista:
Samsung Galaxy Tab Active4 Pro (SM-T636): 01/08/2027
Samsung Galaxy Tab Active4 Pro (SM-T630): 01/08/2027

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

INFORMACIÓN IMPORTANTE

Samsung Galaxy Z Fold4 5G (SM-F936B)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	01/08/2027

Descripción

La familia de dispositivos de la gama Galaxy Zfold4 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.

Versión de Sistema Operativo soportado actualmente: Android 12

Fecha Fin de Soporte prevista:
Samsung Galaxy Z Fold4 5G (SM-F936B): 01/07/2027

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

Samsung Galaxy XCover6 Pro (SM-G736B)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
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.

Versión de Sistema Operativo soportado actualmente: Android 12

Fecha Fin de Soporte prevista:
Samsung Galaxy XCover6 Pro (SM-G736B): 01/06/2027

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

INFORMACIÓN IMPORTANTE

Samsung Galaxy A52 5G (SM-A526B)

Versión	Android 12
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	10/02/2025

Descripción

El modelo Galaxy A52 5G es un teléfono móvil basado en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

Samsung Galaxy Z Flip4 (SM-F721B)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	07/08/2027

Descripción

La familia de dispositivos de la gama Galaxy Zflip 4 son dispositivos empresariales plegables basados en Android que incorpora la Plataforma Samsung Knox, ofreciendo capacidades y mecanismos de protección de integridad basados en Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Versión de Sistema Operativo soportado actualmente: Android 12

Fecha Fin de Soporte prevista:
Samsung Galaxy Z Flip4 (SM-F721B): 01/07/2027

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

INFORMACIÓN IMPORTANTE

Samsung Galaxy S23 5G (SM-G911B), S23+ 5G (SM-G916B), S23 Ultra 5G (SM-G918B)	
Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023
Descripción	

ens Esquema Nacional de Seguridad — ALTA MEDIA BÁSICA — ALTA

La familia de dispositivos de la gama Galaxy S23 5G son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1617 PES Samsung Galaxy Android12

Samsung Galaxy S21 5G (SM-G991B), S21+ 5G (SM-G996B), S21 Ultra+ 5G (SM-G998B), S21 5G FE (SM-G990B)	
Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2021
Revisión de Validez	28/01/2026
Descripción	

ens Esquema Nacional de Seguridad — ALTA MEDIA BÁSICA — ALTA

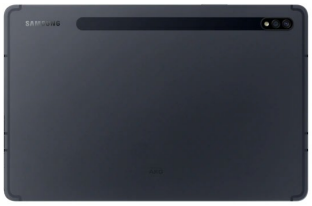
La familia de dispositivos de la gama Galaxy S21 son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

INFORMACIÓN IMPORTANTE

Samsung Galaxy Tab S7 (SM-T870 / SM-T875), Tab S7+ (SM-T970 / SM-T976B)



Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	23/08/2024

Descripción

Galaxy Tab S7 / S7+ es una tableta empresarial 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.

Fecha fin de soporte prevista:
SM-T870: 23/07/2024
SM-T875: 23/07/2024
SM-T875 Enterprise Edition: 23/07/2024
SM-T970: 23/07/2024
SM-T976B: 23/07/2024

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

Samsung Galaxy Note10 (SM-N970F), Note10+ (SM-N975F), Note10 +5G (SM-N976B)

Versión	Android 12
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	31/12/2023

Descripción

Los dispositivos de la familia Note 10 están optimizados para la ultraproductividad, preparados para afrontar los desafíos de cualquier sector empresarial, incluyendo SPen. Toda la familia con las mismas capacidades a nivel empresarial: seguridad garantizada gracias a Samsung Knox, pantalla Infinita para una mejor experiencia de trabajo, un potente procesador, carga rápida e inalámbrica, conexión a PC y unas capacidades de altas prestaciones.

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

INFORMACIÓN IMPORTANTE

Samsung Galaxy Tab S6 (SM-T860, SM-T865)

Versión	Android 12
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2020
Revisión de Validez	31/12/2023

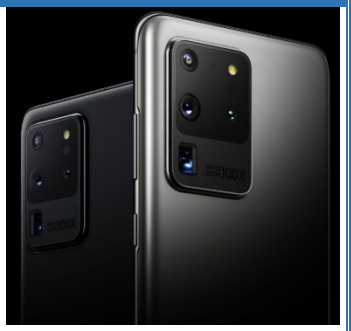
Descripción

Galaxy Tab S6 es una tableta empresarial 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 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

Samsung Galaxy S20+ 5G (SM-G986B), S20 5G (SM-G981B), S20 Ultra 5G (SM-G988B), S20+ 4G (SM-G985F), S20 4G (SM-G980F)



Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2020
Revisión de Validez	24/03/2025

Descripción

La familia de dispositivos de la gama Galaxy S20 son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Fecha fin de soporte prevista:
- SM-G986B Enterprise Edition: 24/01/2025
- SM-G986B: 24/01/2024
- SM-G981B: 24/01/2024
- SM-G988B: 24/01/2024
- SM-G985F Enterprise Edition: 24/01/2025
- SM-G985F: 24/01/2024
- SM-G980F Enterprise Edition: 24/01/2025
- SM-G980F: 24/01/2024

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

INFORMACIÓN IMPORTANTE

Samsung Galaxy Tab Active 3 (SM-T570 / SM-T575)

Versión	Android 12
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	22/09/2025

Descripción

Galaxy Tab Active 3 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 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

Samsung Galaxy A51 (SM-A515F)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2020
Revisión de Validez	05/01/2024

Descripción

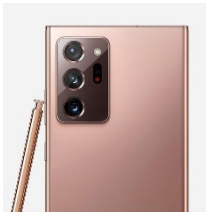
Galaxy A51 es un teléfono móvil basado en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

INFORMACIÓN IMPORTANTE

Samsung Galaxy Note20 4G (SM-N980F), Note20 5G (SM-N981B), Note20 Ultra 5G (SM-N986B)



Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	24/08/2025

Descripción

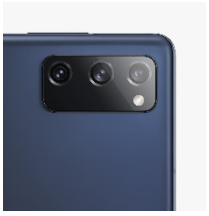
La familia de dispositivos de la gama Galaxy Note20 son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Fecha fin de soporte prevista:
- SM-N980F: 24/07/2024
- SM-N981B: 22/07/2024
- SM-N981B Enterprise Edition: 22/07/2025
- SM-N986B: 22/07/2024

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

Samsung Galaxy S20 FE 4G (SM-G780F), S20 FE 5G (SM-G781B)



Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	17/10/2025

Descripción

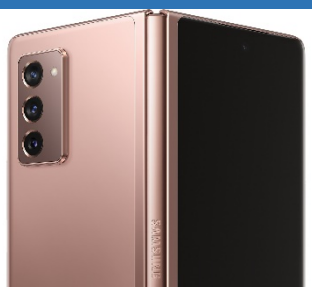
La familia de dispositivos de la gama Galaxy S20 FE son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

INFORMACIÓN IMPORTANTE

Samsung Galaxy Z Fold2 5G (SM-F916B)



Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	27/09/2024

Descripción

Galaxy Z Fold2 5G es un teléfono móvil basado en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

Samsung Galaxy XCoverPro (SM-G715FN)

Versión	Android 13
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2020
Revisión de Validez	10/02/2024

Descripción

Galaxy XCover Pro es un teléfono móvil rugerizado basado en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Fecha fin de soporte prevista:
SM-G715FN: Enterprise Edition: 10/01/2024
SM-G715FN: 10/01/2024

Observaciones

CCN-STIC 1617 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)

INFORMACIÓN IMPORTANTE

7.7.2 SISTEMAS OPERATIVOS

Oracle Solaris - Operating System	
Versión	11.4
Fabricante	Oracle America Inc.
Familia	Sistemas Operativos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2023
Revisión de Validez	31/12/2023
Descripción	

Oracle Solaris es una plataforma consistente sobre la que ejecutar aplicaciones empresariales. Dispone de interfaces administrativas fáciles de usar y que minimizan la ocurrencia de errores críticos. Permite la configuración sencilla de una estrategia integral de defensa en profundidad y está diseñada para satisfacer los requisitos de seguridad, rendimiento y escalabilidad.

Observaciones

Procedimiento de empleo pendiente de publicación

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	09/01/2024
Descripción	

Sistema Operativo para servidores

Observaciones

CCN-STIC-570A, CCN-STIC-570B Anexo A

INFORMACIÓN IMPORTANTE

SUSE Linux Enterprise	
Versión	Server 15 SP2
Fabricante	SUSE Software Solutions
Familia	Sistemas Operativos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2021
Revisión de Validez	31/03/2024

Descripción

SUSE® Linux Enterprise Server (SLES) 15 SP2 es un sistema operativo (SO) modular que ayuda a simplificar el entorno IT, modernizar la infraestructura IT y acelerar la innovación. SLES se adapta a cualquier entorno operativo a la vez que satisface los requisitos de rendimiento, seguridad y confiabilidad. Es una plataforma fácil de administrar para desarrolladores y administradores que permite implementar cargas de trabajo críticas para el negocio en las instalaciones, en la nube y en el perímetro.

Observaciones

CCN-STIC-1615 Procedimiento de empleo seguro SUSE 15 SP2

INFORMACIÓN IMPORTANTE

7.7.3 PROTECCIÓN DE CORREO ELECTRÓNICO

Proofpoint Email Protection & Targeted Email Protection	
Versión	N/A
Fabricante	Proofpoint, Inc.
Familia	Protección de correo electrónico
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/04/2024
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

Procedimiento de empleo seguro pendiente de publicación

Cisco Email Security Appliance (C190, C195, C390, C395, C690, C690X, C695, C695F, C100v, C300v y C600v)	
Versión	AsyncOS 13.0
Fabricante	Cisco Systems
Familia	Protección de correo electrónico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	31/05/2025
Descripción	

Cisco Email Security Appliance es una pasarela de seguridad para el correo electrónico. Está diseñado para detectar y bloquear una amplia variedad de amenazas transmitidas por correo electrónico, como malware, spam e intentos de phishing.

Observaciones

CCN-STIC 1623 Procedimiento de Empleo Seguro Cisco Email Security Appliance

INFORMACIÓN IMPORTANTE

Microsoft Defender for Office 365 (Email Protection)

Versión	n/a
Fabricante	Microsoft Iberica SRL
Familia	Protección de correo electrónico
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/12/2023

Descripción

Microsoft Defender para Office 365 es una solución de seguridad en la nube que protege el correo electrónico en Office365 o en local y los servicios de Office 365 (Microsoft Teams, SharePoint, OneDrive y aplicaciones de Office) contra amenazas como phishing, malware, spam y compromiso de correo electrónico empresarial. También ofrece herramientas para educar a los empleados sobre cómo detectar correos electrónicos de phishing y protege contra descargas de archivos maliciosos a través de navegadores web. Además, utiliza tecnologías para bloquear remitentes no deseados y analiza el contenido de los correos electrónicos para detectar y bloquear contenido inapropiado o no deseado. En resumen, Microsoft Defender para Office 365 es una solución completa y efectiva para proteger a las empresas de las amenazas de correo electrónico y servicios de Office 365 (Microsoft Teams, SharePoint, OneDrive y aplicaciones de Office).

Observaciones

Procedimiento de empleo pendiente de publicación

FortiMail Appliances FML-200F, FML-400F, FML-900F, FML-VM (appliance virtual)

Versión	Firmware 6.2
Fabricante	Fortinet
Familia	Protección de correo electrónico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2019
Revisión de Validez	09/02/2024

Descripción

Sistema de seguridad de correo electrónico que proporciona una protección multicapa contra spam, virus, gusanos y spyware. El motor de filtrado empleado en FortiMail bloquea el spam y el malware antes de que pueda afectar a las redes y usuarios.
Advertencia:
Las funcionalidades de Single Sing-on, DLP y FortiIsolator no han sido evaluadas y, por tanto, no se consideran cualificadas.

Observaciones

CCN-STIC-1614 Procedimiento de empleo seguro Fortimail

INFORMACIÓN IMPORTANTE

7.7.4 PLATAFORMAS CONFIABLES

DELL Precision 3570	
Versión	-
Fabricante	Dell Computer
Familia	Plataformas confiables
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2022
Revisión de Validez	29/02/2024

Descripción

El equipo portátil Dell Precision 3570 con sistema operativo Windows 10 Enterprise N LTSC, Versión 21H2, Compilación 19044.1288 securizable sirve como base o soporte para la ejecución de determinados módulos software con los que es compatible. Proporciona protección de los datos de usuario, protección de las funciones de seguridad, autenticación y autorización seguras, auditoría de seguridad, soporte criptográfico y mecanismos de acceso seguros.

