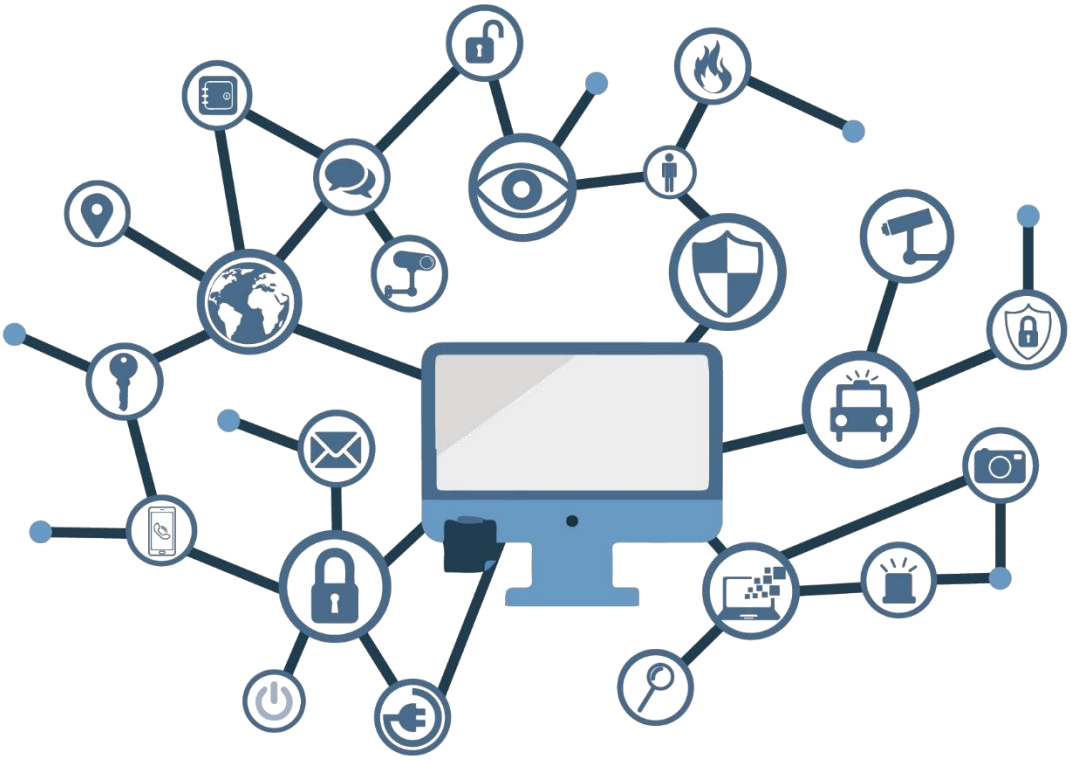
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 105

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



Enero de 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.01.30 12:32:37 +01'00'

NIPO: 083-19-031-4

Fecha de Edición: Enero de 2020

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

PRÓLOGO

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

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

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

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

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

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

Julio de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1 INTRODUCCIÓN

1. La adquisición de un producto de seguridad TIC que va a manejar información nacional clasificada o información sensible debe estar precedida de un proceso de comprobación de que los mecanismos de seguridad implementados en el producto son adecuados para proteger dicha información.

2. La evaluación y certificación de un producto de seguridad TIC es el único medio objetivo que permite valorar y acreditar la capacidad de un producto para manejar información de forma segura. En España, esta responsabilidad está asignada al Centro Criptológico Nacional (CCN) a través del RD 421/2004 de 12 de marzo en su Artículo 1 y en su Artículo 2.1, el cual establece que el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y la comunicación y autoridad de certificación criptológica.

3. Así mismo, dentro del RD 3/2010 de 8 de enero, modificado por el RD 951/2015, de 23 de octubre, 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 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 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 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 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 partes: **Productos Aprobados** y **Productos 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 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	INFORMACIÓN QUE MANEJA
APROBADO	CLASIFICADA
CUALIFICADO	SENSIBLE (ENS)

Tabla 1. Tipos de productos 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 o 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 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 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 en el catálogo, el CCN tendrá en cuenta los siguientes criterios:

    a) En el caso **Productos Aprobados** para el manejo de información clasificada, el máximo nivel de clasificación de la información que puede manejar (Difusión Limitada, Confidencial, Reservado, Secreto).

    b) En el caso de **Productos Cualificados**, la máxima categoría del sistema de información en el que puede emplearse (Alta, Media, Básica[1]).

    c) Las funcionalidades de seguridad que implementa el producto y las certificaciones aportadas.

[1] Clasificación por categorías definida en el ENS.

d) Otros aspectos como el análisis de riesgos del producto o sistema, la necesidad operativa dentro de la Administración, la disponibilidad o no de otros productos certificados que satisfagan la misma funcionalidad, etc.

En función de esta información, se determinarán las pruebas o evaluaciones que deberá superar el producto 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** [REF5]. Ver Figura 1.

14. Así mismo, el procedimiento de inclusión de un producto de seguridad TIC cualificado en el CPSTIC se describe en la presente guía CCN-STIC 106, los requisitos fundamentales de seguridad o los perfiles de protección que deben cumplir los productos de seguridad TIC en función de su taxonomía se detallan en la guía **CCN-STIC 140 Taxonomías de referencia para productos de seguridad TIC** [2] y la descripción detallada del flujo, así como los tiempos máximos del proceso se describen en el Procedimiento de cualificación de productos STIC en el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) **PO-09 Procedimiento de cualificación de productos STIC en el ENECSTI** [5]. Ver Figura 1.

15. El producto de seguridad TIC cualificado por el CCN hará referencia a una versión concreta y con una configuración determinada, de acuerdo a unas normas de utilización que serán descritas en un procedimiento de empleo. 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.

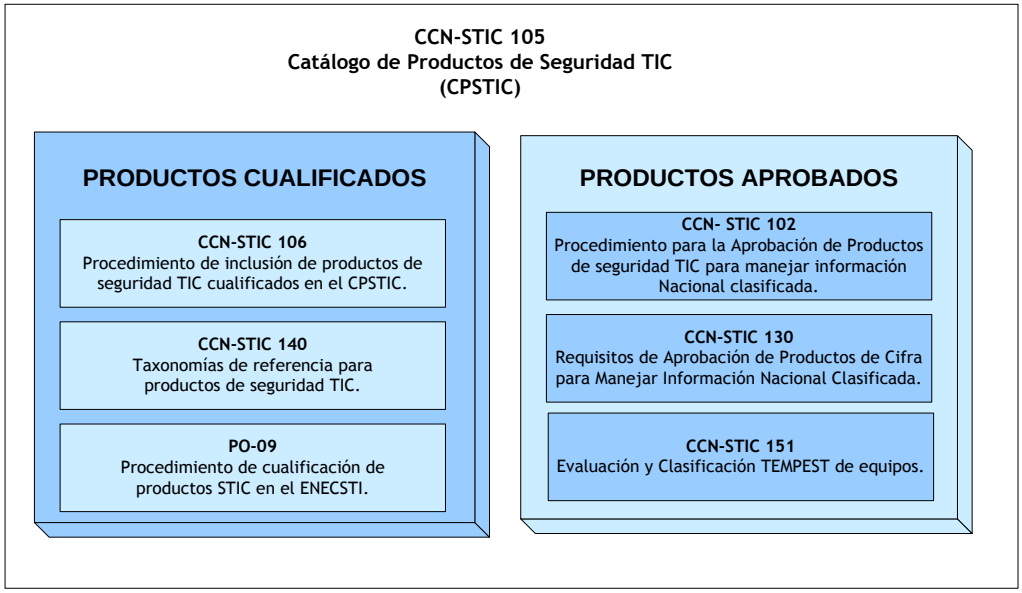


Figura 1. Inclusión de productos de seguridad en el CPSTIC.

5 REVISIÓN DE VALIDEZ DE PRODUCTOS STIC

16. Periódicamente se realizará una revisión de validez de los productos 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.

17. Por esta razón, tras una revisión de validez, un producto 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 DEL CPSTIC

18. Un producto podrá ser excluido del CPSTIC por cualquiera de los siguientes motivos:

    a) Caducidad de su certificado de Producto Cualificado de Seguridad TIC. Todos los certificados de productos cualificados serán emitidos con una fecha de caducidad (que dependerá de la familia de productos considerada y como norma general será de 2 años), 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 del CPSTIC.

    b) Revocación de la certificación CC. En el caso de que fuese revocada la certificación CC de un determinado producto, éste podrá ser excluido del catálogo.

    c) Pérdida de las condiciones de excepcionalidad. En el caso de que el producto 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 sustitutivos con la certificación CC adecuada, pérdida de la consideración de producto 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) El producto presenta vulnerabilidades críticas no corregidas. En el caso de que se detecten vulnerabilidades críticas que afecten al producto, podrá solicitarse al fabricante un informe de impacto de dicha vulnerabilidad. Si éste informe determinase que la vulnerabilidad es explotable siguiendo el procedimiento de empleo del producto, éste será excluido del catálogo.

PRODUCTOS CUALIFICADOS

7 PRODUCTOS CUALIFICADOS

7.1 CATEGORÍA: CONTROL DE ACCESO

7.1.1 FAMILIA: CONTROL DE ACCESO A RED (NAC)

ClearPass Policy Manager (C1000, C2000, C3000)	
Versión	6.7.3
Familia	Control de acceso a red (NAC)
Fabricante	Aruba
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	30/01/2020

Descripción

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

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

OpenNAC Enterprise

Versión V1.2

Familia Control de Acceso a Red (NAC)

Fabricante OpenCloud Factory

Categoría ENS ALTO

Fecha Inclusión 01/12/2018

Revisión de Validez 31/05/2021

Descripción

OpenNAC Enterprise , Network Access Control de nueva generación con capacidad para poder gestionar de manera segura el acceso a las redes corporativas y así poder obtener el control total sobre la red. Disponible como Virtual Appliance, permite su puestaen marcha en grandes redes corporativas con diversos centros de datos y oficinas remotas. OpenNAC Enterprise utiliza múltiple métodos de descubrimiento de dispositivos (802.1x, Traps, Agente..); el Sensor (sonda) admite la visibilidad de activos sin 802.1X y logra una inspección profunda de paquetes fuera de banda. La solución proporciona soporte multi-vendor para infraestructura de red, basado en múltiples métodos de autenticación y enforcement a través de la segmentación (VLAN), microsegmentación etc. Puede integrarse con múltiples LDAPs y Directorios Activos. Es una solución completamente modular en función de la necesidad de las organizaciones. www.opencloudfactory.com https://www.opencloudfactory.com/solucion-opennac/

Observaciones

Procedimiento de empleo pendiente de publicación.