Observaciones

CCN-STIC-1618 Procedimiento de empleo seguro DELL PRECISION 3570

INFORMACIÓN IMPORTANTE

7.7.5 BALANCEADORES DE CARGA

A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655, TH-940, TH-1040, TH-3350E, TH-3350, TH-4440 TH-5440, TH-5840, TH-5845, TH-6440, TH-6655S, TH-7440, TH-7440-11, TH-7650, TH-14045)	
Versión	ACOS 5.2.1-P3
Fabricante	A10 Networks, Inc
Familia	Balanceadores de carga
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	29/02/2024

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

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

A10 Networks VThunder (vTH-1Gbps, vTH-4Gbps, vTH-8Gbps, vTH-10Gbps, vTH-20Gbps, vTH-40Gbps, vTH-100Gbps, FlexPool)	
Versión	ACOS 5.2.1-P3
Fabricante	A10 Networks, Inc
Familia	Balanceadores de carga
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	29/02/2024

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

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

LTM+AFM (Bourne 1035v-F, Shuttle i5000 (i5600, i5800, i5820-DF), Shuttle i7000 (i7600, i7800, i7820-DF), Shuttle i10000 (i10600, i10800), Shuttle i11000 (i11600-DS, i11800-DS), Shuttle i15000 (i15800, i15600-DS), VIPRION B2250 y VIPRION B4450)	
Versión	14.1
Fabricante	F5 Networks Iberia
Familia	Balanceadores de carga
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2023

Descripción

F5 BIG-IP, en su configuración de firewall, es una solución de seguridad perimetral de red para los centros de datos. Dota de mecanismos de seguridad de las capas 3 y 4 basados en políticas y una protección frente a ataques de denegación de servicio distribuidos. Con BIG-IP los ataques serán mitigados antes de llegar a los recursos críticos del centro de datos. Mediante una interfaz de gestión de políticas intuitiva, la generación de reportes y analíticas, BIG-IP proporciona una visión completa del estado de seguridad del perímetro de la red.

BIG-IP es un dispositivo full-proxy capaz de inspeccionar, gestionar y proporcionar visibilidad del tráfico entrante y saliente de las aplicaciones corporativas. Proporciona funcionalidades desde balanceo de carga a las decisiones de gestión de tráfico más complejas basadas en el cliente, las condiciones del servidor o el estado de la aplicación. Permite la gestión integral de las conexiones para la distribución de usuarios de forma inteligente hacia los servidores. BIG-IP es totalmente programable y granular, para cubrir cualquier necesidad existente o futura del control de tráfico de las aplicaciones. Mejora el tiempo de respuesta de las mismas optimizando la experiencia de los usuarios.

Observaciones

CCN-STIC-1613 PES BIG-IP LTM+AFM

INFORMACIÓN IMPORTANTE

LTM+APM (Bourne 1035v-F, Shuttle i5000 (i5600, i5800, i5820-DF), Shuttle i7000 (i7600, i7800, i7820-DF), Shuttle i10000 (i10600, i10800), Shuttle i11000 (i11600-DS, i11800-DS), Shuttle i15000 (i15800, i15600-DS), VIPRION B2250 y VIPRION B4450)	
Versión	14.1
Fabricante	F5 Networks Iberia
Familia	Balanceadores de carga
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2023

Descripción

F5 BIG-IP es una herramienta clave en la publicación y entrega de las aplicaciones. Optimiza su disponibilidad mejorando la velocidad y fiabilidad de las mismas a través de las capas de aplicación y de red. BIG-IP es un dispositivo full-proxy capaz de inspeccionar, gestionar y proporcionar visibilidad del tráfico entrante y saliente de las aplicaciones corporativas. Proporciona funcionalidades desde balanceo de carga a las decisiones de gestión de tráfico más complejas basadas en el cliente, las condiciones del servidor o el estado de la aplicación. Permite la gestión integral de las conexiones para la distribución de usuarios de forma inteligente hacia los servidores. BIG-IP es totalmente programable y granular, para cubrir cualquier necesidad existente o futura del control de tráfico de las aplicaciones. Mejora el tiempo de respuesta de las mismas optimizando la experiencia de los usuarios.

Observaciones

CCN-STIC-1612 PES BIG-IP LTM+APM

INFORMACIÓN IMPORTANTE

7.7.6 HIPERCONVERGENCIA

KATUA SDI PLATFORM	
Versión	1.0
Fabricante	KRC ESPAÑOLA S.A.
Familia	Hiperconvergencia
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	29/02/2024

Descripción

Katua®SDI Platform es una plataforma hiperconvergente escalable y segura, basada en el concepto Software Define Infraestructure, donde todos los elementos que conforman un CPD se definen en una única plataforma hardware y software. Permite el despliegue rápido de servicios (xaaS), consolidación de CPDs, SDN y tiene capacidad de instalación desde equipos móviles hasta grandes centros de procesos de datos. Su flexibilidad permite que se puedan desplegar servicios cloud sobre la plataforma de forma sencilla y eficiente. Dispone de la capacidad para generar bibliotecas de sistemas preconfigurados para su despliegue con un click a través de su interfaz web. Las capacidades de optimización del hipervisor aseguran un rendimiento máximo de la plataforma, haciendo uso de todos los recursos disponibles y ofreciendo de esta forma capacidad de instalación en nodos pequeños y configuraciones hardware básicas. Su capacidad para integrarse con sistemas de almacenamiento masivos, ya sean locales o remotos permite escalar la solución en función de las necesidades. Para más información de la plataforma, vista nuestra web https://www.krc.es

Observaciones

CCN-STIC-1610 Procedimiento de Empleo Seguro KATUA SDI Platform

INFORMACIÓN IMPORTANTE

7.7.7 HERRAMIENTAS DE VIDEOIDENTIFICACIÓN

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	29/02/2024
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

Procedimiento de Empleo Seguro pendiente de publicación

certificadoelectronico.es	
Versión	1.0
Fabricante	Bewor Tech
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/03/2024
Descripción	

Solución de verificación de identidad por videoidentificación a través de la cual, de manera automática, es verificada la identidad de la persona que realiza el proceso. Esta verificación consiste en la comparación biométrica entre la foto del documento acreditativo y el rostro de la persona que realiza el proceso, esta verificación biométrica contiene prueba de vida pasiva. Además, han sido desarrolladas comprobaciones en relación a la veracidad del documento acreditativo mostrado durante el proceso, analizando las dos caras del documento y el holograma. La solución cuenta con una plataforma de verificación a través de la cual, un agente formado para ello realiza una revisión manual de todas las evidencias recogidas durante cada proceso de videoidentificación. En definitiva, con esta solución, Bewor verifica de manera remota la identidad de la persona que realiza el proceso.

Observaciones

CCN-STIC-1627 Procedimiento de empleo seguro CertificadoElectronico.es

INFORMACIÓN IMPORTANTE

Alice Onboarding

Versión

Fabricante Alice Biometrics

Familia Herramientas de videoidentificación

Tipo Servicio

Categoría ENS ALTA

Fecha Inclusión 01/04/2023

Revisión de Validez 31/03/2024

Descripción

Alice Onboarding es un sistema de verificación de identidad remota no asistido y multiplataforma para un caso de uso desatendido, en el que el usuario interactúa directamente con el sistema sin necesidad de establecer una videoconferencia con un operador. Esto se consigue mediante la captura guiada y procesado automático de selfie y documento de identidad, que son analizados con tecnología de inteligencia artificial desarrollada por Alice Biometrics. También se proporciona un dashboard de supervisión en el que un operador dispone de toda la información necesaria para la revisión del proceso y sus evidencias.

Todas las tecnologías involucradas han sido desarrolladas por Alice Biometrics, entre ellas: extracción del perfil biométrico facial para cotejar la identidad contra las fotografías del documento; análisis PAD pasivo y activo (Presentation Attack Detection o Liveness) para detectar ataques de suplantación de identidad; lectura automática del anverso y el reverso del documento; y análisis automático de seguridad documental.

Observaciones

CCN-STIC-1626 Procedimiento de Empleo Seguro Alice Biometrics

INFORMACIÓN IMPORTANTE

MobbScan 2.25

Versión	2.25
Fabricante	Mobbeel, SL
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	11/07/2023
Revisión de Validez	31/12/2023

Descripción

MobbScan es una herramienta que permite la autenticación y videoidentificación remota de usuarios de manera segura y confiable. Para ello incorpora una serie de módulos que posibilitan recabar y validar la información personal de un usuario mediante el análisis de su documento de identidad y posteriormente comprobar mediante biometría facial que la persona que realiza el trámite es la propietaria del mismo. Durante todo el proceso se generan una serie de muestras y evidencias que son almacenadas temporalmente de manera segura hasta que un agente autorizado pueda revisarlas y validarlas a través de un portal web que asiste en esa tarea (proceso desasistido o asíncrono). El sistema utiliza tecnologías de inteligencia artificial para realizar comprobaciones sobre el documento de identidad que permitan determinar su integridad (validez de los datos) o posible uso fraudulento (uso de copias o reproducciones digitales). El motor biométrico cuenta con tecnologías avanzadas que permiten detectar intentos de ataques de suplantación mediante el uso de instrumentos como máscaras, pantallas, caracterización o deepfake. Las conclusiones de estos análisis se muestran igualmente al agente encargado de tomar la decisión sobre la validez del proceso para facilitar su tarea y añadir una capa extra de seguridad y robustez a la solución."

Observaciones

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

Signaturit VideoID by Ivnosys

Versión	v1.0
Fabricante	IVNOSYS SOLUCIONES
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/07/2023
Revisión de Validez	29/02/2024

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

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

Veridas Identity verification service

Versión	n/a
Fabricante	Veridas Digital Authentication Solutions, S.L.
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/09/2022
Revisión de Validez	31/08/2024

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

Mi eID eSIGN

Versión	1.2
Fabricante	ANF Certification Authority
Familia	Herramientas de videoidentificación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	31/10/2023
Revisión de Validez	30/04/2024

Descripción

Sistema de identificación remota no asistido, multiplataforma y multi-idioma para la emisión de certificados cualificados, onboarding, contratación en línea, certificación de manifestaciones de voluntad y actos de presencia en remoto. Incorpora inteligencia artificial y tecnología NFC (lectura chip DNIe y en NIE).

Verifica de manera automática la identidad de la persona; comprueba la autenticidad, vigencia e integridad de los documentos de identificación y su correspondencia con la persona que está en su posesión, obtiene evidencia certificada de video y sonido. Comprueba que el sujeto está vivo, no utiliza máscaras, ni emplea instrumentos de falsificación de imagen.

Cumple la Orden ETD/743/2022, relativa a los métodos de identificación remota para la expedición de certificados electrónicos cualificados.

Incorpora servicio de firma y sellado electrónico cualificado, estampación de tiempo electrónico cualificado, servicio cualificado de conservación de evidencias a largo plazo, y servicio cualificado de validación de firmas y sellos electrónicos, en la generación de sus evidencias con plena eficacia jurídica.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

ElectronicID VideoID High Solution

Versión	3.1
Fabricante	ElectronicID
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/12/2022
Revisión de Validez	01/12/2024

Descripción

Solución de videoidentificación y verificación de identidad que permite la identificación remota del solicitante mediante la comparación de la información biométrica facial extraída del documento de identidad y la biometría facial de la persona que realiza el proceso. VideoID combina tecnologías de transmisión de vídeo con algoritmos de inteligencia artificial para garantizar la identificación biométrica del sujeto, así como la evaluación de ciertas características del documento de identidad.
El proceso a seguir incluye la acreditación de identidad mediante la muestra de las dos caras del documento, su holograma y una prueba de vida. Adicionalmente, el sistema permite la validación de una OTP dentro del propio proceso de videoidentificación.
Se incluye también la plataforma de verificación de identidad por parte de un agente donde se realiza la revisión manual de las evidencias recogidas, así como la evaluación de diferentes elementos de seguridad que apoyen la verificación. El proceso de identificación, por lo tanto, es desasistido y asíncrono.

Observaciones

CCN-STIC-1620 Procedimiento de empleo seguro ElectronicID VideoID High Solution

INFORMACIÓN IMPORTANTE

Entrust VIRA

Versión	13.7.0 (VIRA) / 9.4.7 (JIRA)
Fabricante	Entrust Solutions
Familia	Herramientas de videoidentificación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2022
Revisión de Validez	31/10/2024

Descripción

Producto software que implementa la gestión segura de evidencias de video identificación obtenidas desde el Servicio de Verificación de la Identidad de Veridas. Entrust VIRA ha sido diseñado para cumplir con todas las medidas de seguridad aplicables a este tipo de productos, y para su uso en un QTSP que cumpla con la Orden Ministerial ETD/743/2022, de 26 de julio, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

El producto Entrust VIRA está basado en un caso de uso en el que el operador no está presente en el proceso de identificación (proceso desatendido). En este caso, el operador de video identificación no interacciona con el usuario que se debe identificar, sino que éste solo consulta y analiza las evidencias (imágenes, videos y resultados de las validaciones automáticas) previamente almacenadas en los sistemas de información de la plataforma. El operador accede al panel de control en el cual se muestran las evidencias necesarias para la aprobación, y aprueba o rechaza la identificación de la persona, basándose en el análisis de las evidencias.