Pulse Policy Secure (PSA-300, PSA-3000, PSA-5000, PSA-7000c/f , PSA-V)

Versión 5.3R12.1

Familia Control de Acceso a Red (NAC)

Fabricante Pulse Secure

Categoría ENS ALTO

Fecha Inclusión 01/04/2019

Revisión de Validez 31/03/2020

Descripción

La solución de control de acceso corporativo Pulse Policy Secure (PPS) incorpora tanto elementos de perfilado de elementos de red como de cumplimiento de políticas de seguridad corporativa (NAC). Permite autenticar tanto usuarios (RBAC), sistemas u otrosdispositivos (802.1x, Radius, TACACS+) dentro del entorno corporativo, como el posterior enforcement (802.1x, SNMP).
Se integra de forma nativa con diferentes elementos corporativos como pueden ser MDMs, Firewalls o Switches dentro del entorno, para así hacer cumplir las normativas de seguridad y el control de acceso.
Incorpora la capacidad de federación de perfiles de usuarios con terceros como pueden ser la solución de VPN (PCS) de Pulse Secure o diferentes Firewalls a través de diferentes tecnologías (syslog, IF-MAP, API) permitiendo así elevar la seguridad y el manejo del control de acceso a niveles corporativos.
La solución incluye también funcionalidades de detección especificas para entornos IoT, así como capacidades de análisis de comportamiento (Behaviour Analytics) como una integración avanzada para el análisis de Host (Hostchecker; con o sin Agente), elevando de esta manera el grado de seguridad en las redes corporativas y protegiéndolas contra elementos no autorizados & autenticados (RADIUS, A

Observaciones

Procedimiento de empleo pendiente de publicación.

7.1.2 FAMILIA: DISPOSITIVOS BIOMÉTRICOS

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

7.1.3 FAMILIA: DISPOSITIVOS SINGLE SIGN-ON

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

7.1.4 FAMILIA: SERVIDORES DE AUTENTICACIÓN

ClearPass Policy Manager (C1000, C2000, C3000)

Versión	6.7.3
Familia	Servidores de Autenticación
Fabricante	Aruba
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	30/01/2020

Descripción

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

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

7.1.5 FAMILIA: DISPOSITIVOS ONE-TIME PASSWORD

Pendiente de publicación los Requisitos Fundamentales de Seguridad (RFS) de esta familia.

7.1.6 FAMILIA: GESTIÓN DE ACCESO PRIVILEGIADO (PAM)

CyberArk Privileged Account Security Solution	
Versión	9.1
Familia	Gestión de acceso privilegiado (PAM)
Fabricante	CyberArk
Categoría	ENS ALTO
Fecha Inclusión	1/05/2019
Revisión de Validez	30/04/2020

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.

• 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.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

Thycotic Secret Sever Government Edition	
Versión	10.1
Familia	Gestión de acceso privilegiado (PAM)
Fabricante	Thycotic
Categoría	ENS ALTO
Fecha Inclusión	1/05/2019
Revisión de Validez	30/04/2020

Descripción

Thycotic Secret Server es una solución de gestión de cuentas privilegiadas que permite descubrir, securizar, administrar y auditar contraseñas, credenciales así como monitorizar y grabar las sesiones privilegiadas. Permite gestionar el acceso a cada cuenta privilegiada y activo crítico, automatizar las mejores prácticas de seguridad y cumplir las regulaciones normativas.

Las capacidades de PAM de Secret Server para la administración de las cuentas privilegiadas incluyen:

- Gestión del Ciclo de Vidade las credenciales con privilegios:
  - Descubrimiento Automatizado de cuentas privilegiadas y "onboarding" de las mismas en un Repositorio central seguro
  - Rotado automático de las credenciales y Gestión, control y auditoria de las sesiones privilegiadas
- Análisis del comportamiento del usuario privilegiado
- Gestión de cuentas de servicio
- Políticas de acceso basadas en RBAC y Gestión de políticas de seguridad.
- Arquitectura escalable. Alta Disponibilidad y DR. Integración con múltiples plataformas Out-Of-The-Box
- Módulo de Reporting capaz de generar informes totalmente a medida
- Securización de los procesos de DevOps.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

7.2 CATEGORÍA: EXPLOTACIÓN DE LA SEGURIDAD

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

McAfee Endpoint Security	
Versión	10.1.0 with ePolicy Orchestrator 5.3.1
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Fabricante	McAfee
Categoría	ENS ALTO
Fecha Inclusión	01/10/2018
Revisión de Validez	31/03/2020

Descripción

McAfee Endpoint Security es una solución de protección del EndPoint de última generación, integra varias tecnologías del ciclo de vida de las defensas frente a amenazas. Utiliza un solo agente y consola de administración centralizada para que las operaciones de seguridad sean ágiles. Principales características:
1) Prevención de amenazas fundamental mediante uso de los fundamentales antivirus, prevención de exploits, firewall y control web que se inter comunican,
2) Aprendizaje automático mediante técnicas punteras que identifican el código malicioso analizando sus atributos estáticos y de comportamiento,
3) Contención de aplicaciones para limitar el impacto de los archivos sospechosos y el malware zero-day. Bloquea los comportamientos maliciosos y los detiene antes de que infecten o se extiendan en el entorno.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Panda Adaptive Defense 360

Versión	3.25.00 (Protection Agent v8.0)
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Fabricante	Panda Security
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

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 cubrentodas 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

Procedimiento de empleo seguro pendiente de publicación.

Symantec Endpoint Protection Mobile

Versión	iOS versión 8.0 o superior Android 4.0 o superior
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Fabricante	Symantec Corporation
Categoría	ENS MEDIO
Fecha Inclusión	01/06/2019
Revisión de Validez	31/05/2020

Descripción

SEP Mobile es una solución de defensa de entornos móviles multiplataforma, cuyo objetivo es detectar amenazas tanto existentes como desconocidas.
Incorpora tecnología predictiva y mecanismos de protección contra el malware, las amenazas de red y los exploits de vulnerabilidad de aplicaciones/SO, con o sin conexión a Internet, permitiendo definir reglas específicas de cumplimiento basado en características, funciones o comportamientos de los dispositivos móviles y aplicaciones.
SEP Mobile dispone de la capacidad de tomar acciones de remediación o respuesta como puedes ser entre otras; Bloqueo a los recursos o servicios corporativos, Establecimiento de conexión VPN para proteger el tráfico y la información intercambiada, Bloqueo de instalación o ejecuciónde aplicaciones maliciosas, Bloqueo de cualquier comunicación de aplicaciones maliciosas o con un nivel de riesgo elevado, etc
SEP Mobile permite integraciones con soluciones SIEM, aportando información sobre amenazas detectadas y bloqueadas, situacionesde no cumplimiento e incidentes de seguridad, asi como integraciones con soluciones de MDM, y EMM

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Symantec™ Endpoint Protection Version	
Versión	14.2
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Fabricante	Symantec Corporation
Categoría	ENS ALTO
Fecha Inclusión	01/04/2019
Revisión de Validez	31/03/2020

Descripción

SEP v14.2 es una aplicación de protección anti-malware para puesto de trabajo y servidores, junto con un componente de gestión que se ejecuta en un servidor central para controlar y supervisar la ejecución de la aplicación antivirus.
SEP v14.2 combina elAntivirus de Symantec con prevención de amenazas avanzada en múltiples capas, para ofrecer una defensa contra el malware para equipos portátiles, de escritorio y servidores. Proporciona protección contra ataques sofisticados que evaden medidas de seguridad tradicionales, como rootkits, ramsonware, trojanos, malware polimórfico, y ataques de día cero, con idependiencia de las técnicas de ataque empleadas.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

7.2.2 FAMILIA: EDR (ENDPOINT DETECTION AND RESPONSE)

Panda Adaptive Defense 360	
Versión	3.25.00 (Protection Agent v8.0)
Familia	EDR (Endpoint Detection and Response)
Fabricante	Panda Security
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

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

Procedimiento de empleo seguro pendiente de publicación.

7.2.3 FAMILIA: HERRAMIENTAS DE GESTIÓN DE RED

FortiManager Appliances
FMG-200D, FMG-1000D, FMG-3900E, FMG-4000D, FMG4000E

Versión	Firmware 5.2.4
Familia	Herramientas de gestión de red
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

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

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

7.2.4 FAMILIA: ACTUALIZACIÓN DE SISTEMAS

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

7.2.5 FAMILIA: FILTRADO DE NAVEGACIÓN

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

7.2.6 FAMILIA: SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD

FortiAnalyzer™ Centralized Reporting Appliances
FAZ-200D, FAZ-1000C, FAZ-1000D, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ3500E, FAZ-3900E, FAZ-4000B

Versión	Firmware 5.2.4
Familia	Sistemas de gestión de eventos de seguridad
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

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

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

LogICA Next Generation SIEM	
Versión	v5.7.1
Familia	Sistemas de gestión de eventos de seguridad
Fabricante	Grupo ICA Sistemas y Seguridad
Categoría	ENS ALTO
Fecha Inclusión	01/01/2020
Revisión de Validez	31/05/2020

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

Procedimiento de empleo seguro pendiente de publicación.

IBM Qradar	
Versión	v7.3.2
Familia	Sistemas de gestión de eventos de seguridad
Fabricante	IBM
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

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, aplicando tanto en entornos IT como OT.
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, nuestra tecnología ofrece facilidades de búsquedas profundas para ayudar a encontrar nuevas amenazas de forma proactiva.
QRadar proporciona todas las funcionalidades que una organización necesita para abordar los desafíos de seguridad más importantes, ya sean amenazas avanzadas, amenazas internas, riesgos en la nube u otras vulnerabilidades.
https://www.ibm.com/support/knowledgecenter/es/SS42VS_7.3.2/com.ibm.qradar.doc/qradar_IC_welcome.html

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

NetWitness	
Versión	v.11
Familia	Sistemas de gestión de eventos de seguridad
Fabricante	RSA
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

La plataforma RSA Netwitness es la solución de SIEM evolucionado, con capacidades de visibilidad completa gracias a su modelo de datos unificado pudiendo capturar logs, netflow, tráfico de red y end point 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. RSA Netwitness Platform cuenta además con componentes adicionales como UEBA y SOAR. 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 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, 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.rsa.com/en-us/products/threat-detection-response

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

7.2.7 FAMILIA: DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS

EP543N	
Versión	V.1.2
Familia	Dispositivos para gestión de claves criptográficas
Fabricante	Epicom
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2021

Descripción

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

Observaciones

EP543X	
Versión	SW v 4.15
Familia	Dispositivos para gestión de claves criptográficas
Fabricante	Epicom
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2021

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

7.2.8 HERRAMIENTAS DE GESTIÓN DE DISPOSITIVOS MÓVILES (MDM)

Mobileiron Core – Plataforma de Seguridad	
Versión	10.0.1
Familia	Herramientas de Gestión de dispositivos móviles (MDM)
Fabricante	Mobileiron
Categoría	ENS ALTO
Fecha Inclusión	01/08/2019
Revisión de Validez	30/01/2020

Descripción

La administración Unificada de Puntos de Conexión (UEM) de MobileIron permite a los usuarios de una organización disfrutar de un acceso fluido a aplicaciones y datos corporativos a través de dispositivos móviles, tabletas y equipos, a la vez que mantieneun total control de su privacidad. Permite además optimizar al máximo y de forma segura el potencial de los dispositivos, las aplicaciones y la movilidad en general, posibilitando así la transformación digital y la innovación corporativa.
Vídeo descriptivo del producto: https://youtu.be/I1N7uqKfMLk

Observaciones

Procedimiento de empleo pendiente de publicación.

7.2.9 FAMILIA: OTRAS HERRAMIENTAS

authUsb safeDoor	
Versión	2.0.0.8
Familia	Otras Herramientas
Fabricante	authUSB
Categoría	ENS ALTO
Fecha Inclusión	01/05/2019
Revisión de Validez	31/10/2021

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

7.3 CATEGORÍA: MONITORIZACIÓN DE LA SEGURIDAD

7.3.1 FAMILIA: DISPOSITIVOS DE PREVENCIÓN DE INTRUSIONES

ASA 5500 Series (5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X, 5525-X, 5545-X, 5555-X) con FireSIGHT (FMC) y FMCv	
Versión	FTD 6.2
Familia	Dispositivos de prevención y detección de intrusiones
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	31/12/2019

Descripción

Cisco Firepower Threat Defense (FTD) es un appliance, virtual o físico, con capacidades de firewall, VPN e IPS. Ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).
Cisco FireSIGHT, también conocido como Cisco Firepower Management Center (FMC), es una appliance, virtual o físico, que proporciona una consola de gestión centralizada y una base de datos de eventos centralizados para el FTD y FTDv, con capacidades de agregación y correlación.
Cisco ASA, son firewalls de nueva generación que soportan el servicio Cisco Firepower para ofrecer conjuntamente los servicios de firewall, VPN e IPS.
Compatible con:
- FireSIGHT Series (FMC) FS750, FS1000, FS2000, FS2500, FS4000, FS4500
- FMCv running on ESXi 5.5 or 6.0on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E160S-M3, and E180D-M2/K9 installed on ISR

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Firepower 2100 Series: FP2110, FP2120, FP2130, FP2140 con FireSIGHT (FMC) y FMCv	
Versión	FTD 6.2, FXOS 2.2 y FMC/FCMv 6.2
Familia	Dispositivos de prevención y detección de intrusiones
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Cisco Firepower Threat Defense (FTD) es un appliance, virtual o físico, que tiene las 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:
-FireSIGHT Series (FMC) FS750, FS1000, FS2000, FS3500, FS4000, FS4500
- FMCv: running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E180D-M2/K9and E160S-M3

Observaciones

Procedimiento de empleo seguro pendiente de publicación.
Los dispositivos deben trabajar en "CC mode"

FP 4100 Series: FP4110, FP4120, FP4140, FP4150 con FireSIGHT (FMC) y FMCv	
Versión	FTD 6.2, FXOS 2.2 y FMC/FCMv 6.2
Familia	Dispositivos de prevención y detección de intrusiones
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Cisco Firepower Threat Defense (FTD) es un appliance, virtual o físico, que tiene las 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:
-FireSIGHT Series (FMC) FS750, FS1000, FS2000, FS3500, FS4000, FS4500
- FMCv: running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E180D-M2/K9and E160S-M3

Observaciones

Procedimiento de empleo seguro pendiente de publicación.
Los dispositivos deben trabajar en "CC mode"

FTDv running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E160S-M3, and E180D-M2/K9 installed on ISR con FireSIGHT (FMC) y FMCv

Versión	FTD 6.2
Familia	Dispositivos de prevención y detección de intrusiones
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	31/12/2019

Descripción

Cisco Firepower Threat Defense (FTD) es un appliance, virtual o físico, con capacidades de firewall, VPN e IPS. Ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).
Cisco FireSIGHT, también conocido como Cisco Firepower Management Center (FMC), es una appliance, virtual o físico, que proporciona una consola de gestión centralizada y una base de datos de eventos centralizados para el FTD y FTDv, con capacidades de agregación y correlación.
Cisco ASA, son firewalls de nueva generación que soportan el servicio Cisco Firepower para ofrecer conjuntamente los servicios de firewall, VPN e IPS.
Compatible con:
- FireSIGHT Series (FMC) FS750, FS1000, FS2000, FS2500, FS4000, FS4500
- FMCv running on ESXi 5.5 or 6.0on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E160S-M3, and E180D-M2/K9 installed on ISR

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Junos 12.3X48 for SRX Platforms SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650, SRX5400, SRX5400E, SRX5600 y SRX5600E, SRX5800 y SRX5800E with SPC-4-15-320.

Versión	SW: Junos 12.3X48-D30
Familia	Dispositivos de prevención y detección de intrusiones
Fabricante	Juniper Networks
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 “Procedimiento de Empleo Seguro Plataformas SRX Juniper“

Junos 12.3X48-D30 for SRX XLR Platforms SRX1400, SRX3400 and SRX3600; SRX5400, SRX5400E, SRX5600, SRX5600E, SRX5800E with SPC-2-10-20.	
Versión	SW: Junos 12.3X48-D30
Familia	Dispositivos de prevención y detección de intrusiones
Fabricante	Juniper Networks
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 "Procedimiento de Empleo Seguro Plataformas SRX Juniper"

Junos 15.1X49-D60 for SRX platforms SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400E, SRX5400X, SRX5600E, SRX5600X, SRX5800E and SRX 5800X	
Versión	SW: Junos 15.1X49-D60
Familia	Dispositivos de prevención y detección de intrusiones
Fabricante	Juniper Networks
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 "Procedimiento de Empleo Seguro Plataformas SRX Juniper"

Serie SOHO (SOHOW)	
Versión	SonicOS 6.5.2
Familia	Dispositivos de prevención y detección de intrusiones
Fabricante	SonicWall
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	31/05/2020

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

Procedimiento de empleo seguro pendiente de publicación.

SonicWall NSA Serie (2650, 3600, 3650, 4600, 4650, 5600, 5650, 6600, 6650, 9250, 9450, 9650)	
Versión	SonicOS 6.5.2
Familia	Dispositivos de prevención y detección de intrusiones
Fabricante	SonicWall
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	31/05/2020

Descripción

Los firewall de la serie NSa de SonicWall están indicados para compañías medianas / grandes (de entre 50 y 3000 usuarios aprox), 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. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/mid-range

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

SonicWall SM Serie (9200, 9400, 9600, 9800)	
Versión	SonicOS 6.5.2
Familia	Dispositivos de prevención y detección de intrusiones
Fabricante	SonicWall
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	31/05/2020

Descripción

Diseñado 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. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/high-end

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

SonicWall TZ Serie (300/W, 400/W, 500/W, 600)	
Versión	SonicOS 6.5.2
Familia	Dispositivos de prevención y detección de intrusiones
Fabricante	SonicWall
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	31/05/2020

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

Procedimiento de empleo seguro pendiente de publicación.

7.3.2 FAMILIA: SISTEMAS HONEYPOT / HONEYNET

Pendiente de publicación los Requisitos Fundamentales de Seguridad (RFS) de esta familia.

7.3.3 FAMILIA: CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO

GigaVUE (HD8, HD4, HC3, HC2, HC1)

Versión	version 5.1.01
Familia	Captura, Monitorización y Análisis de Tráfico
Fabricante	Gigamon
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	31/05/2020

Descripción

Network Packet Brokers HC/HD Series. Network Packet Brokers de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1000m/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, TAPsintegrados.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

GigaVUE (TA10, TA40, TA100)

Versión	version 5.1.01
Familia	Captura, Monitorización y Análisis de Tráfico
Fabricante	Gigamon
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	31/05/2020

Descripción

Agregadores TA Series (TA10/TA40/TA100)
Agregadores de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1000m/10g en cobre y funcionalidades de filtrado de trafico L2-3-4, Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Clustering, Balanceo, Cambio de medio y velocidad

Observaciones

Procedimiento de empleo seguro pendiente de publicación

7.3.4 FAMILIA: HERRAMIENTAS DE SANDBOX

Pendiente de publicación los Requisitos Fundamentales de Seguridad (RFS) de esta familia.

7.4 CATEGORÍA: PROTECCIÓN DE LAS COMUNICACIONES

7.4.1 FAMILIA: ENRUTADORES

Aruba 2930F y 2930M Switch Series

Versión Aruba OS version 16.04

Familia Enrutadores

Fabricante Aruba

Categoría ENS ALTO

Fecha Inclusión 01/03/2019

Revisión de Validez 31/08/2021

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

Procedimiento de empleo pendiente de publicación.

Aruba 3810M Switch Series

Versión Aruba OS version 16.04

Familia Enrutadores

Fabricante Aruba

Categoría ENS ALTO

Fecha Inclusión 01/03/2019

Revisión de Validez 31/08/2021

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

Procedimiento de empleo pendiente de publicación.

Aruba 5400R Switch Series

Versión Aruba OS version 16.04

Familia Enrutadores

Fabricante Aruba

Categoría ENS ALTO

Fecha Inclusión 01/03/2019

Revisión de Validez 31/08/2021

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

Procedimiento de empleo pendiente de publicación.