Observaciones

No se considera necesaria la publicación del Procedimiento de Empleo Seguro asociado.

INFORMACIÓN IMPORTANTE

IQP VideoID and SelfID_BO products	
Versión	V13.3.0
Fabricante	Infocert Spa
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	19/05/2023
Revisión de Validez	31/12/2023

Descripción

Remote-ID by InfoCert es un sistema de verificación de identidad remota que guía al sujeto en la toma de selfi y fotografías de su documento de identidad para que puedan ser procesados y comparados con su biometría facial y así verificar si es quien dice ser.
Hay dos procesos de identificación disponibles:
- asistido con operador (videoID)
- desasistido sin operador (selfID)

El resultado se pone a disposición de los operadores a través de la plataforma Identity Qualification Plaform, IQP, donde pueden llevar a cabo la revisión de las evidencias y así concluir la identificación del sujeto.
Los procesos han sido diseñados para cumplir con la Orden Ministerial ETD/743/2022, de 26 de julio, donde quedan regulados los métodos de identificación remota para la emisión de certificados electrónicos cualificados.
La solución se puede contratar a través de AC Camerfirma S.A.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

NebulaID Engine	
Versión	v2.0
Fabricante	VINTEGRIS
Familia	Herramientas de videoidentificación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	31/12/2023

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

Procedimiento de empleo pendiente de publicación

INFORMACIÓN IMPORTANTE

7.7.8 CONMUTADORES KVM

KVS4-8004VPX	
Versión	4.11.004
Fabricante	Black Box
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	31/12/2023

Descripción

Conmutadores KVM (Keyboard, Video and Mouse) seguros de Black Box, con conectividad de vídeo DisplayPort y funcionalidad de multivisor, que proporcionan aislamiento de puertos entre redes garantizando que no existan fugas de datos entre los puertos seguros y el mundo exterior. Estos dispositivos permiten controlar múltiples ordenadores desde un solo teclado, monitos y ratón, incluso con varios canales de vídeo y una combinación de periféricos USB.
Además, disponen de un puerto CAC (Common Access Card), que permite a los administradores autenticados registrar y asignar dispositivos periféricos específicos al puerto CAC.

Observaciones

Procedimiento de Empelo Seguro pendiente de publicación

KVS4-2002VX, KVS4-2004VX, KVS4-4004VX, KVS4-1008VX, KVS4-2008VX	
Versión	4.11.001
Fabricante	Black Box
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	31/12/2023

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 Empelo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

KVS4-2004DX, KVS4-1008DX, KVS4-2008DX

Versión	4.11.010
Fabricante	Black Box
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	31/12/2023

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

KVS4-2002VX, KVS4-2002HVX, KVS4-1004HVX, KVS4-2004HVX

Versión	4.11.202
Fabricante	Black Box
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	31/12/2023

Descripción

Conmutadores KVM (Keyboard, Video and Mouse) seguros de Black Box, con conectividad de vídeo DisplayPort/HDMI, que proporcionan aislamiento de puertos entre redes garantizando que no existan fugas de datos entre los puertos seguros y el mundo exterior. Estos dispositivos permiten controlar múltiples ordenadores desde un solo teclado, monitos y ratón, incluso con varios canales de vídeo y una combinación de periféricos USB.
Además, disponen de un puerto CAC (Common Access Card), que permite a los administradores autenticados registrar y asignar dispositivos periféricos específicos al puerto CAC.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

KVS4-4004DHVX

Versión	4.11.111
Fabricante	Black Box
Familia	Conmutadores KVM
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2023
Revisión de Validez	31/12/2023

Descripción

Conmutadores KVM (Keyboard, Video and Mouse) seguros de Black Box, con conectividad de vídeo DVI/HDMI/DisplayPort, que proporcionan aislamiento de puertos entre redes garantizando que no existan fugas de datos entre los puertos seguros y el mundo exterior. Estos dispositivos permiten controlar múltiples ordenadores desde un solo teclado, monitos y ratón, incluso con varios canales de vídeo y una combinación de periféricos USB.
Además, disponen de un puerto CAC (Common Access Card), que permite a los administradores autenticados registrar y asignar dispositivos periféricos específicos al puerto CAC.

Observaciones

Procedimiento de Empelo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.7.9 SISTEMAS DE GESTIÓN DE BASES DE DATOS (DBMS)

Oracle Database 19c Enterprise Edition - Relational Database Management System	
Versión	19.11 with Critical Patch Update April 2021
Fabricante	Oracle America Inc.
Familia	Sistemas de Gestión de Bases de Datos (DBMS)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2023
Revisión de Validez	30/12/2023
Descripción	
Pendiente	
Observaciones	
Procedimiento de empleo pendiente de publicación	

INFORMACIÓN IMPORTANTE

7.8 OTRAS HERRAMIENTAS

7.8.1 OTRAS HERRAMIENTAS

TrustCloud	
Versión	4
Fabricante	TrustCloud Tech SL
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	MEDIA
Fecha Inclusión	01/01/2023
Revisión de Validez	31/12/2024
Descripción	

La plataforma Trustcloud es un 'Coreógrafo de Transacciones digitales seguras'. Trustcloud es un Orquestador de orquestadores, y los Servicios son proporcionados en modelo SaaS: Software as a Service. TrustCloud orquesta y blinda las transacciones digitales llevadas a cabo entre los distintos casos de uso de los clientes. Es una plataforma única de orquestación y custodia de todas las evidencias generadas por las transacciones digitales, que permite preservar cualificadamente los activos digitales, garantizando su identidad, integridad e intención de todos los participantes en cualquier parte del mundo, y con ello se consigue que sean seguras, ya que por sí solas no lo son.

Observaciones

CCN-STIC-1622 Procedimiento de empleo seguro Branddocs TrustCloud

AWS Config	
Versión	n/a
Fabricante	AWS
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/08/2022
Revisión de Validez	31/12/2023
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

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

AWS Organizations

Versión	-
Fabricante	AWS
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/03/2023
Revisión de Validez	31/12/2023

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

Procedimiento de empleo pendiente de publicación

MetaClean Sync Workstation y MetaClean Sync Server

Versión	v.2.2.6
Fabricante	Adarsus Tecnologies
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/04/2024

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

Procedimiento de Empleo Seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

MetaClean Dashboard

Versión	v1.1.0
Fabricante	Adarsus Technologies S.L
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2023
Revisión de Validez	30/04/2024

Descripción

MetaClean Dashboard: Consola de administración de MetaClean para las distintas modalidades de despliegue. Administra, centraliza y controla la aplicación de políticas preventivas de seguridad corporativas. Permite obtener estadísticas de los metadatos procesados y controlar la exfiltración de información de forma global.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

Cloud Trail

Versión	-
Fabricante	AWS
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/06/2022
Revisión de Validez	31/12/2023

Descripción

AWS CloudTrail es un servicio web que registra las llamadas al API de AWS de su cuenta y le entrega archivos de registro. La información registrada incluye la identidad de la persona que llama a la API, la hora de la llamada a la API, la dirección IP de origen de la persona que llama a la API, los parámetros de la solicitud y los elementos de respuesta devueltos por el servicio de AWS.
Con CloudTrail, se puede obtener un historial de llamadas a la API de AWS para su cuenta, incluidas las llamadas a la API realizadas mediante la consola de administración de AWS, los SDK de AWS, las herramientas de línea de comandos y los servicios de AWS de nivel superior (como AWS CloudFormation). El historial de llamadas a la API de AWS producido por CloudTrail permite el análisis de seguridad, el seguimiento de los cambios en los recursos y la auditoría de conformidad.

Observaciones

CCN-STIC-887A Guía de configuración segura AWS

INFORMACIÓN IMPORTANTE

AWS Security Hub

Versión	-
Fabricante	AWS
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/09/2022
Revisión de Validez	31/12/2023

AWS Security Hub

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

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Microsoft Defender for Identity

Versión	n/a
Fabricante	Microsoft Iberica SRL
Familia	Otras Herramientas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/11/2024

Descripción

Microsoft Defender for Identity es una solución de seguridad basada en la nube que aprovecha las señales de Active Directory locales para identificar, detectar e investigar amenazas avanzadas, identidades comprometidas y acciones internas maliciosas dirigidas a una organización.
Microsoft Defender for Identity permite a los analistas de operaciones de seguridad y a los profesionales de la seguridad, que pueden tener problemas para detectar ataques avanzados en entornos híbridos, identificar e investigar las actividades sospechosas de usuarios y ataques avanzados. Defender for Identity utiliza perfiles del comportamiento del usuario y el aprendizaje automático para crear una línea base normalizada para cada usuario. A continuación, identifica anomalías con indicadores adaptativos que asignan un peso a cada anomalía según el nivel de riesgo asociado.
Microsoft Defender for Identity es una solución que se integra con otras soluciones de seguridad como Microsoft 365 Defender, Microsoft Cloud App Security o Azure Sentinel para ofrecer una visión más completa del estado de seguridad y facilitar la respuesta a incidentes. Se puede implementar mediante sensores instalados en controladores de dominio o mediante un agente integrado en Windows Server 2019 o posterior. Defender for Identity es un producto que se utiliza para proteger las infraestructuras críticas contra ataques sofisticados como el robo o el uso indebido de credenciales, el movimiento lateral o el acceso no autorizado a recursos sensibles ayudando a prevenir estos ataques al alertar sobre actividades sospechosas, proporcionando información detallada sobre los actores y las técnicas involucradas y sugerir acciones correctivas para mitigar el impacto.

Observaciones

CCN-STIC-885F Guía de configuración segura para Microsoft Defender for Identity (Guía en proceso de adaptación)

INFORMACIÓN IMPORTANTE

authUsb safeDoor

Versión	2.0.0.8
Fabricante	authUSB
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2019
Revisión de Validez	31/12/2023

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

Personal Code

Versión	2020.3
Fabricante	HUBOX
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/09/2021
Revisión de Validez	29/02/2024

Descripción

PERSONAL CODE es una solución de identidad digital que resuelve el problema de fraudes por suplantación de identidad. Véase la solución como una secuencia de bits que almacena, de forma segura, características biométricas e información biográfica de un individuo. Estos datos son firmados y reconocidos por una autoridad y se protegen mediante criptografía asimétrica para su posterior verificación a través de una aplicación que no requiere conectividad ni consultas a bases de datos. PERSONAL CODE implementa su solución en forma de dos librerías o DLLs, una librería de generación que se encarga de procesar la información del individuo y otra de verificación para la posterior extracción y validación de los datos.

Observaciones

CCN-STIC-1218 Procedimiento de empleo seguro Personal Code de HUBOX

INFORMACIÓN IMPORTANTE

7.9 SEGURIDAD OT

7.9.1 SEGURIDAD OT

Ágata	
Versión	2.3.3
Fabricante	Ágata Technology
Familia	Seguridad OT
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024

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

8. PRODUCTOS APROBADOS

8.1 HERRAMIENTAS PARA EL DESARROLLO DE PRODUCTOS DE SEGURIDAD

Módulo criptográfico para aplicaciones móviles Telcryp	
Versión	1.11
Fabricante	Cryptographic and Security System (CS2)
Familia	-
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/10/2023
Revisión de Validez	31/10/2025
Descripción	

Este módulo provee los servicios de cifrado y seguridad para garantizar la comunicación tanto con el servidor IMS como con los terminales remotos con un cifrado extremo a extremo.
Este módulo criptográfico está diseñado como una librería criptográfica e incorporado a aplicaciones de comunicaciones en entorno de movilidad debidamente aprobadas, e instaladas en plataformas confiables.