Aruba 8320 Switch Series

Versión Aruba OS-CX version 10.03

Familia Enrutadores

Fabricante Aruba

Categoría ENS ALTO

Fecha Inclusión 01/11/2019

Revisión de Validez 30/04/2022

Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. 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.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Aruba 8325 Switch Series

Versión	Aruba OS-CX version 10.03
Familia	Enrutadores
Fabricante	Aruba
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. 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.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Aruba 8400 Switch Series

Versión	Aruba OS-CX version 10.03
Familia	Enrutadores
Fabricante	Aruba
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. 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.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

ASR 1000 Series: 1001-X, 1001-HX, 1002-HX, 1006-X, 1009-X, 1013.	
Versión	IOS XE 16.3
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	31/05/2020

Descripción

La serie Agregation Services Router (ASR) 1000 de CISCO es una plataforma de enrutamiento que entrega aceleración de hardware integrada para múltiples servicios de software Cisco IOS-XE. En apoyo a las capacidades de enrutamiento, Cisco ASR1K proporcionacapacidades de conexión IPsec para facilitar la seguridad comunicaciones con entidades externas, según sea necesario. Los Cisco ASR1kK son soluciones de enrutamiento y seguridad de dispositivo único para proteger la red.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASR 1002X, ASR 1006 and Cloud Services Router 1000V	
Versión	IOS-XE 16.3
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2018
Revisión de Validez	31/05/2020

Descripción

Cisco Aggregation Services Router 1000 Series (ASR1K) son plataformas específicas para servicios de enrutamiento (routing). Disponen de hardware de aceleración embebido empleado por múltiples servicios ofrecidos por el software Cisco IOS-XE.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASR1K-1004	
Versión	IOS XE 16.3
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	31/05/2020

Descripción

La serie ASR1K de Cisco ofrece aceleración de hardware integrada para múltiples servicios de Cisco IOS-XE Software. Además, los enrutadores de Cisco de la serie ASR1K presentan enrutado redundante y procesadores de servicios integrados, así como redundancia basada en software. Cisco ASR1K proporciona capacidades de conexión IPsec para comunicaciones seguras.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Catalyst 3650 and 3850 Series	
Versión	IOS XE 16.3
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	31/05/2020

Descripción

La serie de conmutadores Cisco Catalyst 3650 y 3850 ejecutan IOS-XE 16.3 (en adelante, la serie Cat3K). Es una plataforma de enrutamiento y conmutación especialmente diseñada con capacidades de filtrado de tráfico OSI Layer2 y Layer3.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Catalyst 4500 Series Wired Access Switches: 4503-E, 4506-E, 4507R+E, 4510R+E, 4500-X, 4500-XF	
Versión	IOS-XE 3.10
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/04/2019
Revisión de Validez	31/03/2020

Descripción

Las series Cisco Catalyst 4500 son plataformas de enrutamiento y conmutación especialmente diseñada con capacidades de filtrado de tráfico OSI Layer2 y Layer3. Se utilizan para construir redes IP mediante la interconexión de redes más pequeñas o de segmentos de red. En la función de Switch de capa 2, el producto realiza el análisis del tráfico entrante, decide sobre el direccionamiento del tráfico basándose en la información contenida en los paquetes, y los envía hacia su destino. En la función de Enrutador de capa 3, el producto enruta cada paquete recibido por la mejor ruta que determina basándose en las rutas disponibles, condiciones, distancias y costes.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Catalyst 6500 and 6807-XL Series	
Versión	IOS 15.5SY
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	31/05/2020

Descripción

La serie Cisco Cat 6K son plataformas de conmutación y enrutamiento que brindan servicios de conectividad y seguridad en un solo dispositivo seguro. Estos conmutadores pueden entregar entre 2 y 11 Tbps de capacidad de ancho de banda y desde 80 Gbps hasta440 Gbps de ancho de banda por ranura. Los conmutadores de la serie Cat 6K también ofrecen una administración simplificada adecuada para entornos empresariales de núcleo y agregación. Los switches Cisco Cat 6K Series son soluciones de seguridad y conmutación de un solo dispositivo para proteger la red.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Catalyst 9300 and 9500 Series

Versión IOS-XE 16.6

Familia Enrutadores

Fabricante Cisco Systems

Categoría ENS ALTO

Fecha Inclusión 01/12/2018

Revisión de Validez 31/05/2020

Descripción

Las series Cisco Catalyst 9300 y 9500 (Cat9K) son plataformas específicas que proporcionan servicios de switching y de routing. Se utilizan para construir redes IP mediante la interconexión de redes más pequeñas o de segmentos de red. En la función de Switch de capa 2, el producto realiza el análisis del tráfico entrante, decide sobre el direccionamiento del tráfico basándose en la información contenida en los paquetes, y los envía hacia su destino. En la función de Enrutador de capa 3, el producto enrutacada paquete recibido por la mejor ruta que determina basándose en las rutas disponibles, condiciones, distancias y costes.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Catalyst 9400 Series

Versión IOS-XE 16.6

Familia Enrutadores

Fabricante Cisco Systems

Categoría ENS ALTO

Fecha Inclusión 01/12/2018

Revisión de Validez 31/05/2020

Descripción

Las series Cisco Catalyst 9400 (Cat9K) son plataformas específicas que proporcionan servicios de switching y de routing. Se utilizan para construir redes IP mediante la interconexión de redes más pequeñas o de segmentos de red. En la función de Switch decapa 2, el producto realiza el análisis del tráfico entrante, decide sobre el direccionamiento del tráfico basándose en la información contenida en los paquetes, y los envía hacia su destino. En la función de Enrutador de capa 3, el producto enruta cada paquete recibido por la mejor ruta que determina basándose en las rutas disponibles, condiciones, distancias y costes.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Catalyst Switches 2960CX, 2960X, 2960XR y 3560CX	
Versión	IOS 15.2
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	31/12/2019

Descripción

Las series Cisco Catalyst 2K/3K WAS (Wired Access Switches) son equipos switches de acceso a LAN que proporciona la base para una infraestructura cableada en una única plataforma.
Ofrecen servicios de switching y routing con capacidades de filtrado de nivel 2 y 3 de la capa OSI.
Disponen de capacidades de stack, POE+, Cisco UPOE, conexiones multiGigabit y fuentes de alimentación modulares y reemplazables en campo. Presentan, además, capacidades de conexiones Ethernet de 100/1000 Mbps, y opciones de 1/10/40 Gbps.
Por otro lado, Cisco IOS es un sistema operativo propietario y altamente configurable desarrollado por Cisco que provee servicios de routing y switching.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 3650 Series: WS-C3650-24TS, WS-C3650-48TS, WS-C3650-24PS, WS-C3650-48PS, WS-C3650-48FS, WS-C3650-24TD, WS-C3650-48TD, WS-C3650-24PD, WS-C3650-48PD, WS-C3650-48FD, WS-C3650-48TQ, WS-C3650-48PQ, WS-C3650-48FQ, WS-C3650-48FQM.	
Versión	IOS XE 16.3
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

La serie Cisco Catalyst 3650 ejecutan IOS-XE 16.3 es una plataforma de enrutamiento y conmutación especialmente diseñada con capacidades de filtrado de tráfico OSI Capa 2 y Capa 3.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 3850 Series:
WS-C3850-24T, WS-C3850-48T, WS-C3850-24P, WS-C3850-48P, WS-C3850-48F, WS-C3850-24U, WS-C3850-48U, WS-3850-12S, WS-C3850-24S, WS-C3850-12XS, WS-C3850-24XS, WS-C3850-24XU, WS-C3850-48XS.

Versión	IOS XE 16.3
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

La serie Cisco Catalyst 3850 ejecutan IOS-XE 16.3 es una plataforma de enrutamiento y conmutación especialmente diseñada con capacidades de filtrado de tráfico OSI Capa 2 y Capa 3.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 9200L Series:
C9200L-24P-4G, C9200L-24P-4X, C9200L-24T-4G, C9200L-24T-4X, C9200L-48P-4G, C9200L-48P-4X, C9200L-48T-4G, C9200L-48T-4X

Versión	IOS XE 16.9
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/01/2020
Revisión de Validez	30/06/2020

Descripción

Las series Cisco Catalyst 9200L son plataformas específicas que incluyen servicios de routing y switching con capacidades de filtrado de nivel 2 y 3 de la capa OSI. Estos dispositivos utilizan el software Universal Cisco Internet Operating System (IOS) XE (IOS XE 16.9).

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 9300 Series: C9300-24T, C9300-48T, C9300-24P, C9300-48P, C930024U, C930024UX, C9300-48UXM and C9300-48UN.	
Versión	IOS XE 16.9
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

La serie Cisco Catalyst 9300 ejecutan IOS-XE 16.9 es una plataforma de enrutamiento y conmutación especialmente diseñada con capacidades de filtrado de tráfico OSI Capa 2 y Capa 3.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 9400 Series: C9404R, C9407R, C9410R	
Versión	IOS XE 16.9
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/01/2020
Revisión de Validez	30/06/2020

Descripción

Las series Cisco Catalyst 9400 son plataformas específicas que incluyen servicios de routing y switching con capacidades de filtrado de nivel 2 y 3 de la capa OSI. Estos dispositivos utilizan el software Universal Cisco Internet Operating System (IOS) XE (IOS XE 16.9).

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 9500 Series: C9500-12Q, C9500-16X, C9500-24Q, C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-40X and C9500-48Y4C	
Versión	IOS XE 16.9
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

La serie Cisco Catalyst 9500 ejecutan IOS-XE 16.9 es una plataforma de enrutamiento y conmutación especialmente diseñada con capacidades de filtrado de tráfico OSI Capa 2 y Capa 3.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

IE2000 Series, IE4000 Series, IE5000 Series y 2500 Series CGS	
Versión	IOS 15.2
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	31/12/2019

Descripción

Los Cisco IoT son switches, que incluyen servicios de routing, usados para construir redes IP conectando pequeñas redes y segmentos de red.
Estos equipos Cisco están especialmente desarrollados para soportar entornos industriales complejos. Ofrecen configuraciones flexibles con administración simple y ejecución de aplicaciones avanzadas en un único dispositivo.
Por otro lado, Cisco IOS es un sistema operativo propietario y altamente configurable desarrollado por Cisco que provee servicios de routing y switching.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ISR 1100 Series: C1111-8P, C1111-4P, C1112-8P, C1113-8P, C1114-8P, C1115-8P, C1116-4P, C1117-4P.	
Versión	IOS XE 16.6
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/04/2019
Revisión de Validez	31/03/2020

Descripción

Cisco ISR 1100 es una plataforma de enrutamiento que brinda conectividad y servicios de seguridad. Cisco ISR ejecuta el software modular Cisco IOS-XE. En apoyo de las capacidades de enrutamiento, Cisco ISR 1100 proporciona capacidades de conexión IPsec para clientes habilitados para VPN.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ISR 4000 Series: 4321, 4331, 4351, 4431, 4451-X	
Versión	IOS XE 16.3
Familia	Enrutadores
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

Cisco ISR4K es una plataforma de enrutamiento que
ofrece aceleración de encriptación y brinda conectividad y servicios de seguridad. Cisco ISR ejecuta el software modular Cisco IOS-XE. En apoyo de las capacidades de enrutamiento, Cisco ISR4K proporciona capacidades de conexión IPsec para clientes habilitados para VPN.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Junos 12.3X48 for SRX Platforms SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650, SRX5400, SRX5400E, SRX5600 y SRX5600E, SRX5800 y SRX5800E with SPC-4-15-320.

Versión	SW: Junos 12.3X48-D30
Familia	Enrutadores
Fabricante	Juniper Networks
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 "Procedimiento de Empleo Seguro Plataformas SRX Juniper"

Junos 12.3X48-D30 for SRX XLR Platforms SRX1400, SRX3400 and SRX3600; SRX5400, SRX5400E, SRX5600, SRX5600E, SRX5800E with SPC-2-10-20.

Versión	SW: Junos 12.3X48-D30
Familia	Enrutadores
Fabricante	Juniper Networks
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 "Procedimiento de Empleo Seguro Plataformas SRX Juniper"

Junos 15.1X49-D60 for SRX platforms
SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400E, SRX5400X, SRX5600E, SRX5600X, SRX5800E and SRX 5800X

Versión	SW: Junos 15.1X49-D60
Familia	Enrutadores
Fabricante	Juniper Networks
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 "Procedimiento de Empleo Seguro Plataformas SRX Juniper"

7.4.2 FAMILIA: SWITCHES

Alcatel-Lucent OmniSwitch (OS6860, OS6865, OS6900, OS9900, OS10K)

Versión	AOS 8.3.1.348.R01
Familia	Switches
Fabricante	Alcatel Lucent
Categoría	ENS ALTO
Fecha Inclusión	01/09/2018
Revisión de Validez	29/02/2020

Descripción

OS9900: Conmutadores LAN con chasis 1GE y 10GE de alta capacidad con conmutación de núcleo segura de alta disponibilidad para redes empresariales, campus y redes Metro Ethernet.
OS10K: Conmutador LAN Ethernet modular de alta capacidad y alto rendimientopara Data Center, campus y servicios basados en Cloud
OS6860: Plataformas Gigabit Ethernet (GigE) y 10 GigE compactas, de alta densidad, diseñadas para redes convergentes. Con funciones de Acceso unificado avanzadas que permiten a los usuarios utilizar Application Fluent Networks. Puede supervisar y controlar las aplicaciones de su red con capacidades de Deep Packet Inspection.
OS6865: Modelo homologo al 6860 preparado para entorno industrial.
OS6900: Plataformas 10 y 40 GigE, compactas de alta densidad. Diseñadas para que sean flexibles. Pueden instalarse como conmutadores convergentes situados en la parte superior del bastidor 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

Procedimiento de empleo pendiente de publicación.

X930 Series AlliedWare Plus

Versión Software Version 5.4.6-1

Familia Switches

Fabricante Allied Telesys

Categoría ENS ALTO

Fecha Inclusión 01/10/2019

Revisión de Validez 30/03/2020

Descripción

La familia x930 de Allied Telesis está formada por 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 puertoscon 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.
Modelos Hardware: AT-x930-28GTX, AT-x930-28GPX, AT-x930-52GTX, AT-x930-28GPX,AT-x930-28GSTX.
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

Procedimiento de empleo pendiente de publicación.

Aruba 2930F y 2930M Switch Series

Versión Aruba OS version 16.04

Familia Switches

Fabricante Aruba

Categoría ENS ALTO

Fecha Inclusión 01/03/2019

Revisión de Validez 31/08/2021

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

Procedimiento de empleo pendiente de publicación.

Aruba 3810M Switch Series

Versión Aruba OS version 16.04

Familia Switches

Fabricante Aruba

Categoría ENS ALTO

Fecha Inclusión 01/03/2019

Revisión de Validez 31/08/2021

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

Procedimiento de empleo pendiente de publicación.

Aruba 5400R Switch Series

Versión Aruba OS version 16.04

Familia Switches

Fabricante Aruba

Categoría ENS ALTO

Fecha Inclusión 01/03/2019

Revisión de Validez 31/08/2021

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

Procedimiento de empleo pendiente de publicación.

Aruba 8320 Switch Series

Versión	Aruba OS-CX version 10.03
Familia	Switches
Fabricante	Aruba
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. 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.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Aruba 8325 Switch Series

Versión	Aruba OS-CX version 10.03
Familia	Switches
Fabricante	Aruba
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. 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.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Aruba 8400 Switch Series

Versión	Aruba OS-CX version 10.03
Familia	Switches
Fabricante	Aruba
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. 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.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

ASR 1000 Series: 1001-X, 1001-HX, 1002-HX, 1006-X, 1009-X, 1013.

Versión	IOS XE 16.3
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La serie Agregation Services Router (ASR) 1000 de CISCO es una plataforma de enrutamiento que entrega aceleración de hardware integrada para múltiples servicios de software Cisco IOS-XE. En apoyo a las capacidades de enrutamiento, Cisco ASR1K proporcionacapacidades de conexión IPsec para facilitar la seguridad comunicaciones con entidades externas, según sea necesario. Los Cisco ASR1kK son soluciones de enrutamiento y seguridad de dispositivo único para proteger la red.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASR1K-1004	
Versión	IOS XE 16.3
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La serie ASR1K de Cisco ofrece aceleración de hardware integrada para múltiples servicios de Cisco IOS-XE Software. Además, los enrutadores de Cisco de la serie ASR1K presentan enrutado redundante y procesadores de servicios integrados, así como redundancia basada en software. Cisco ASR1K proporciona capacidades de conexión IPsec para comunicaciones seguras.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Catalyst 3650 and 3850 Series	
Versión	IOS XE 16.3
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La serie de conmutadores Cisco Catalyst 3650 y 3850 ejecutan IOS-XE 16.3 (en adelante, la serie Cat3K). Es una plataforma de enrutamiento y conmutación especialmente diseñada con capacidades de filtrado de tráfico OSI Layer2 y Layer3.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Catalyst 3K/4K Wired Access Switches running IOS-XE 3.8.0E (3650, 3850, 4503-E, 4506-E, 4507R+E, 4510R+E, 4500-X y 4500-XF)

Versión	IOS-XE 3.8.0E
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	30/11/2020

Descripción

Los conmutadores para redes LAN de las series 3K/4K proveen capacidades de convergencia en redes cableadas e inalámbricas. Son dispositivos de conmutación para redes LAN que presentan características y capacidades de stack, multi-gigabit ethernet y conmutación de capas de agregación. Las series 3K/4K presentan los nuevos Cisco Unified Access Data Plane (UADP) Application Specific Integrated Circuit (ASIC) que permite reforzar políticas de acceso, visualizar aplicaciones, ofrecer flexibilidad y optimización sobre aplicaciones. Soportan PoE+, Cisco UPOE, fuentes de alimentación reemplazables en campo y modulares, ventiladores y fuentes redundantes e interfaces en estándares RJ-45 y fibra óptica. Estos modelos de conmutadores de red presentan Cisco IOS-XE como sistema operativo.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Catalyst 4500 Series Wired Access Switches: 4503-E, 4506-E, 4507R+E, 4510R+E, 4500-X, 4500-XF

Versión	IOS-XE 3.10
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/04/2019
Revisión de Validez	31/03/2020

Descripción

Las series Cisco Catalyst 4500 son plataformas de enrutamiento y conmutación especialmente diseñada con capacidades de filtrado de tráfico OSI Layer2 y Layer3. Se utilizan para construir redes IP mediante la interconexión de redes más pequeñas o de segmentos de red. En la función de Switch de capa 2, el producto realiza el análisis del tráfico entrante, decide sobre el direccionamiento del tráfico basándose en la información contenida en los paquetes, y los envía hacia su destino. En la función de Enrutador de capa 3, el producto enruta cada paquete recibido por la mejor ruta que determina basándose en las rutas disponibles, condiciones, distancias y costes.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Catalyst 6500 and 6807-XL Series	
Versión	IOS 15.5SY
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La serie Cisco Cat 6K son plataformas de conmutación y enrutamiento que brindan servicios de conectividad y seguridad en un solo dispositivo seguro. Estos conmutadores pueden entregar entre 2 y 11 Tbps de capacidad de ancho de banda y desde 80 Gbps hasta440 Gbps de ancho de banda por ranura. Los conmutadores de la serie Cat 6K también ofrecen una administración simplificada adecuada para entornos empresariales de núcleo y agregación. Los switches Cisco Cat 6K Series son soluciones de seguridad y conmutación de un solo dispositivo para proteger la red.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Catalyst 9300 and 9500 Series	
Versión	IOS-XE 16.6
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2018
Revisión de Validez	30/11/2020

Descripción

Las series Cisco Catalyst 9300 y 9500 (Cat9K) son plataformas específicas que proporcionan servicios de switching y de routing. Se utilizan para construir redes IP mediante la interconexión de redes más pequeñas o de segmentos de red. En la función de Switch de capa 2, el producto realiza el análisis del tráfico entrante, decide sobre el direccionamiento del tráfico basándose en la información contenida en los paquetes, y los envía hacia su destino. En la función de Enrutador de capa 3, el producto enrutacada paquete recibido por la mejor ruta que determina basándose en las rutas disponibles, condiciones, distancias y costes.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Catalyst 9400 Series	
Versión	IOS-XE 16.6
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2018
Revisión de Validez	30/11/2020

Descripción

Las series Cisco Catalyst 9400 (Cat9K) son plataformas específicas que proporcionan servicios de switching y de routing. Se utilizan para construir redes IP mediante la interconexión de redes más pequeñas o de segmentos de red. En la función de Switch decapa 2, el producto realiza el análisis del tráfico entrante, decide sobre el direccionamiento del tráfico basándose en la información contenida en los paquetes, y los envía hacia su destino. En la función de Enrutador de capa 3, el producto enruta cada paquete recibido por la mejor ruta que determina basándose en las rutas disponibles, condiciones, distancias y costes.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Catalyst Switches 2960CX, 2960X, 2960XR y 3560CX	
Versión	IOS 15.2
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	31/12/2019