Observaciones

Procedimiento de empleo pendiente de publicación

8.2 CONTROL DE ACCESO

8.2.1 CONTROL DE ACCESO A RED (NAC)

Forescout 8.3 (CT-R, CT-100, CT-1000, CT-2000, CT-4000, CT-10000, CEM-5, CEM-10, CEM-25, CEM-50, CEM-100, CEM-150, CEM-200, 4130, 5110, 5120, 5140, 5160)	
Versión	8.4
Fabricante	Forescout
Familia	Control de acceso a red (NAC)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2023
Revisión de Validez	31/10/2025
Descripción	
La plataforma Forescout es una plataforma unificada de seguridad que permite a las empresas y organismos oficiales obtener información completa sobre el estado de sus entornos empresariales ampliados y orquestar medidas destinadas a reducir el riesgo operativo y de ciberseguridad. Se despliega de forma rápida y segura en entornos de campus, centros de datos, la nube y redes de OT. Ofrece descubrimiento, clasificación en tiempo real y evaluación continua de estado, sin necesidad de agentes. Para más información, véase: https://forescouttechnologies.es	
Observaciones	
CCN-STIC-1106 Procedimiento de empleo seguro Forescout	

8.2.2 GESTIÓN DE ACCESO PRIVILEGIADO (PAM)

CyberArk Privileged Account Security Solution	
Versión	10.10
Fabricante	CyberArk
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	24/06/2024

Descripción

CyberArk Core PAS es una solución de seguridad que permite proteger, controlar y monitorizar el acceso privilegiado a infraestructura locales, en la nube e híbridas. Permite a las organizaciones administrar y proteger las credenciales de las cuentas privilegiadas y los derechos de acceso, monitorizar y controlar la actividad de las cuentas privilegiadas, identificar las actividades sospechosas y responder a las amenazas. Permite:

- Asegurar y controlar centralmente el acceso a las credenciales privilegiadas basadas en políticas de seguridad definidas administrativamente
- Aislar y asegurar sesiones de usuarios privilegiados. Las capacidades de monitorización y grabación permiten a los equipos de seguridad ver sesiones privilegiadas en tiempo real, suspender automáticamente y terminar remotamente las sesiones sospechosas.
- Detectar, alertar y responder a actividades privilegiadas anómalas.
- Controlar el acceso de privilegios mínimos para * NIX y Windows. La solución permite a los usuarios con privilegios ejecutar comandos administrativos autorizados desde sus sesiones nativas de Unix o Linux, a la vez que se eliminan los privilegios de raíz innecesarios.
- Proteger los controladores de dominio de Windows.

No se incluye en la cualificación los conectores basados en Internet Explorer.

Observaciones

CCN-STIC-1108 PES CyberArk Privileged Account Security Solution PAS

8.3 SEGURIDAD EN LA EXPLOTACIÓN

8.3.1 ANTI-VIRUS / EPP (ENDPOINT PROTECTION PLATFORM)

Deep Security (Manager y Agente/Relay Linux/Windows)	
Versión	11.0
Fabricante	Trend Micro
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024

Descripción

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

Observaciones

CCN-STIC-1216 PES Trendmicro Deep Security

8.3.2 EDR (ENDPOINT DETECTION AND RESPONSE)

Deep Security (Manager y Agente/Relay Linux/Windows)	
Versión	11.0
Fabricante	Trend Micro
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024

Descripción

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

Observaciones

CCN-STIC-1216 PES Trendmicro Deep Security

8.3.3 HERRAMIENTAS DE FILTRADO DE NAVEGACIÓN

Cisco Web Security Appliance (S690, S690X, S695, S695F, S680, S390, S380, S395, S190, S195)	
Versión	AsyncOS 11.8
Fabricante	Cisco Systems
Familia	Herramientas de filtrado de navegación
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/12/2022
Revisión de Validez	31/05/2025
Descripción	

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

Observaciones

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

8.3.4 SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM)

NetWitness Platform	
Versión	11.6
Fabricante	Netwitness, an RSA Business.
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/07/2022
Revisión de Validez	31/12/2024

Descripción

La plataforma XDR de Netwitness (an RSA Business), es la solución de SIEM evolucionado o XDR (eXtended Detection and Response), con capacidades de visibilidad completa gracias a su modelo de datos unificado pudiendo capturar logs, netflows, tráfico de red, actividad en los end points, además de información de inteligencia de seguridad, de forma integrada, bajo un único motor de análisis y correlación avanzada. Además, incluye funcionalidades necesarias por un SOC para hacer frente a amenazas complejas. Netwitness Platform XDR cuenta además con componentes adicionales como UEBA (User and Entity Behaviour 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

LogICA5 Next Generation SIEM

Versión	v7.1
Fabricante	Grupo ICA Sistemas y Seguridad
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/01/2020
Revisión de Validez	30/06/2024

Descripción

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

Observaciones

CCN-STIC-1206 PES NGSIEM LogICA

8.3.5 DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS

EP543N	
Versión	V.1.7
Fabricante	Epicom
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Producto
Clasificación	RESERVADO
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2024
Descripción	

Centro de Gestión de cifradores IP EP430GN sobre ordenador seguro EP1140.

Observaciones

EP543X	
Versión	SW v 4.15
Fabricante	Epicom
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Producto
Clasificación	SECRETO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2024
Descripción	

Centro de Gestión sobre la plataforma EP1140, que da soporte a los cifradores de la familia EP430, incluidos los modelos EP430TX y EP430GX.

Observaciones

Utilización según PE-2012-49 Procedimiento de Empleo EP430GX v2

8.4 MONITORIZACIÓN DE LA SEGURIDAD

8.4.1 CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO

CARMEN	
Versión	Versión 7.16.1
Fabricante	S2 GRUPO / CCN
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2022
Revisión de Validez	31/12/2023

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 7.2.4

GigaVUE (GVS-HC301, GVS-HC302, GVS-HC2A1, GVS-HC2A2, GVS-HC101 y GVS-HC102)	
Versión	6.1
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	28/06/2023
Revisión de Validez	30/06/2024

Descripción

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

Observaciones

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

GigaVUE (GVS-TAX21-HW, GVS-TAX22-HW, GVS-TAX21A-HW, GVS-TAX22A-HW, GVS-TAC21, GVS-TAC22, GTP-ATX21, GTP-ASF21)	
Versión	6.1
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	28/06/2023
Revisión de Validez	30/06/2024

Descripción

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

Observaciones

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

8.5 PROTECCIÓN DE LAS COMUNICACIONES

8.5.1 ENRUTADORES

Aruba Switch 2930F, 2930M, 3810M y 5400R	
Versión	ArubaOS 16.08
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	31/05/2024

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-647C Seguridad en conmutadores HPE Aruba

ACX5448-M

Versión	Junos OS 20.3R1
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	31/12/2024

Descripción

La línea Juniper Networks® ACX5000 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. La línea ACX5000 simplifica las arquitecturas de acceso y agregación al eliminar capas innecesarias y superposiciones de red, lo que reduce drásticamente CapEx y OpEx. Está basada en la simplificación de la arquitectura y en la reducción de costos, la línea ACX5000 brinda a los proveedores de servicios y empresas la capacidad de adoptar un verdadero paradigma de 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-M: El ACX5448-M tiene 44 puertos 1GbE/10GbE y 6 puertos 40GbE/100GbE, así como capacidades de seguridad avanzadas como such as Media Access Control Security (MACsec) on all 1GbE/10GbE ports.

Observaciones

CCN-STIC-1445 PES Router_Juniper_ACX5448-M_JunOS 20.3R1

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

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	31/07/2024

Descripción

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

Observaciones

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

Cisco Nexus 3500 Series Switches (3524-X/XL, 3548-X/XL)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	31/07/2024
Descripción	

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

Observaciones

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

Cisco Nexus 3200 Series Switches (3232C, 3264C-E)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	31/07/2024
Descripción	

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

Observaciones

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

Cisco Nexus 3600 Series Switches (36180YC-R, 3636C-R)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	31/07/2024
Descripción	

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

Observaciones

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

Cisco ASR9000 Series y NCS4200 Series (ASR902, ASR903, ASR907, ASR920 y NCS4201, NCS4202, NCS4206, NCS4216)	
Versión	IOS-XE 16.9
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2023
Revisión de Validez	30/04/2025
Descripción	
Las familias ASR900 y NCS4200 son equipos hechos a propósito como plataformas de routing, soportando adicionalmente cifrado MACsec.	
Observaciones	
CCN-STIC 1454 Procedimiento de Empleo Seguro Routers CISCO ASR9000 y NCS4200 Series	

Cisco Nexus 9500 Series Switches (9504, 9508, 9516, Supervisor 9500-Sup-A , Supervisor 9500-Sup-A +, Supervisor 9500-Sup-B , Supervisor 9500-Sup-B, System Controller N9k-SC-A)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	04/10/2025
Descripción	
Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.	
Observaciones	
CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9	

- Cisco Nexus 9200 Series Switches (92348GC-X, 92160YC-X, 92300YC, 9272Q)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	10/04/2025
Descripción	

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

Observaciones

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

Cisco Nexus 9300 Series Switches (93108TC-EX, 93108TC-FX, 9348GC-FXP, 93216TC-FX2, 93180LC-EX, 93180YC-EX, 93180YC-FX, 93240YC-FX2, 93360YC-FX2, 9364C, 9332C, 9336C-FX2, 9364C-GX, 9316D-GX, 93600CD-GX	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	04/10/2025
Descripción	

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

Observaciones

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

Dell EMC Networking SmartFabric (Modelos: S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, MX5108n, S4248FB-ON, S4248FBL-ON, S6010-ON, Z9100-ON, MX9116n, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9264F-ON y Z9332F-ON)	
Versión	OS 10 Build: 10.5.1.3.
Fabricante	Dell Computer
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	04/01/2022
Revisión de Validez	31/08/2024

Descripción

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

Observaciones

CCN-STIC-1429 PES DELL EMC Networking

Aruba 6200F, 6300M, 6300F, 6405, 6410, 8320, 8325, 8360, and 8400

Versión	Aruba OS-CX version 10.06
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	29/02/2024

Descripción

La familia Aruba CX implementan soluciones de switching y routing para redes de sucursales, campus y datacenter. Los equipos 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.

Observaciones

CCN-STIC-1432 Procedimiento de empleo seguro ARUBA OS-CX

SLX Product Series (SLX 9740 y SLX 9540)

Versión	20.2.1
Fabricante	Extreme Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2021
Revisión de Validez	29/02/2024

Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack. El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados

Observaciones

CCN-STIC-1430 PES Switches Extreme Networks SLXOS

8.5.2 SWITCHES

Aruba Switch 2930F, 2930M, 3810M y 5400R	
Versión	ArubaOS 16.08
Fabricante	Aruba
Familia	Switches
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	31/05/2024

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-647C Seguridad en conmutadores HPE Aruba

Switches EXOS: x440-G2, x460-G2, x465, x435, x695, 5520, 5420	
Versión	EXOS 31.3.100
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2023
Revisión de Validez	31/05/2025

Descripción

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

Observaciones

CCN-STIC-1446 PES Switches EXoS

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

Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2022
Revisión de Validez	28/02/2026

Descripción

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

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

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	31/07/2024

Descripción

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

Observaciones

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

Cisco Nexus 3500 Series Switches (3524-X/XL, 3548-X/XL)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	31/07/2024
Descripción	

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

Observaciones

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

Cisco Nexus 3200 Series Switches (3232C, 3264C-E)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	31/07/2024
Descripción	

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

Observaciones

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

Cisco Nexus 3600 Series Switches (36180YC-R, 3636C-R)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	31/07/2024
Descripción	

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

Observaciones

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

Series AlliedWare Plus x550 (X550-18XTQ, X550-18XSQ, X550-18XSPQm) y x530-x530L (X530-28GPXm, X530-28GPXm, X530-52GTXm, X530-52GPXm, X530L-28GTX, X530L-28GPX, X530L-52GTX, X530L-52GPX)	
Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2019
Revisión de Validez	31/12/2023

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+) versión 5.5.0-0.6

Cisco Nexus 9500 Series Switches (9504, 9508, 9516, Supervisor 9500-Sup-A , Supervisor 9500-Sup-A +, Supervisor 9500-Sup-B , Supervisor 9500-Sup-B, System Controller N9k-SC-A)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	04/10/2025

Descripción

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

Observaciones

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

- Cisco Nexus 9200 Series Switches (92348GC-X, 92160YC-X, 92300YC, 9272Q)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	10/04/2025
Descripción	
Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.	
Observaciones	
CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9	

Cisco Nexus 9300 Series Switches (93108TC-EX, 93108TC-FX, 9348GC-FXP, 93216TC-FX2, 93180LC-EX, 93180YC-EX, 93180YC-FX, 93240YC-FX2, 93360YC-FX2, 9364C, 9332C, 9336C-FX2, 9364C-GX, 9316D-GX, 93600CD-GX	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	04/10/2025
Descripción	
Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad.	
Observaciones	
CCN-STIC-1447 PES Cisco Nexus 9000 NX-OS 9	

Dell EMC Networking SmartFabric (Modelos: S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, MX5108n, S4248FB-ON, S4248FBL-ON, S6010-ON, Z9100-ON, MX9116n, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9264F-ON y Z9332F-ON)

Versión	OS 10 Build: 10.5.1.3.
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	04/01/2022
Revisión de Validez	31/08/2024

Descripción

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

Observaciones

CCN-STIC-1429 PES DELL EMC Networking

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

Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026

Descripción

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6865 (OS6865-P16X, OS6865-U12X y OS6865-U28X)	
Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026
Descripción	

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6860 (OS6860E-24, OS6860E-P24, OS6860E-48, OS6860E-P48, OS6860E-U28, OS6860E-P24Z8, TA6860E-P48, OS6860N-U28, OS6860N-P48Z, OS6860N-P48M, O6860N-P24M, OS6860N-P24Z)	
Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026
Descripción	