Descripción

Las series Cisco Catalyst 2K/3K WAS (Wired Access Switches) son equipos switches de acceso a LAN que proporciona la base para una infraestructura cableada en una única plataforma.
Ofrecen servicios de switching y routing con capacidades de filtrado de nivel 2 y 3 de la capa OSI.
Disponen de capacidades de stack, POE+, Cisco UPOE, conexiones multiGigabit y fuentes de alimentación modulares y reemplazables en campo. Presentan, además, capacidades de conexiones Ethernet de 100/1000 Mbps, y opciones de 1/10/40 Gbps.
Por otro lado, Cisco IOS es un sistema operativo propietario y altamente configurable desarrollado por Cisco que provee servicios de routing y switching.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

CGS2500 Series
(CGS-2520-16S-8PC, CGS2520-24TC)

Versión	IOS 15.2(4)E.
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	30/11/2020

Descripción

La serie IE2000 de equipos industriales de conmutación para redes LAN son dispositivos robustos, compactos y adaptados para ser la base de infraestructura de cableado en ambientes industriales donde las condiciones pueden ser extremas. Son escalables y administrables, presentan opciones de seguridad, diferentes formatos de puertos y conexiones, interfaces de estandares RJ-45 y Fibra Óptica, PoE y certificaciones y cumplimientos de normativas para uso industrial. Estos dispositivos utilizan la versión Cisco IOS versiones 15.X como sistema operativo.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 3650 Series:
WS-C3650-24TS, WS-C3650-48TS, WS-C3650-24PS, WS-C3650-48PS, WS-C3650-48FS, WS-C3650-24TD, WS-C3650-48TD, WS-C3650-24PD, WS-C3650-48PD, WS-C3650-48FD, WS-C3650-48TQ, WS-C3650-48PQ, WS-C3650-48FQ, WS-C3650-48FQM.

Versión	IOS XE 16.3
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

La serie Cisco Catalyst 3650 ejecutan IOS-XE 16.3 es una plataforma de enrutamiento y conmutación especialmente diseñada con capacidades de filtrado de tráfico OSI Capa 2 y Capa 3.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 3850 Series:
WS-C3850-24T, WS-C3850-48T, WS-C3850-24P, WS-C3850-48P, WS-C3850-48F, WS-C3850-24U, WS-C3850-48U, WS-3850-12S, WS-C3850-24S, WS-C3850-12XS, WS-C3850-24XS, WS-C3850-24XU, WS-C3850-48XS.

Versión	IOS XE 16.3
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

La serie Cisco Catalyst 3850 ejecutan IOS-XE 16.3 es una plataforma de enrutamiento y conmutación especialmente diseñada con capacidades de filtrado de tráfico OSI Capa 2 y Capa 3.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 9200L Series:
C9200L-24P-4G, C9200L-24P-4X, C9200L-24T-4G, C9200L-24T-4X, C9200L-48P-4G, C9200L-48P-4X, C9200L-48T-4G, C9200L-48T-4X

Versión	IOS XE 16.9
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/01/2020
Revisión de Validez	30/06/2020

Descripción

Las series Cisco Catalyst 9200L son plataformas específicas que incluyen servicios de routing y switching con capacidades de filtrado de nivel 2 y 3 de la capa OSI. Estos dispositivos utilizan el software Universal Cisco Internet Operating System (IOS) XE (IOS XE 16.9).

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 9300 Series:
C9300-24T, C9300-48T, C9300-24P, C9300-48P, C930024U, C930024UX, C9300-48UXM and C9300-48UN.

Versión	IOS XE 16.9
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

La serie Cisco Catalyst 9300 ejecutan IOS-XE 16.9 es una plataforma de enrutamiento y conmutación especialmente diseñada con capacidades de filtrado de tráfico OSI Capa 2 y Capa 3.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 9400 Series:
C9404R, C9407R, C9410R

Versión	IOS XE 16.9
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/01/2020
Revisión de Validez	30/06/2020

Descripción

Las series Cisco Catalyst 9400 son plataformas específicas que incluyen servicios de routing y switching con capacidades de filtrado de nivel 2 y 3 de la capa OSI. Estos dispositivos utilizan el software Universal Cisco Internet Operating System (IOS) XE (IOS XE 16.9).

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 9500 Series: C9500-12Q, C9500-16X, C9500-24Q, C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-40X and C9500-48Y4C	
Versión	IOS XE 16.9
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

La serie Cisco Catalyst 9500 ejecutan IOS-XE 16.9 es una plataforma de enrutamiento y conmutación especialmente diseñada con capacidades de filtrado de tráfico OSI Capa 2 y Capa 3.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

IE2000 Series (IE-2000-16TC-G-E, IE2000-4TS-G-B, IE-2000-16PTC-G-E, IE-2000-16TC-L, IE-2000-8TC-L)	
Versión	IOS 15.2(4)E.
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

La serie IE2000 de equipos industriales de conmutación para redes LAN son dispositivos robustos, compactos y adaptados para ser la base de infraestructura de cableado en ambientes industriales donde las condiciones pueden ser extremas. Son escalables y administrables, presentan opciones de seguridad, diferentes formatos de puertos y conexiones, interfaces de estandares RJ-45 y Fibra Óptica, PoE y certificaciones y cumplimientos de normativas para uso industrial. Estos dispositivos utilizan la versión Cisco IOS versiones 15.X como sistema operativo.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

IE2000 Series, IE4000 Series, IE5000 Series y 2500 Series CGS	
Versión	IOS 15.2
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	31/12/2019

Descripción

Los Cisco IoT son switches, que incluyen servicios de routing, usados para construir redes IP conectando pequeñas redes y segmentos de red.
Estos equipos Cisco están especialmente desarrollados para soportar entornos industriales complejos. Ofrecen configuraciones flexibles con administración simple y ejecución de aplicaciones avanzadas en un único dispositivo.
Por otro lado, Cisco IOS es un sistema operativo propietario y altamente configurable desarrollado por Cisco que provee servicios de routing y switching.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

IE4000 Series (IE-4000-4GC4GP4-G-E, IE4000-16GT4G-E, IE-4000-8GT8GP4-G-E, IE-4000-4GS8GP4-G-E)	
Versión	IOS 15.2(4)E.
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

La serie IE4000 de equipos industriales de conmutación para redes LAN son dispositivos robustos, compactos y adaptados para ser la base de infraestructura de cableado en ambientes industriales donde las condiciones pueden ser extremas. Son escalables y administrables, presentan opciones de seguridad, diferentes formatos de puertos y conexiones, interfaces de estandares RJ-45 y Fibra Óptica, PoE y certificaciones y cumplimientos de normativas para uso industrial. Estos dispositivos utilizan la versión Cisco IOS versiones 15.X como sistema operativo.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

IE4010 Series
(IE-4010-16S12P, IE4010-4S24P)

Versión	IOS 15.2(4)E.
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

La serie IE4010 de equipos industriales de conmutación para redes LAN son dispositivos robustos, compactos y adaptados para ser la base de infraestructura de cableado en ambientes industriales donde las condiciones pueden ser extremas. Son escalables y administrables, presentan opciones de seguridad, diferentes formatos de puertos y conexiones, interfaces de estandares RJ-45 y Fibra Óptica, PoE y certificaciones y cumplimientos de normativas para uso industrial. Estos dispositivos utilizan la versión Cisco IOS versiones 15.X como sistema operativo.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

IE5000 Series
(IE-5000-12S12P-10G, IE5000-16S12P)

Versión	IOS 15.2(4)E.
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

La serie IE5000 de equipos industriales de conmutación para redes LAN son dispositivos robustos, compactos y adaptados para ser la base de infraestructura de cableado en ambientes industriales donde las condiciones pueden ser extremas. Son escalables y administrables, presentan opciones de seguridad, diferentes formatos de puertos y conexiones, interfaces de estandares RJ-45 y Fibra Óptica, PoE y certificaciones y cumplimientos de normativas para uso industrial. Estos dispositivos utilizan la versión Cisco IOS versiones 15.X como sistema operativo.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ISR 1100 Series: C1111-8P, C1111-4P, C1112-8P, C1113-8P, C1114-8P, C1115-8P, C1116-4P, C1117-4P.	
Versión	IOS XE 16.6
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/04/2019
Revisión de Validez	31/03/2020

Descripción

Cisco ISR 1100 es una plataforma de enrutamiento que brinda conectividad y servicios de seguridad. Cisco ISR ejecuta el software modular Cisco IOS-XE. En apoyo de las capacidades de enrutamiento, Cisco ISR 1100 proporciona capacidades de conexión IPsec para clientes habilitados para VPN.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ISR 4000 Series: 4321, 4331, 4351, 4431, 4451-X	
Versión	IOS XE 16.3
Familia	Switches
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	31/05/2020

Descripción

Cisco ISR4K es una plataforma de enrutamiento que ofrece aceleración de encriptación y brinda conectividad y servicios de seguridad. Cisco ISR ejecuta el software modular Cisco IOS-XE. En apoyo de las capacidades de enrutamiento, Cisco ISR4K proporciona capacidades de conexión IPsec para clientes habilitados para VPN.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Dell Networking C-Series (C9010 y C1048P)

Versión	V9.11
Familia	Switches
Fabricante	Dell Computer
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	30/11/2019

Descripción

Este swich 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 usuarioy 2 puertos uplink SFP+ para la conectividad con el C9010

Observaciones

Procedimiento de empleo pendiente de publicación.

Dell Networking S-Series 10GbE (S5000, S4048-ON, S4048T-ON)

Versión	V9.11
Familia	Switches
Fabricante	Dell Computer
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	30/11/2019

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 comoun 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

Procedimiento de empleo pendiente de publicación.

Dell Networking S-Series 1GbE (S3124, S3124P, S3124F, S3148, S3148P, S3048-ON)	
Versión	V9.11
Familia	Switches
Fabricante	Dell Computer
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	30/11/2019

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

Procedimiento de empleo pendiente de publicación.

Dell Networking S-Series 25/40/50/100GbE (S6010-ON, S6100-ON)	
Versión	V9.11
Familia	Switches
Fabricante	Dell Computer
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	30/11/2019

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 dela 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

Procedimiento de empleo pendiente de publicación.