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 9900 (OS9907-CFM, OS99-CMM, OS99-XNI-48, OS99-XNI-U48, OS99-GNI-48, OS99-GNI-P48, OS99-CNI-U8, OS99-XNI-P24Z8, OS99-XNI-P48Z16, OS99-XNI-U12Q, OS99-XNI-U24, OS99-XNI-U48, OS99-GNI-U48, y OS99-XNI-UP24Q2)	
Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026
Descripción	

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6560 (OS6560-P24Z8, OS6560-P24Z24, OS6560-P48Z16, OS6560-24Z8, OS6560-24Z24, OS6560-24X4, OS6560-P24X4, OS6560-48X4, OS6560-P48X4 y OS6560-X10)	
Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026
Descripción	

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Series AlliedWare Plus SBX81CFC960 (SBx81CFC960, SBx81GP24, SBx81GT24, SBx81GS24a, SBx81GC40, SBx81XLEM) y SBX908 GEN2 (XEM2-8XSTm, XEM2-12XTm, XEM2-12XT, XEM2-12XS, XEM2-4QS, XEM2-1CQ)

Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2019
Revisión de Validez	31/12/2023

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+) versión 5.5.0-0.6

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

Versión	AOS 8.9.R01
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	28/02/2026

Descripción

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

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Dell Networking C-Series (C9010 y C1048P)

Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2020
Revisión de Validez	31/12/2023

Descripción

Este switch ofrece una plataforma de conmutación modular, de varias velocidades. Puede admitir redes de grandes empresas, medianas empresas y campus. Su plataforma de 8U cuenta con ranuras para hasta 10 módulos de tarjetas de línea, 2 módulos de procesadores de ruta, 3 módulos de ventiladores y 4 módulos de fuente de alimentación. El chasis viene equipado con un plano posterior integrado y compatible con varias velocidades 100GbE. El C1048 incluye 48 puertos 10/100/1000Base-T POE+ para el acceso de usuario y 2 puertos uplink SFP+ para la conectividad con el C9010

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

Dell Networking Z-Series (Z9100-ON)

Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2020
Revisión de Validez	31/12/2023

Descripción

Este switch Open Networking de formato fijo y preparado para redes definidas por software (SDN) se ha diseñado para centros de datos y ofrece las siguientes prestaciones: - Switch multivelocidad con opciones 10/25/40/50/100GbE. - Alta densidad con hasta 32 puertos 100GbE en 1U. - Selección de los principales sistemas operativos de red. - Vía de acceso fácil a las SDN para una parte o la totalidad de su entorno de producción.

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

Dell Networking S-Series 25/40/50/100GbE (S6010-ON, S6100-ON)

Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2020
Revisión de Validez	31/12/2023

Descripción

Los Swtiches Serie S ofrecen una solución preparada para redes definidas por software, con las siguientes pestaciones: - Alta densidad para las implementaciones basadas en 25/40/50/100GbE para la parte superior del rack, en medio de la fila o al final de la fila. - Selección de switches 40GbE S5048F-ON, S6000-ON y S6010-ON, además del switch modular 10/25/40/50/100GbE S6100-ON. - Módulos S6100-ON que incluyen: 16 puertos 14GbE, 8 puertos 100GbE, módulo combinado de 4 puertos 100GbE CXP y 4 puertos 100GbE

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

Dell Networking S-Series 1GbE (S3124, S3124P, S3124F, S3148, S3148P, S3048-ON)

Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2020
Revisión de Validez	31/12/2023

Descripción

Estos switches 1GbE ofrecen las siguientes prestaciones: - Proporcionan baja latencia y alta densidad con redundancia de hardware y software.. - Ofrecen diseños de Active Fabric con el uso de switches principales de la serie S o Z para crear una arquitectura de red de centro de datos 1/10/40GbE de dos niveles.

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

Dell Networking S-Series 10GbE (S5048F, S4048-ON, S4048T-ON)

Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2020
Revisión de Validez	31/12/2023

Descripción

Estos switches 10GbE flexibles ofrecen las siguientes prestaciones: - S4048-ON es un switch de baja latencia y alta densidad para la parte superior del rack con 48 puertos 10GbE SFP+ y 6 puertos 40 GbE (o 72 puertos 10 GbE en modo de transición), así como un rendimiento de 720 Gb/s máscimo. Es compatible con el entorno Open Network Install Environment (ONIE). - S5000 ofrece un diseño modular que permite añadir módulos Ethernet y Fibre Channel. El módulo Fibre Channel es compatible con el modo NPG los servicios completos de estructura Fibre Channel. Admite 4 módulos.

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

Series AlliedWare Plus x510 (X510-28GSX)

Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2019
Revisión de Validez	31/12/2023

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+) versión 5.5.0-0.6

Series AlliedWare Plus x230 (X230-10GP, X230-10GT, X230-18GP, X230-18GT, X230-28GP, X230-28GT, X230L-17GT, X230L-26GT) y x200 (X220-28GS, X220-52GP, X220-52GT)

Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2019
Revisión de Validez	31/12/2023

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+) versión 5.5.0-0.6E

Series AlliedWare Plus x930 (x930-28GTX, x930-28GPX, x930-28GSTX, x930-52GTX, x930-52GPX) y x950 (x950-28XSQ y x950-28XTQm)

Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2019
Revisión de Validez	31/12/2023

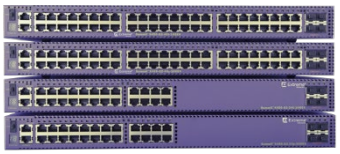
Descripción

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+) versión 5.5.0-0.6

Summit x450-G2 Series: X450-G2-24t-GE4, X450-G2-24p-GE4, X450-G2-48t-GE4, X450-G2-48p-GE4, X450-G2-24t-10GE4, X450-G2-24p-10GE4, X450-G2-48t-10GE4, X450-G2-48p-10GE4, X450-G2-24p-10GE4-FB-715-TAA, X450-G2-48p-10GE4-FB-1100-TAA,X450-G2-24t-GE4-FB-TAA, X450-G2-24p-GE4-FB-715-TAA



Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023

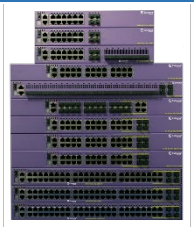
Descripción

Conmutador apilable de alto rendimiento, posicionado como equipo de acceso de altas prestaciones. Proporciona conmutación avanzada de Nivel 2 y routing de Nivel 3, con interfaces 10/100/1000 Mbps, así como 10Gb. Existen versiones PoE y no PoE, y puede apilarse con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit X440-G2 Series: X440-G2-12t-10GE4, X440-G2-12p-10GE4, X440-G2-24t-10GE4 X440-G2-24p-10GE4, X440-G2-48t-10GE4, X440-G2-48p-10GE4, X440-G2-24t-10GE4-DC, X440-G2-48t-10GE4-DC, X440-G2-24x-10GE4, X440-G2-24fx-GE4, X440-G2-12t8fx-GE4, X440-G2-24t-GE4



Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023

Descripción

Conmutador apilable de alto rendimiento, posicionado como equipo de acceso. Proporciona conmutación inteligente de Nivel 2 y routing básico de Nivel 3, con interfaces 10/100/1000 Mbps así como 10 Gb. Existen versiones PoE y no PoE y de puertos de fibra óptica y puede apilarse también con otras familias de switches Extreme Networks

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit X690 Series: (X690-48x-2q-4c, X690-48t-2q-4c)	
Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023

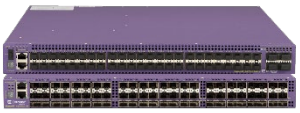
Descripción

La familia de productos x690 proporciona servicios avanzados de switching y routing, pudiendo utilizarse como equipo concentrador o bien como una solución Top of Rack para una granja de servidores, gracias a su baja latencia y capacidades avanzadas. Se soportan interfaces 10Gb, 25Gb, 40Gb, 50 Gb y 100Gb. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit x670-G2 Series: X670-G2-72x, X670-G2-48x-4q, X670-G2-48x-4q-FB-AC-TAA	
Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023



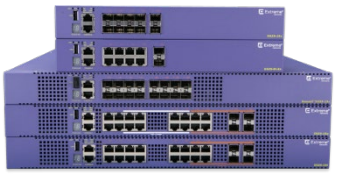
Descripción

La familia de productos x670-G2 proporciona servicios avanzados de switching y routing, pudiendo utilizarse como equipo concentrador o bien como una solución Top of Rack para una granja de servidores, gracias a su baja latencia y capacidades avanzadas. Se soportan interfaces 10Gb y 40Gb. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit X620 Series: X620–16x, X620–16t, X620–10x, X620–8t-2x	
Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023



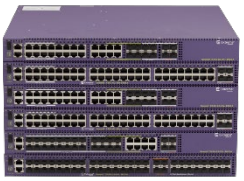
Descripción

Conmutador apilable de alto rendimiento, proporcionando servicios avanzados de switching y enrutamiento básico. Destinado como concentrador de redes pequeñas y también para conexión de servidores. Soporta interfaces 100Mb, 1Gb y 10Gb. Asimismo puede proporcionar PoE. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit X460-G2 Series: X460-G2-24t-10GE4, X460-G2-48t-10GE4, X460-G2-24p-10GE4, X460-G2-48p-10GE4, X460-G2-24x-10GE4, X460-G2-48x-10GE4, X460-G2-24t-GE4, X460-G2-48t-GE4, X460-G2-24p-GE4, X460-G2-48p-GE4	
Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023



Descripción

Conmutador apilable de alta rendimiento, posicionado como equipo de acceso de altas prestaciones y backbone de redes medias. Proporciona conmutación avanzada de Nivel 2 y de Nivel 3, con soporte de protocolos de alta complejidad (BGP, MPLS, etc). con interfaces 10/100/1000 Mbps, así como 10Gb y 40 Gb. Existen versiones PoE y no PoE, y puede apilarse con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Aruba 6200F, 6300M, 6300F, 6405, 6410, 8320, 8325, 8360, and 8400

Versión	Aruba OS-CX version 10.06
Fabricante	Aruba
Familia	Switches
Tipo	Producto
Clasificación	N/A
Fecha Inclusión	01/11/2023
Revisión de Validez	29/02/2024

Descripción

La familia Aruba CX implementan soluciones de switching y routing para redes de sucursales, campus y datacenter. Los equipos 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.

Observaciones

CCN-STIC-1432 Procedimiento de empleo seguro ARUBA OS-CX

Summit X870 Series: (X870-32c, X870-96x-8c)

Versión	EXOS v22.3.1
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2023

Descripción

La familia de productos x870 proporciona servicios de switching y de routing. Soporta velocidades de 10 Gb, 25Gb, 40GB, 50Gby 100GB en un formato compacto de 1U. La conmutación directa de baja latencia y un conjunto de características avanzadas lo hacen ideal para centros de datos de alto rendimiento. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

8.5.3 CORTAFUEGOS

Stormshield Network Security UTM/NG-Firewall (Appliances desde SN200 a SN6100 en 4 compilaciones distintas: S, M, L y XL).	
Versión	3.11.LTSB
Fabricante	Stormshield SAS
Familia	Cortafuegos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2022
Revisión de Validez	30/06/2024
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 Cortafuegos UTMNG Stormshield

8.5.4 PASARELAS SEGURAS DE INTERCAMBIO DE DATOS

Pasarelas de intercambio seguro de información para sistemas específicos militares	
Versión	No aplica
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2022
Revisión de Validez	01/05/2025
Descripción	

Pasarelas desarrolladas ad-hoc para sistemas / protocolos específicos militares. ISR, Asterix, Datalink, ADEXP, etc. Consultar disponibilidad y estado de aprobación en itsec.ccn@cni.es o cpstic.ccn@cni.es.

Observaciones

N/A

PSTfile	
Versión	v4.4.2
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2023
Descripción	

PSTfile es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de ficheros entre dominios de seguridad. Se establece una correspondencia entre carpetas, en servidores de ficheros de ambas redes y PSTfile, automáticamente, mueve o copia los ficheros del origen al destino. Soporta los protocolos FTP, FTPS, SFTP y SMB. La transferencia de ficheros desde el dominio de alta seguridad al de baja requiere autorización mediante firma digital.

Observaciones

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

PSTmail

Versión	v3.0.5
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2023

Descripción

PSTmail es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de correo electrónico entre dominios de seguridad. Posibilita el empleo de direcciones de correo de redes externas, desde una red interna, más segura. Soporta las versiones seguras de los protocolos de correo. Los mensajes de salida requieren autorización mediante firma digital (S/MIME).

Observaciones

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

8.5.5 DIODOS DE DATOS

PSTdiode	
Versión	v1.3.1-A
Fabricante	Autek Ingeniería
Familia	Diodos de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2019
Revisión de Validez	31/08/2024

Descripción

El diodo de datos hardware PSTdiode es un dispositivo de protección de perímetro que permite la transferencia de información en un único sentido entre dos dominios de seguridad con garantía física de transmisión unidireccional. Su aplicación principal es la introducción de información en una red aislada en entornos clasificados. También se puede aplicar para extraer información de una red de control industrial en entornos de infraestructuras críticas. En ambos casos se garantiza que no existe tráfico en el sentido inverso. Existen modelos de transferencia de ficheros y tráfico UDP.

Observaciones

Procedimeinto de empleo seguro: CCN-STIC 1408 Procedimiento de empleo seguro Diodo Autek Ingeniería

8.5.6 HERRAMIENTAS PARA COMUNICACIONES MÓVILES SEGURAS

COMSec Admin +	
Versión	v4.2
Fabricante	Indra
Familia	Herramientas para comunicaciones móviles seguras
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/12/2023

Descripción

COMSec Admin+ es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con su alto nivel de seguridad, gran calidad de audio y facilidad de uso protege de forma eficaz información clasificada (hasta difusión limitada) de la organización. Las llamadas y los datos intercambiados por COMSec son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: comsec.indracompany.com

Observaciones

Utilización según el PE-2018-24 Procedimiento de empleo COMSec Admin + v2 Para su empleo en entornos tácticos o desplegables, este producto deberá emplearse sobre un dispositivo móvil perteneciente a la familia “plataformas y dispositivos tácticos confiables"

8.5.7 HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA (IM)

COMSec Admin +	
Versión	v5.0
Fabricante	Indra
Familia	Herramientas de mensajería instantánea (IM)
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/12/2023

Descripción

COMSec Admin+ es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con su alto nivel de seguridad, gran calidad de audio y facilidad de uso protege de forma eficaz información clasificada (hasta difusión limitada) de la organización. Las llamadas y los datos intercambiados por COMSec son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: comsec.indracompany.com

Observaciones

Utilización según el PE-2018-24 Procedimiento de empleo COMSec Admin + v2 Para su empleo en entornos tácticos o desplegables, este producto deberá emplearse sobre un dispositivo móvil perteneciente a la familia “plataformas y dispositivos tácticos confiables"

8.5.8 HERRAMIENTAS VOZ IP

COMSec Admin +	
Versión	v5.0
Fabricante	Indra
Familia	Herramientas Voz IP
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/12/2023

Descripción

COMSec Admin+ es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con su alto nivel de seguridad, gran calidad de audio y facilidad de uso protege de forma eficaz información clasificada (hasta difusión limitada) de la organización. Las llamadas y los datos intercambiados por COMSec son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: comsec.indracompany.com

Observaciones

Utilización según el PE-2018-24 Procedimiento de empleo COMSec Admin + v2 Para su empleo en entornos tácticos o desplegables, este producto deberá emplearse sobre un dispositivo móvil perteneciente a la familia “plataformas y dispositivos tácticos confiables"

8.5.9 CIFRADORES IP

EP430TX	
Versión	1.04
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Clasificación	SECRETO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2024
Descripción	

Cifrador de comunicaciones IP hasta 200 Mbps, interoperable con el resto de cifradores de la familia EP430.

Observaciones

Utilización según PE-2016-28 Procedimiento de empleo EP430TX.

EP430GX	
Versión	v.1.08
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Clasificación	SECRETO
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2024
Descripción	

Cifrador de redes IP a 2 Gbps (agregados), interoperable con el resto de cifradores de la familia EP430.

Observaciones

Utilización según PE-2012-49 Procedimiento de Empleo EP430GX.

EP430GN	
Versión	v2.04
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Clasificación	RESERVADO
Fecha Inclusión	01/12/2022
Revisión de Validez	31/12/2024
Descripción	

Cifrador de redes IP a 2 Gbps (agregados).

Observaciones

Este modelo no es compatible con el resto de la familia de cifradores EP430 de EPICOM. Utilización según P029-PE-2011-33 Operational doctrine EP430GN v2.

EP430GN	
Versión	1.08.29
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Clasificación	RESERVADO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2024
Descripción	

Cifrador de redes IP a 2 Gbps (agregados).

Observaciones

Este modelo no es compatible con el resto de la familia de cifradores EP430 de EPICOM. Utilización según P029-PE-2011-33 Operational doctrine EP430GN v2.

Centro de gestión 543U/B

Versión	2.01
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	01/09/2020
Revisión de Validez	14/12/2023

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

EP430GU/B

Versión	2.01
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Clasificación	RESERVADO
Fecha Inclusión	01/09/2020
Revisión de Validez	14/12/2023

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

8.6 PROTECCIÓN DE LA INFORMACIÓN Y LOS SOPORTES DE LA INFORMACIÓN

8.6.1 CIFRADO Y COMPARTICIÓN SEGURA DE INFORMACIÓN

EP852	
Versión	3.05
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2025

Descripción

El EP852 es un cifrador de ficheros fuera de línea que permite el cifrado y descifrado de ficheros y el transporte de información cifrada en el dispositivo. Mejora las prestaciones en cuanto a almacenamiento y velocidad de las versiones anteriores de los Token USB así como la puesta en marcha del dispositivo, carga y distribución de claves.

Observaciones

Utilización según el PE-2020-4 -Procedimiento de Empleo Seguro EP852 -(ESP)

EP880	
Versión	V2.08.36 y V2.09.35
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2026

Descripción

El EP880 es una aplicación software que se ejecuta sobre ordenador con sistema operativo Windows y que permite realizar, en origen, el cifrado y firma de ficheros de datos “off-line” almacenados en el disco duro del ordenador o dispositivos de almacenamiento externos conectados al ordenador, para su posterior almacenamiento y/o envío de forma segura desde el correo electrónico u otro medio y, en destino, el descifrado y verificación de la integridad de los datos.

Observaciones

CCN-STIC-1506 Procedimiento de Empleo Seguro EP880

EP852

Versión	3.04
Fabricante	Epicom
Familia	Cifrado y compartición segura de información
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2025

Descripción

El EP852 es un cifrador de ficheros fuera de línea que permite el cifrado y descifrado de ficheros y el transporte de información cifrada en el dispositivo. Mejora las prestaciones en cuanto a almacenamiento y velocidad de las versiones anteriores de los Token USB así como la puesta en marcha del dispositivo, carga y distribución de claves.

Observaciones

Utilización según el PE-2020-4 -Procedimiento de Empleo Seguro EP852 -(ESP)

8.6.2 HERRAMIENTAS DE BORRADO SEGURO

OLVIDO Windows	
Versión	1.0.6
Fabricante	authUSB
Familia	Herramientas de borrado seguro
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2022
Revisión de Validez	29/02/2024

Descripción

OLVIDO es una herramienta de borrado seguro que realiza tareas de sobreescritura y borrado sobre los sistemas de archivos y discos reconocidos. Ofrece al usuario la posibilidad de borrar de forma segura distintos elementos guardados en los dispositivos de almacenamiento:

- Ficheros y carpetas
- Espacio Libre
- Fragmentos de clúster no utilizados
- Discos y volúmenes

Dispone de un módulo de planificación con el que se permite al usuario programar la ejecución de las tareas de borrado. OLVIDO implementa distintos algoritmos estándar de borrado y permite al usuario seleccionar el algoritmo de borrado a aplicar en cada tarea. Así mismo, ofrece la posibilidad al administrador de definir algoritmos de borrado personalizados, especificando el número de pases y el patrón de sobreescritura. Permite la integración con un servidor Syslog para el envío de registros de actividad y estado de las tareas de borrado realizadas.

La versión aprobada permite, con el algoritmo de borrado CCN-Clasificado, la reclasificación y desclasificación de:

- Discos magnéticos hasta RESERVADO o equivalente.
- Discos SSD hasta DIFUSIÓN LIMITADA o equivalente.

Se ejecuta sobre Windows 10, Windows Server 2016 y Windows Server 2021.

Observaciones

CCN-STIC-1508 Procedimiento de empleo seguro OLVIDO

8.6.3 HERRAMIENTAS PARA FIRMA ELECTRÓNICA

Keyone	
Versión	v 4.0
Fabricante	Safelayer
Familia	Herramientas para firma electrónica
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2023
Descripción	
Aplicación para la gestión de infraestructura de clave pública. Aprobado para proteger la confidencialidad hasta Difusión Limitada y la integridad (Firma digital) hasta Reservado.	
Observaciones	
Utilización según el PE-2015-38 Operational Doctrine KeyOne System.	

8.7 PROTECCIÓN DE EQUIPOS Y SERVICIOS

8.7.1 DISPOSITIVOS MÓVILES

Färist Mobile en Bittium Tough Mobile 2 (FM T200)	
Versión	5.1
Fabricante	Tutus
Familia	Dispositivos móviles
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	14/07/2023
Revisión de Validez	14/07/2025

Descripción

Sistema de comunicación seguro de terminales móviles basado en S.O. Android. El Färist Mobile System además de proteger la comunicación protege la plataforma (Bittium Tough Mobile 2) para almacenar información clasificada hasta el grado de Difusión Limitada.

Observaciones

Utilización según PE-2022-2 Comercializado en España por la empresa Epicom.

Färist Mobile en Google Pixel 4A 5G (FM T120)	
Versión	7.0
Fabricante	Tutus
Familia	Dispositivos móviles
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	14/07/2023
Revisión de Validez	14/07/2025

Descripción

Sistema de comunicación seguro de terminales móviles basado en S.O. Android. El Färist Mobile System además de proteger la comunicación protege la plataforma (Google Pixel 4A 5G) para almacenar información clasificada hasta el grado de Difusión Limitada.

Observaciones

Utilización según PE-2022-2 Comercializado en España por la empresa Epicom.

8.7.2 SISTEMAS OPERATIVOS

Windows Server 2016	
Versión	Datacenter Edition
Fabricante	Microsoft Corporation
Familia	Sistemas Operativos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2018
Revisión de Validez	09/01/2024
Descripción	
Sistema Operativo para servidores	
Observaciones	
CCN-STIC-570A, CCN-STIC-570B Anexo A	

SUSE Linux Enterprise	
Versión	Server 15 SP2
Fabricante	SUSE Software Solutions
Familia	Sistemas Operativos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2022
Revisión de Validez	31/03/2024
Descripción	
SUSE® Linux Enterprise Server (SLES) 15 SP2 es un sistema operativo (SO) modular que ayuda a simplificar el entorno IT, modernizar la infraestructura IT y acelerar la innovación. SLES se adapta a cualquier entorno operativo a la vez que satisface los requisitos de rendimiento, seguridad y confiabilidad. Es una plataforma fácil de administrar para desarrolladores y administradores que permite implementar cargas de trabajo críticas para el negocio en las instalaciones, en la nube y en el perímetro.	
Observaciones	
CCN-STIC-1615 Procedimiento de empleo seguro SUSE 15 SP2	

8.7.3 PROTECCIÓN DE CORREO ELECTRÓNICO

Cisco Email Security Appliance (C190, C195, C390, C395, C690, C690X, C695, C695F, C100v, C300v y C600v)	
Versión	AsyncOS 13.0
Fabricante	Cisco Systems
Familia	Protección de correo electrónico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2023
Revisión de Validez	31/05/2025
Descripción	

Cisco Email Security Appliance es una pasarela de seguridad para el correo electrónico. Está diseñado para detectar y bloquear una amplia variedad de amenazas transmitidas por correo electrónico, como malware, spam e intentos de phishing.

Observaciones

CCN-STIC 1623 Procedimiento de Empleo Seguro Cisco Email Security Appliance

FortiMail Appliances FML-200F, FML-400F, FML-900F, FML-VM (appliance virtual)	
Versión	Firmware 6.2
Fabricante	Fortinet
Familia	Protección de correo electrónico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	09/02/2024
Descripción	

Sistema de seguridad de correo electrónico que proporciona una protección multicapa contra spam, virus, gusanos y spyware. El motor de filtrado empleado en FortiMail bloquea el spam y el malware antes de que pueda afectar a las redes y usuarios.
Advertencia:
Las funcionalidades de Single Sing-on, DLP y FortiIsolator no han sido evaluadas y, por tanto, no se consideran cualificadas.