Dell Networking Z-Series (Z9100-ON)

Versión	V9.11
Familia	Switches
Fabricante	Dell Computer
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	30/11/2019

Descripción

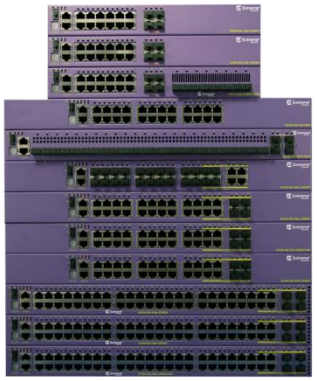
Este switch Open Networking de formato fijo y preparado para redes definidas por software (SDN) se ha diseñado para centros de datos y ofrece las siguientes prestaciones:
- Switch multivelocidad con opciones 10/25/40/50/100GbE.
- Alta densidad con hasta32 puertos 100GbE en 1U.
- Selección de los principales sistemas operativos de red.
- Vía de acceso fácil a las SDN para una parte o la totalidad de su entorno de producción.

Observaciones

Procedimiento de empleo pendiente de publicación.

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 v22.3.1.4-patch1CC-2
Familia	Switches
Fabricante	Extreme Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021



Descripción

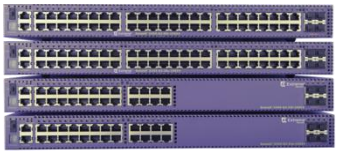
Conmutador apilable de alto rendimiento, posicionado como equipo de acceso. Proporciona conmutación inteligente de Nivel 2 y routing básico de Nivel 3, con interfaces 10/100/1000 Mbps así como 10 Gb. Existen versiones PoE y no PoE y de puertos de fibra óptica y puede apilarse también con otras familias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

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit 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

Versión	EXOS v22.3.1.4-patch1CC-2
Familia	Switches
Fabricante	Extreme Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021



Descripción

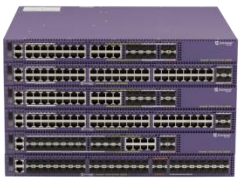
Conmutador apilable de alto rendimiento, posicionado como equipo de acceso de altas prestaciones. Proporciona conmutación avanzada de Nivel 2 y routing de Nivel 3, con interfaces 10/100/1000 Mbps, así como 10Gb. Existen versiones PoE y no PoE, y puede apilarse con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit 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 v22.3.1.4-patch1CC-2
Familia	Switches
Fabricante	Extreme Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021



Descripción

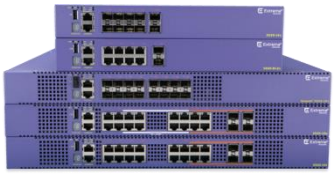
Conmutador apilable de alta rendimiento, posicionado como equipo de acceso de altas prestaciones y backbone de redes medias. Proporciona conmutación avanzada de Nivel 2 y de Nivel 3, con soporte de protocolos de alta complejidad (BGP, MPLS, etc). con interfaces 10/100/1000 Mbps, así como 10Gb y 40 Gb. 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

Summit X620 Series:
X620–16x, X620–16t, X620–10x, X620–8t-2x

Versión	EXOS v22.3.1.4-patch1CC-2
Familia	Switches
Fabricante	Extreme Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021



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 x670-G2 Series:
X670-G2-72x, X670-G2-48x-4q, X670-G2-48x-4q-FB-AC-TAA

Versión	EXOS v22.3.1.4-patch1CC-2
Familia	Switches
Fabricante	Extreme Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

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 X690 Series:
(X690-48x-2q-4c, X690-48t-2q-4c)

Versión	EXOS v22.3.1.4-patch1CC-2
Familia	Switches
Fabricante	Extreme Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

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 X870 Series:
(X870-32c, X870-96x-8c)

Versión	EXOS v22.3.1.4-patch1CC-2
Familia	Switches
Fabricante	Extreme Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

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 hacenideal 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

7.4.3 FAMILIA: CORTAFUEGOS

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

Versión	R77.30
Familia	Cortafuegos
Fabricante	Check Point Software Technologies
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 76Gbps de inspección Firewall, 18Gbps de IPS y 13,11Gbps para protección ante amenazas avanzadas. Un máximo de 12.8 millones de conexiones concurrentes y 185.000 nuevas por segundo.
https://www.checkpoint.com/products/15000-security-appliances/

Observaciones

CCN-STIC 653 Seguridad en Check Point

Check Point Security Gateway Serie 23000 (CPAP-SG23500-NGTX, CPAP-SG23800-NGTX)

Versión	R77.30
Familia	Cortafuegos
Fabricante	Check Point Software Technologies
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Son dispositivos dedicados y 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, 30Gbps de IPS y 18,6 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 200.000 nuevas por segundo.
https://www.checkpoint.com/products-solutions/next-generation-firewalls/enterprise-firewall/check-point-security-appliances-comparison/

Observaciones

CCN-STIC 653 Seguridad en Check Point

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

Versión	R77.30
Familia	Cortafuegos
Fabricante	Check Point Software Technologies
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 4 Gbps de inspección Firewall, 1,44 Gbps de IPS y 740 Mbps para protección ante amenazas avanzadas. Un máximo de 3,2 millones de conexiones concurrentes y 48.000 nuevas por segundo.
https://www.checkpoint.com/products/3000-security-appliances/

Observaciones

CCN-STIC 653 Seguridad en Check Point

Check Point Security Gateway Serie 5000 (CPAP-SG5100-NGTX, CPAP-SG5200-NGTX, CPAP-SG5400-NGTX, CPAP-SG5600-NGTX, CPAP-SG5800-NGTX, CPAP-SG5900-NGTX)

Versión	R77.30
Familia	Cortafuegos
Fabricante	Check Point Software Technologies
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 52Gbps de inspección Firewall, 13,5Gbps de IPS y 6,75 Gbps para protección ante amenazas avanzadas. Un máximo de 12,8 millones de conexiones concurrentes y 185.000 nuevas por segundo.
https://www.checkpoint.com/products/5000-security-appliances/

Observaciones

CCN-STIC 653 Seguridad en Check Point

Licencias Check Point Open Server (CPSG-2C-NGTX, CPSG-4C-NGTX, CPSG-8C-NGTX, CPSG-16C-NGTX, CPSG-24C-NGTX, CPSG-32C-NGTX)

Versión	R77.30
Familia	Cortafuegos
Fabricante	Check Point Software Technologies
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Las licencias de Open Server ofrecen la posibilidad de instalar el software de Check Point en un appliance no propietario en base una lista certificada y probada por Check Point. Las funcionalidades serán las mismas que si de un hardware dedicado se tratase. Dependiendo del número de cores del gateway software, ofrece capacidades que van de 22Gbps a 128 Gbps de inspección Firewall, de 3,9 a 30 Gbps de IPS y de 1,745 a 18,6 Gbps para protección ante amenazas avanzadas.
Especificaciones:https://www.checkpoint.com/products/next-generation-threat-prevention/

Observaciones

Únicamente con las plataformas HW descritas en la declaración de seguridad de la certificación del producto.
CCN-STIC 653 Seguridad en Check Point

Smart1 Appliances (CPAP-NGSM405, CPAP-NGSM410, CPAP-NGSM225, CPAP-NGSM3050, CPAP-NGSM3150)

Versión	R77.30
Familia	Cortafuegos
Fabricante	Check Point Software Technologies
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Smart-1 es la solución hardware para el servidor que gestiona los Gateways de Check Point. Se trata de un hardware que puede combinar la definición de políticas, logs y monitorización aplicación normativa GDPR, y la correlación de eventos, en un solo dispositivo dedicado. Dependiendo del modelo, puede gestionar de 5 a más de 50 gateways y entre 6.000 y 44.000 registros de log indexados por segundo, con unas capacidades que oscilan entre los 16GB y los 256 GB de memoria RAM y entre los 2TB y 24TB de discoduro. Dispone de interfaces GBE, puerto consola y USB. Las versiones mayores también ofrecen la posibilidad de puertos de 10GbE y SAN fiber channel.
Especificaciones: https://www.checkpoint.com/downloads/product-related/datasheets/ds-smart-1-appliances.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

Smart1 Licencias Open Server (CPSM-NGSM5, CPSM-NGSM10, CPSM-NGSM25, CPSM-NGSM50, CPSM-NGSM150)

Versión	R77.30
Familia	Cortafuegos
Fabricante	Check Point Software Technologies
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Las licencias para open server ofrecen la posibilidad de desplegar la consola en un servidor genérico, obteniendo así las mismas funcionalidades que en Smart-1. Dependiendo del modelo tienen capacidad de gestionar de 5 a 150 gateways.
https://www.checkpoint.com/downloads/product-related/datasheets/ds-security-management.pdf

Observaciones

Únicamente con las plataformas HW descritas en la declaración de seguridad de la certificación del producto. Procedimiento de empleo pendiente de publicación.

ASA 5500 Series (5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40, 5585X SSP-60) con FireSIGHT Series (FCM) with FirePOWER

Versión	ASA 9.6.2 , ASDM 7.6 and FirePOWER 6.1
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/09/2018
Revisión de Validez	28/02/2020

Descripción

Los dispositivos de seguridad adaptables de Cisco con FirePOWER (FP) Services están diseñados para trabajar como
plataforma de firewall con capacidades VPN e IPS. Los dispositivos FMC proporcionan un sistema centralizado,
consola de administración y basede datos de eventos para los Servicios de FirePOWER, y agregados y correlaciona los datos de intrusión, descubrimiento y conexión de los Servicios de FirePOWER. En esta implementación, ASA proporciona VPN, filtro de firewall y pasa el tráfico al FirePOWER.
Dispositivos FirePOWER Management Center (FMC) compatibles: FireSIGHT (FS750, FS1500, FS2000, FS3500, FS4000)

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA 5500 Series (5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X, 5525-X, 5545-X, 5555-X) con FireSIGHT (FMC) y FMCv	
Versión	FTD 6.2
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	31/12/2019

Descripción

Cisco Firepower Threat Defense (FTD) es un appliance, virtual o físico, con capacidades de firewall, VPN e IPS. Ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).
Cisco FireSIGHT, también conocido como Cisco Firepower Management Center (FMC), es una appliance, virtual o físico, que proporciona una consola de gestión centralizada y una base de datos de eventos centralizados para el FTD y FTDv, con capacidades de agregación y correlación.
Cisco ASA, son firewalls de nueva generación que soportan el servicio Cisco Firepower para ofrecer conjuntamente los servicios de firewall, VPN e IPS.
Compatible con:
- FireSIGHT Series (FMC) FS750, FS1000, FS2000, FS2500, FS4000, FS4500
- FMCv running on ESXi 5.5 or 6.0on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E160S-M3, and E180D-M2/K9 installed on ISR

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA 5500 Series (5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X) and (5512-X, 5515-X, 5525-X, 5545-X, 5555-X).	
Versión	Platform version 9.6.2.
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

La serie Cisco ASA 5500-X Adaptative Security Appliance (Sw: ASA release 9.6.2) ofrece una gama de cortafuegos en formato de appliance físico. Con funcionalidades de cortafuegos stateful, capacidades VPN, mecanismos de alta disponibilidad y cluster.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA 5500-X Series
(5512-X, 5515-X, 5525-X, 5545-X, 5555-X)

Versión	Platform version 9.4(1).
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

La serie Cisco ASA 5500-X Adaptative Security Appliance (Sw: ASA release 9.4(1)) ofrece una gama de cortafuegos en formato de appliance físico. Con funcionalidades de cortafuegos stateful, capacidades VPN, mecanismos de alta disponibilidad y cluster. Posee 6-14 interfaces Gigabit Ethernet y soporta hasta 5.000 VPN.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA 5585 Series
(5585-X SSP-10, 5585-X SSP-20, 5585X-SSP-40, 5585X-SSP-60).