Observaciones

CCN-STIC-1614 Procedimiento de empleo seguro Fortimail

8.7.4 HIPERCONVERGENCIA

KATUA SDI PLATFORM	
Versión	1.0
Fabricante	KRC ESPAÑOLA S.A.
Familia	Hiperconvergencia
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2021
Revisión de Validez	29/02/2024

Descripción

Katua®SDI Platform es una plataforma hiperconvergente escalable y segura, basada en el concepto Software Define Infraestructure, donde todos los elementos que conforman un CPD se definen en una única plataforma hardware y software. Permite el despliegue rápido de servicios (xaaS), consolidación de CPDs, SDN y tiene capacidad de instalación desde equipos móviles hasta grandes centros de procesos de datos. Su flexibilidad permite que se puedan desplegar servicios cloud sobre la plataforma de forma sencilla y eficiente. Dispone de la capacidad para generar bibliotecas de sistemas preconfigurados para su despliegue con un click a través de su interfaz web. Las capacidades de optimización del hipervisor aseguran un rendimiento máximo de la plataforma, haciendo uso de todos los recursos disponibles y ofreciendo de esta forma capacidad de instalación en nodos pequeños y configuraciones hardware básicas. Su capacidad para integrarse con sistemas de almacenamiento masivos, ya sean locales o remotos permite escalar la solución en función de las necesidades. Para más información de la plataforma, vista nuestra web https://www.krc.es

Observaciones

CCN-STIC-1610 Procedimiento de Empleo Seguro KATUA SDI Platform

8.8 OTRAS HERRAMIENTAS

8.8.1 OTRAS HERRAMIENTAS

authUsb safeDoor	
Versión	2.0.0.8
Fabricante	authUSB
Familia	Otras Herramientas
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2019
Revisión de Validez	31/12/2023

Descripción

AuthUsb safeDoor es un dispositivo hardware que actúa como barrera entre las memorias USB y los equipos de una organización, identificando amenazas a tres niveles: -Eléctrico: identificando y deteniendo ataques destructivos de sobretensión tipo UsbKiller. -Hardware: detectando y desactivando ataques de la familia BadUsb, ataques HID (rubber ducky y similares), falsas tarjetas de red, interfaces compuestas, etc. -Software: antivirus integrado que realiza un análisis previo a la descarga de cualquier contenido.

Observaciones

CCN-STIC 1201 Procedimiento de empleo seguro AuthUsb SafeDoor

8.9 COMUNICACIONES TÁCTICAS SEGURAS

8.9.1 PLATAFORMAS Y DISPOSITIVOS TÁCTICOS CONFIABLES

GETAC F110	
Versión	G6 con firmware 15.0.35.1951
Fabricante	GETAC
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/10/2023
Revisión de Validez	14/10/2025

Descripción

Tableta robusta diseñada para dar soporte a usuarios civiles y militares. Este dispositivo se considera una plataforma confiable donde ejecutar aplicaciones software de forma protegida (p.ej.: aplicaciones de mando y control). El sistema operativo de la tableta es Windows 10 IoT Enterprise 21H2 LTSB. La tableta incluye un TPM 2.0.

Observaciones

CCN-STIC-1628 Procedimiento de empleo seguro GETAC F110G6

GETAC F110	
Versión	G5 con firmware GETAC 12.0.45.1509
Fabricante	GETAC
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/06/2021
Revisión de Validez	14/10/2025

Descripción

Tableta robusta diseñada para dar soporte a usuarios civiles y militares. Este dispositivo se considera una plataforma confiable donde ejecutar aplicaciones software de forma protegida (p.ej.: aplicaciones de mando y control). El sistema operativo de la tableta es Windows 10 Enterprise 1607 LTSB. La tableta incluye un TPM 2.0.

Observaciones

Configuración y empleo seguro según la CCN-STIC-1609. Para protección de las comunicaciones en tránsito es necesario un producto aprobado perteneciente a la familia “soluciones para protección de las comunicaciones tácticas”.

GETAC F110

Versión	G4 con firmware GETAC R1.12.070520
Fabricante	GETAC
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/06/2019
Revisión de Validez	14/10/2025

Descripción

Tableta robusta diseñada para dar soporte a usuarios civiles y militares. Este dispositivo se considera una plataforma confiable donde ejecutar aplicaciones software de forma protegida (p.ej.: aplicaciones de mando y control). El sistema operativo de la tableta es Windows 10 Enterprise 1607 LTSB. La tableta incluye un TPM 2.0.

Observaciones

Configuración y empleo seguro según la CCN-STIC-1605. Para protección de las comunicaciones en tránsito es necesario un producto aprobado perteneciente a la familia “soluciones para protección de las comunicaciones tácticas”.

HP Elitebook 840

Versión	G7 y G8
Fabricante	HP PRINTING AND COMPUTING SOLUTIONS SL
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/09/2021
Revisión de Validez	29/02/2024

Descripción

Equipos portátiles con sistema operativo Windows 10 Enterprise, Versión 20H2, Compilación (19042.1023) securizable mediante la aplicación de las guías STIC para manejo de información clasificada.

Observaciones

Plataforma bastionada según CCN-STIC 599B19

8.9.2 SOLUCIONES PARA PROTECCIÓN DE LAS COMUNICACIONES TÁCTICAS

Bittium Tough SDR Handheld – Soldier Radio	
Versión	9400132
Fabricante	Bittium
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/08/2021
Revisión de Validez	30/06/2024

Descripción

El producto Bittium Tough SDR Handheld es una radio táctica militar V-UHF de mano basada en tecnología SDR conforme a la arquitectura ESSOR SCA. Esta radio, en función de la forma de onda empleada, proporciona diferentes servicios de comunicaciones de voz y datos con unas prestaciones determinadas en términos de ancho de banda, alcance, número de nodos soportados en la red radio, etc. La Tough SDR Handheld cubre la banda de frecuencias desde 30 MHz hasta 2,5 GHz y puede ejecutar formas de onda tanto de banda estrecha como de banda ancha, las cuales incluyen diferentes mecanismos de protección COMSEC, TRANSEC y NETSEC. La aprobación para la protección de información clasificada nacional de grado DIFUSIÓN LIMITADA es aplicable cuando el producto se emplee con la forma de onda ESSOR High Data Rate Waveform.

Observaciones

Utilización según el PE-2021-21 “Procedimiento de empleo seguro de la radio táctica Bittium Tough SDR Hand-Held”

TZ-2001R-MC	
Versión	SW 1.8 y 1.8.1
Fabricante	TECNOBIT
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/02/2023
Revisión de Validez	30/06/2025

Descripción

El TZ-2001R-MC es una aplicación de cifrado software para sistemas Windows que se ejecuta como un servicio del Sistema Operativo a disposición de otras aplicaciones (típicamente aplicaciones de mando y control). Proporciona las siguientes capacidades de cifrado:
a) Cifrado de voz táctica ("push to talk") según varios estándares (SCIP multipunto, STaC-IS 2400, TSVCIS 600, TSVCIS 1200, TSVCIS 600/2400 y TSVCIS 1200/2400).
b) Cifrado de datos IP en modo transporte (solo "payload"), estando disponible un modo autenticado (AES-GCM) y un modo no autenticado (AES-CTR).
c) Cifrado no autenticado (AES-CTR) de los datos DAP del Sistema BMS-ET que se transmiten por el TDMA de la radio F@stnet PR4G.
En sus modos de cifra de voz táctica y datos IP, el TZ-2001R-MC es interoperable con otros productos de la familia CIFPECOM, tales como el TZ-1001R o la Unidad de Comunicaciones Seguras con módulo de seguridad TZ-501. El TZ-2001R-MC se configura con el mismo centro de gestión (CMAP) que el TZ-1001R y el TZ-501.

Observaciones

Según su procedimiento de empleo, el TZ-2001R-MC deberá ejecutarse sobre una plataforma Windows cualificada como confiable, o en su defecto en una estación de trabajo bastionada conforme a lo requerido en la CCN-STIC-599 para manejar información DIFUSIÓN LIMITADA. La mayor parte de las funciones de seguridad lógica residen en la plataforma Windows que se emplee. Utilización según el Procedimiento de Empleo Seguro T00741700PDE001 Ed. 01.

Bittium SafeMove VPN Client for Android	
Versión	Android (genérico): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb
Fabricante	Bittium
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/06/2024

Descripción

SafeMove Mobile VPN forma parte de la Bittium Secure Suite. Proporciona los servicios de firewall y VPN IPSec a las plataformas Android y Windows conectadas de forma remota a la infraestructura corporativa, y está concebido para ser un servicio siempre activo y aplicado a todo el tráfico de red que entra y sale del dispositivo. Nada sensible se escapa, nada dañino puede entrar. La SafeMove Mobile VPN es una solución cliente-servidor. El cliente instalado en el dispositivo se conecta a la puerta de enlace Bittium SafeMove VPN Gateway instalada en el servidor, con el resto de los componentes de la Bittium Secure Suite, que son el gestor de dispositivos (MDM), el gestor de las aplicaciones instaladas en los dispositivos (solo Android) y los servicios de comprobación de la integridad (solo Android). Usado en combinación con los smartphones de la familia Bittium Tough Mobile proporciona servicios de recuperación de los registros de auditoría y actualización OTA del firmware de los dispositivos. Más información de Bittium SafeMove® Mobile VPN: https://www.bittium.com/secure-communications-connectivity/bittium-safemove-mobile-vpn

Observaciones

PE-2021-7-Procedimiento de empleo seguro Bittium SafeMove VPN (Android y Windows)

TZ-1001R	
Versión	V4.26
Fabricante	TECNOBIT
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/10/2020
Revisión de Validez	31/12/2023

Descripción

El TZ-1001R es un cifrador táctico de pequeño tamaño para la protección de las comunicaciones sobre redes de bajo ancho de banda y sin estabilidad de enlace garantizada. Cuenta con dos modos de operación diferenciados: como cifrador en línea (modo “tactical crypto”), o alternativamente en modo “slave crypto” como elemento de cifra esclavo de otro elemento que gestiona la interacción con los medios de transmisión y con el usuario (caso del Gestor de Comunicaciones del ET). El TZ-1001R tiene capacidad para cifrar de forma simultánea varios flujos de voz táctica (“push to talk”) según varios estándares OTAN, pudiendo elegirse en cada caso el más adecuando según el tipo de radio por el que se va a realizar la transmisión. Simultáneamente también puede cifrar datos IP unicast y multicast. Cuando el cifrador se configura en modo “tactical crypto” implementa IPSec con asociaciones de seguridad manuales. En configuración “slave crypto” el TZ-1001R implementa un protocolo específico de cifra IP para facilitar la integración con los sistemas CIS de dotación. En modo “slave crypto” la cifra del TZ-1001R es interoperable con la cifra del TZ-501 (módulo de seguridad de la UCS) y con la aplicación de cifrado para S.O. Windows TZ-2001.

Observaciones

Utilización según el Procedimiento de empleo T90431000PDE003 v2.0

Bittium SafeMove VPN Client for Windows

Versión	4.11.722
Fabricante	Bittium
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/06/2024

Descripción

SafeMove Mobile VPN forma parte de la Bittium Secure Suite. Proporciona los servicios de firewall y VPN IPSec a las plataformas Android y Windows conectadas de forma remota a la infraestructura corporativa, y está concebido para ser un servicio siempre activo y aplicado a todo el tráfico de red que entra y sale del dispositivo. Nada sensible se escapa, nada dañino puede entrar. La SafeMove Mobile VPN es una solución cliente-servidor. El cliente instalado en el dispositivo se conecta a la puerta de enlace Bittium SafeMove VPN Gateway instalada en el servidor, con el resto de los componentes de la Bittium Secure Suite, que son el gestor de dispositivos (MDM), el gestor de las aplicaciones instaladas en los dispositivos (solo Android) y los servicios de comprobación de la integridad (solo Android). Usado en combinación con los smartphones de la familia Bittium Tough Mobile proporciona servicios de recuperación de los registros de auditoría y actualización OTA del firmware de los dispositivos. Más información de Bittium SafeMove® Mobile VPN: https://www.bittium.com/secure-communications-connectivity/bittium-safemove-mobile-vpn

Observaciones

PE-2021-7-Procedimiento de empleo seguro Bittium SafeMove VPN (Android y Windows)

COMSec Admin +

Versión	v4.2
Fabricante	Indra
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/12/2023

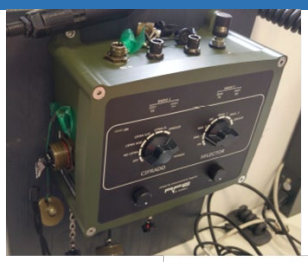
Descripción

COMSec Admin+ es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital. Con su alto nivel de seguridad, gran calidad de audio y facilidad de uso protege de forma eficaz información clasificada (hasta difusión limitada) de la organización. Las llamadas y los datos intercambiados por COMSec son seguros, independientemente del operador móvil utilizado y el país donde se encuentre. Más información: comsec.indracompany.com

Observaciones

Utilización según el PE-2018-24 Procedimiento de empleo COMSec Admin + v2 Para su empleo en entornos tácticos o desplegables, este producto deberá emplearse sobre un dispositivo móvil perteneciente a la familia “plataformas y dispositivos tácticos confiables"

Unidad de Comunicaciones Seguras (UCS) con módulo de seguridad TZ-501



Versión	UCS v2.4 con TZ-501 (versión SW 4.26)
Fabricante	TECNOBIT y RF Española
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/09/2021
Revisión de Validez	31/12/2023

Descripción

La UCS es un gestor de comunicaciones para su uso en entornos tácticos militares en los que se requiere contar con comunicaciones seguras tanto de voz táctica CNR como de de datos IP. La UCS permite la conexión de varias radios tácticas, u otros medios CIS, que actuan como medio de transporte. El sistema incorpora un módulo de gestión de radiofonía, un módulo para la gestión de la interfonía y un servidor de telefonía de Voz IP para la integración con equipos telefónicos SIP, todo ello acompañado de un módulo de cifrado seguro, denominado TZ-501. El TZ-501 es el módulo encargado de cifrar la voz táctica según estándares OTAN, así como los datos IP unicast y multicast. La UCS cuenta con una “Crypto Ignition Key” (CIK) para el arranque seguro del equipo, y que además facilita el transporte y almacenamiento del equipo (sin la CIK la UCS se considera un equipo no clasificado). La cifra del TZ-501 es compatible con la cifra del TZ-1001R en modo “slave-crypto” y con la cifra del TZ-2001.

Observaciones

Utilización según el Procedimiento de Empleo Seguro T00741600PDE001 V3

8.10 TEMPEST

8.10.1 ARMARIOS APANTALLADOS

P.AT07D	
Versión	_
Fabricante	CONSUEGRA S. COOP.
Familia	Armarios apantallados
Tipo	Producto
Clasificación	Apto ZONA 0
Fecha Inclusión	01/04/2019
Revisión de Validez	31/10/2024

Descripción

Armario Tempest de sobremesa de dimensiones reducidas con dos posibles opciones. El armario PAT 07D ofrece alta protección electromagnética para que el cliente incluya su propia CPU, convirtiendo el conjunto en una CPU Tempest aceptada para procesar información clasificada en locales ZONA 0. CONSUEGRA se ocupa de las adaptaciones necesarias para su correcta instalación y funcionamiento. Posteriormente, si el cliente deseara cambiar la CPU por una más actualizada, CONSUEGRA también puede ocuparse de su instalación y funcionamiento. CONSUEGRA también ofrece la posibilidad de suministrar e instalar la CPU solicitada por el cliente como parte del pedido, en este caso, el producto se codifica como P.COMPT0-03.

Observaciones

P.AT-06E	
Versión	
Fabricante	CONSUEGRA S. COOP.
Familia	Armarios apantallados
Tipo	Producto
Clasificación	Apto ZONA 0
Fecha Inclusión	01/12/2017
Revisión de Validez	30/06/2024

Descripción

Armario apantallado ciego de 38U. Dimensiones 2102x625x1000 mm. Ventilación a través de 2 ventiladores con termostatos independientes con caudal de hasta 2.700 m3/h. Distribuidor interno con diferencial y automático. Apto para instalación en locales con clasificación de ZONA 0.

Observaciones

P.AT-02D

Versión

Fabricante CONSUEGRA S. COOP.

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2024

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-07

Versión _

Fabricante CONSUEGRA S. COOP.

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2024

Descripción

Armario apantallado para CPU. Dispone de bandeja extraible, ventilación y filtrado de las líneas de datos y alimentación. Apto para instalación en locales con clasificación ZONA 0.

Observaciones

SHATEM - SHELTER ARPA TEMPEST MULTIPROPOSITO

Versión

Fabricante ARPA, EQUIPOS MÓVILES DE CAMPAÑA

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0

Fecha Inclusión 01/01/2020

Revisión de Validez 31/05/2024

Descripción

Contenedor shelter para alojamiento y/o operación de equipos informáticos, electrónicos, optrónicos de telecomunicaciones y asimilables para entornos CIS. Equipado con los elementos de filtrado y protección EMI necesarios en acometidas de potencia, datos y servicios para disponer de apantallamiento intergral TEMPEST frente a emanaciones comprometedoras radiadas y conducidas.

Observaciones

P.AT-06D

Versión

Fabricante CONSUEGRA S. COOP.

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2024

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

8.10.2 MONITORES

P.MONT0-11	
Versión	_
Fabricante	CONSUEGRA S. COOP.
Familia	Monitores
Tipo	Producto
Clasificación	SDIP-27 Level A
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024
Descripción	

Monitor LED Full HD de 22" y resolución 1920 x 1080p con formato panorámico.

Observaciones

8.10.3 PERIFÉRICOS

P.RATT0-04

Versión _
Fabricante CONSUEGRA S. COOP.
Familia Periféricos
Tipo Producto
Clasificación SDIP-27 Level A
Fecha Inclusión 01/12/2017
Revisión de Validez 31/05/2024
Descripción

Ratón óptico USB
Observaciones

P.KVMT0-01

Versión
Fabricante CONSUEGRA S. COOP.
Familia Periféricos
Tipo Producto
Clasificación SDIP-27 Level A
Fecha Inclusión 01/12/2017
Revisión de Validez 31/05/2024
Descripción

Conmutador KVM para dos sistemas. Basado en BELKIN SECURE OMNIVIEW F1DN102Uea con certificación NIAP EAL 4+.
Observaciones

P.TECT0-07	
Versión	
Fabricante	CONSUEGRA S. COOP.
Familia	Periféricos
Tipo	Producto
Clasificación	SDIP-27 Level A
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2024
Descripción	
Teclado QWERTY español. Conexión USB.	
Observaciones	

8.10.4 CPU

P.COMPT0-06

Versión _

Fabricante CONSUEGRA S. COOP.

Familia CPU

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 01/12/2021

Revisión de Validez 31/05/2024

Descripción

CPU de sobremesa tempestizada del modelo comercial HP PRODESK 600 G5 SFF. Aprobado para su uso combinado con periféricos TEMPEST de la empresa CONSUEGRA S.COOP. en locales con clasificación de ZONA 0.

Observaciones

P.COMT0-01

Versión -

Fabricante CONSUEGRA S. COOP.

Familia CPU

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 01/06/2018

Revisión de Validez 31/12/2023

Descripción

CPU de sobremesa tempestizada del modelo comercial HP ELITE 8000. Aprobado para su uso combinado con periféricos TEMPEST de la empresa CONSUEGRA S. COOP. en locales con clasificación de ZONA 0.

Observaciones

8.10.5 IMPRESORAS

P.IMPT0-04

Versión _

Fabricante CONSUEGRA S. COOP.

Familia Impresoras

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 01/12/2021

Revisión de Validez 31/05/2024

Descripción

Impresora TEMPEST basada en el model HP Color LaserJet Enterprise M553dn.

Observaciones

8.10.6 SERVIDOR

SOC-1-TP	
Versión	-
Fabricante	KRC ESPAÑOLA S.A.
Familia	Servidor
Tipo	Producto
Clasificación	SDIP-27 Level A
Fecha Inclusión	15/10/2023
Revisión de Validez	26/10/2025

Descripción

Servidor multipropósito de alto rendimiento orientado a despliegues en entornos móviles, donde el consumo y el espacio son elementos críticos.
Sus capacidades le permiten actuar como servidor multifuncional e incluso ofrecer servicios de virtualización en una red con requerimientos medios. Compatible con distintos sistemas operativos.

Observaciones

N/A

9. PRODUCTOS Y SERVICIOS DE CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD

PRODUCTOS Y SERVICIOS DE CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD

9.1 CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD

9.1.1 GOBERNANZA Y PLANIFICACIÓN DE LA SEGURIDAD

LightHouse Vulnerability Manager	
Versión	n/a
Fabricante	INNOTEC SYSTEM
Familia	Gobernanza y Planificación de la Seguridad
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/04/2023
Revisión de Validez	31/03/2025

Descripción

LightHouse VM (Vulnerability Management) de Innotec Security es la plataforma de auditoría continua para la detección y priorización de riesgos de una organización, permitiendo optimizar esfuerzos y personalizar la gestión, acortando el tiempo de exposición frente a las amenazas.
LightHouse es la herramienta perfecta para la gestión de vulnerabilidades y la reducción de la superficie de exposición de los organismos minimizando los tiempos de gestión a través de una eficiente detección de vulnerabilidades y notificación de alertas, así como, ofreciendo recomendaciones para un tratamiento oportuno de estas.
Con su enfoque Asset Centric, LightHouse VM permite, entre otros:
- Gestionar vulnerabilidades durante su ciclo de vida.
- Obtener el nivel de riesgo de una organización.
- Alertar y evaluar el riesgo de una organización de forma temprana.
- Agrupar en grupos lógicos de gestión a medida.
- Planificar los ciclos de revisión de vulnerabilidades.
- Medir el nivel de desempeño en la mitigación de las vulnerabilidades con sus cuadros de mandos de seguimiento y SLAs.
- Integrarse con sistemas de escaneo líderes del mercado y las principales herramientas de ticketing para la gestión directa de las vulnerabilidades.

Observaciones

No aplica Procedimiento de Empleo Seguro

9.1.2 NORMATIVA DE SEGURIDAD Y CONFORMIDAD

CLARA ENS WINDOWS	
Versión	2.0.2.1
Fabricante	Centro Criptológico Nacional
Familia	Normativa de Seguridad y Conformidad
Tipo	Producto
Categoría ENS	N/A
Fecha Inclusión	01/10/2021
Revisión de Validez	30/04/2024

Descripción

CLARA es una herramienta para analizar las características de seguridad técnicas en equipos Windows definidas por el Esquema Nacional de Seguridad. El análisis del cumplimiento está basado en las normas proporcionadas a través de las plantillas de seguridad de las guías de configuración segura de equipos Windows (la CCN-STIC-599, entre otras).

Observaciones

Para más información, contactar con clara@ccn-cert.cni.es.

9.1.3 ANÁLISIS Y GESTIÓN DE RIESGOS

Archer Suite	
Versión	6.11 (con IRM Mobile v1.4)
Fabricante	RSA
Familia	Análisis y Gestión de Riesgos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2023
Revisión de Validez	29/02/2024

Descripción

Archer es una solución de Gestión Integral de Riesgos (o también conocida como GRC) que permite unificar las actividades de gobierno corporativo, riesgo y cumplimiento de normas en una sola plataforma integrada. Actúa como una protección perimetral para aplicar una cultura de administración de riesgo y responsabilidad compartida en toda la institución. Les permite instituir programas eficaces para fomentar las mejores prácticas y estandarizar los procesos directamente a través de su tecnología. Tiene plena visibilidad para responder preguntas de la junta directiva y generar claridad entorno al estado del cumplimiento de normas y de los riesgos para toda la institución. Contamos con modalidad servicio SaaS y también on-premises.
Dentro de Archer, los dominios de riesgo principales que se cubren son:
• Gestión de Riesgos de Seguridad e IT (incluyendo gestión para cumplimiento del ENS)
• Continuidad de Negocio y Resiliencia Operacional
• Gestión de Riesgos de Terceros
• Cumplimiento (incluyendo GDPR)
• Gestión de Riesgo Operacional
• Auditoría Interna
• ESG (Environmental, Social and Governance)
• Cuantificación de Riesgos
Para más información: https://www.archerirm.com/

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

9.1.4 NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES

LUCIA	
Versión	4.1
Fabricante	Centro Criptológico Nacional
Familia	Notificación y Gestión de Ciberincidentes
Tipo	Producto
Categoría ENS	N/A
Fecha Inclusión	01/10/2021
Revisión de Validez	30/04/2024

Descripción

LUCIA es una herramienta para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Con ella, se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora. LUCIA ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el seguimiento del mismo. El sistema permite, además, automatizar las tareas e integrarse con otros sistemas ya implantados.

Observaciones

Para más información, contactar con lucia@ccn-cert.cni.es.

9.1.5 FORMACIÓN Y CONCENCIACIÓN

SMARTFENSE	
Versión	3 y 4
Fabricante	Defense Balance
Familia	Formación y Concenciación
Tipo	Servicio
Categoría ENS	N/A
Fecha Inclusión	01/10/2022
Revisión de Validez	31/10/2024

Descripción

SMARTFENSE es la plataforma online de concienciación en Seguridad de la Información que permite generar comportamientos seguros en los usuarios, favoreciendo la creación de una cultura cibersegura. SMARTFENSE provee catálogos de contenidos predefinidos 100% editables para adecuarse a la cultura de la organización y además, posibilita la creación de contenido propio. Ofrece también herramientas de simulación de Phishing y Ransomware para medir la efectividad de las acciones realizadas y conocer la evolución en las respuestas de los usuarios.

Observaciones

No aplica la publicación de procedimiento de empleo seguro.

PSAT – Proofpoint Security Awareness Training

Versión	-
Fabricante	Proofpoint
Familia	Formación y Concenciación
Tipo	Servicio
Categoría ENS	N/A
Fecha Inclusión	01/03/2022
Revisión de Validez	31/03/2024

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

Ángeles

Versión	1.0
Fabricante	CSA
Familia	Formación y Concenciación
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/09/2023
Revisión de Validez	31/08/2024

Descripción

Ángeles, plataforma de formación, capacitación y talento en ciberseguridad, con una oferta formativa completa, incluyendo cursos online, webinars y diferente documentación en función del perfil del usuario. La plataforma, disponible en Google Play y App Store, dispone de un área privada, con acceso a través del sistema Cl@ve, desde el que acceder al expediente de cada alumno, con las horas de formación recibidas, así como los cursos y sesiones de concienciación realizadas en la plataforma.

Observaciones

N/A

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