Versión	Platform version 9.6.2.
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

La serie ASA 5585-X Adaptative Security Appliance (Sw: ASA release 9.6.2) ofrece una gama de cortafuegos en formato de appliance físico. Con funcionalidades de cortafuegos stateful, capacidades VPN, mecanismos de alta disponibilidad y cluster.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA 5585-X Series (5585-10, 5585-20, 5585-40, 5585-60).	
Versión	Platform version 9.4(1).
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

La serie ASA 5585-X Adaptative Security Appliance (Sw: ASA release 9.4(1)) ofrece una gama de cortafuegos en formato de appliance físico. Con funcionalidades de cortafuegos stateful, capacidades VPN, mecanismos de alta disponibilidad y cluster. Posee 6-16 interfaces Gigabit Ethernet, 2-10 10Gigabit Ethernet y soporta hasta 10.000 VPN.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA Firepower 2100 Series: 2110, 2120, 2130, 2140	
Versión	FXOS 2.2, ASA 9.8.2 and ASDM 7.8
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/04/2019
Revisión de Validez	31/03/2020

Descripción

Los dispositivos de seguridad Cisco Firepower 2100 son plataformas escalables especialmente diseñadas con funciones de firewall y VPN provistas por el software Adaptive Security Appliances (ASA).

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA Firepower 4100 Series (4110, 4120, 4140, y 4150) and ASA Firepower 9300.	
Versión	ASA 9.6.2
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	31/05/2020

Descripción

Los dispositivos de seguridad Cisco Firepower 4100 y 9300 son plataformas escalables especialmente diseñadas con funciones de firewall y VPN provistas por el software Adaptive Security Appliances (ASA).

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA Firepower 4100 Series (4110, 4120, 4140, y 4150) and ASA Firepower 9300.	
Versión	FXOS 2.2, ASA 9.8 and ASDM 7.8
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2018
Revisión de Validez	31/05/2020

Descripción

Los dispositivos de seguridad Cisco Firepower 4100 y 9300 son plataformas escalables especialmente diseñadas con funciones de firewall y VPN provistas por el software Adaptive Security Appliances (ASA).

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA Services Module (ASA-SM)	
Versión	Platform version 9.6.2.
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

ASA-SM ofrece un módulo de cortafuegos para la serie Cisco Catalyst 6500. Con funcionalidades de cortafuegos stateful, capacidades VPN, mecanismos de alta disponibilidad y cluster.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA Services Module (ASA-SM) on Catalyst 6500 series switches (6503-E, 6504-E, 6509-E, 6513-E).

Versión	Platform version 9.4(1).
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

ASA-SM ofrece un módulo de cortafuegos para la serie Cisco Catalyst 6500. Con funcionalidades de cortafuegos stateful, capacidades VPN, mecanismos de alta disponibilidad y cluster. Permite un throughput de firewall máximo de 20 Gbps, 16 Gbps de throughput de firewall máximo (multiprotocolo), 300.000 conexiones por segundo, 10 millones de conexiones concurrentes y 250 contextos de seguridad.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASAv running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) (E140S M1, E140S M2, E140D M1, E160D M2, E160D M1, E180D M2, E140DP M1, E160DP M1) installed on ISR

Versión	Platform version 9.6.2.
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Cisco ASAv (ASA Virtual Appliance, release 9.6.2) es una plataforma de firewall virtual que ofrece funcionalidades de cortafuegos stateful, capacidades VPN y mecanismos de alta disponibilidad y cluster. Puede correr en hipervisores Vmware, KVM, Hiper-V yCitrix Xen

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASAv running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) B22 M3, B200 M3, B200 M4, B230 M2, B260 M4, B420 M3, B420 M4, B440 M2, B460 M4, C22 M3, C24 M3, C220 M3, C220 M4, C240 M3, C240 M4, C260 M2 and C460 M4, C240 M3, C240 M4, C260 M2, and C

Versión	Platform version 9.6.2.
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

consola de administración y base de datos de eventos para los Servicios de FirePOWER, y agregados y

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Firepower 2100 Series: FP2110, FP2120, FP2130, FP2140 con FireSIGHT (FMC) y FMCv

Versión	FTD 6.2, FXOS 2.2 y FMC/FCMv 6.2
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Cisco Firepower Threat Defense (FTD) es un appliance, virtual o físico, que tiene las 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:
-FireSIGHT Series (FMC) FS750, FS1000, FS2000, FS3500, FS4000, FS4500
- FMCv: running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E180D-M2/K9and E160S-M3

Observaciones

Procedimiento de empleo seguro pendiente de publicación.
Los dispositivos deben trabajar en “CC mode”

FP 4100 Series: FP4110, FP4120, FP4140, FP4150 con FireSIGHT (FMC) y FMCv

Versión	FTD 6.2, FXOS 2.2 y FMC/FCMv 6.2
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Cisco Firepower Threat Defense (FTD) es un appliance, virtual o físico, que tiene las 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:
-FireSIGHT Series (FMC) FS750, FS1000, FS2000, FS3500, FS4000, FS4500
- FMCv: running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E180D-M2/K9and E160S-M3

Observaciones

Procedimiento de empleo seguro pendiente de publicación.
Los dispositivos deben trabajar en “CC mode”

FTDv running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E160S-M3, and E180D-M2/K9 installed on ISR con FireSIGHT (FMC) y FMCv

Versión	FMC/FCMv 6.2
Familia	Cortafuegos
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	31/12/2019

Descripción

Cisco Firepower Threat Defense (FTD) es un appliance, virtual o físico, con capacidades de firewall, VPN e IPS. Ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).
Cisco FireSIGHT, también conocido como Cisco Firepower Management Center (FMC), es una appliance, virtual o físico, que proporciona una consola de gestión centralizada y una base de datos de eventos centralizados para el FTD y FTDv, con capacidades de agregación y correlación.
Cisco ASA, son firewalls de nueva generación que soportan el servicio Cisco Firepower para ofrecer conjuntamente los servicios de firewall, VPN e IPS.
Compatible con:
- FireSIGHT Series (FMC) FS750, FS1000, FS2000, FS2500, FS4000, FS4500
- FMCv running on ESXi 5.5 or 6.0on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E160S-M3, and E180D-M2/K9 installed on ISR

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Forcepoint NGFW 1100 Series y 2100 Series (NGFW 1101, NGFW 1105, NGFW 2101 y NGFW 2105)

Versión	SW: 6.3.1
Familia	Cortafuegos
Fabricante	Forcepoint
Categoría	ENS ALTO
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2022

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 hasta un rendimiento de 3 Gbps de Throughput NGFW/NGIPS, 20 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

Forcepoint NGFW 3300 Series (NGFW 3301 y NGFW 3305)	
Versión	SW: 6.3.1
Familia	Cortafuegos
Fabricante	Forcepoint
Categoría	ENS ALTO
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2022

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 15 Gbps de Throughput NGFW/NGIPS, 50 millones de conexiones concurrentes y 250 contextos virtuales. Más información en:
https://www.forcepoint.com/environments/forcepoint-ngfw-appliances

Observaciones

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

Forcepoint NGFW 6200 Series (NGFW 6205)	
Versión	SW: 6.3.1
Familia	Cortafuegos
Fabricante	Forcepoint
Categoría	ENS ALTO
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2022

Descripción

Firewall de Nueva Generación orientado a Grandes Empresas y Datacenters, de tipo appliance físico en formato chasis de 4RU, IPS, SD-WAN, URL Filtering y Detección Avanzada de Malware. Proporciona un rendimiento de hasta de 22 Gpbs de Throughput NGFW/NGIPS, 60 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

FG-1000D, FG-1200D, FG-1500D, FG-2000E, FG-2500E	
Versión	FortiOS 5.6
Familia	Cortafuegos
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos que incluyen diferentes procesadores de seguridad para proporcionar mayor rendimiento en entornos grandes, tanto para protección perimetral como para centro de proceso de datos o segmentación interna. Las funcionalidades de seguridad son similares a las del resto de modelos (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, capacidades SDWAN, etc,, como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf)
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

FG-100E, FG-100EF, FG-101E, FG-140E, FG-140EPoE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG- 501E, FG-600D, FG-900D	
Versión	FortiOS 5.6
Familia	Cortafuegos
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos que incluyen procesadores de seguridad para proporcionar mayor rendimiento en entornos de tamaño medio. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (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, capacidades SDWAN, etc.,como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf)
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

FG-3000D, FG-3100D, FG-3200D, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG- 3960E, FG-3980E	
Versión	FortiOS 5.6
Familia	Cortafuegos
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos que incluyen diferentes procesadores de seguridad para proporcionar mayor rendimiento en entornos muy grandes, tanto para protección perimetral como para centro de proceso de datos o segmentación interna. Las funcionalidades de seguridad son similares a las del resto de modelos (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, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf)
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

FG-30E, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-PoE, FG-61E, FG-80E, FG-80E- PoE, FG-81E, FG-81E-PoE	
Versión	FortiOS 5.6
Familia	Cortafuegos
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (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, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

FG-5001D, FG-5001E	
Versión	FortiOS 5.6
Familia	Cortafuegos
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC en formato chasis. Incluyen diferentes procesadores de seguridad para proporcionar mayor rendimiento en grandes centros de procesos de datos, proveedores de servicios de seguridad gestionada y compañías de telecomunicaciones. Las funcionalidades de seguridad son similares a las del resto de modelos (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadasy ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf)
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

FWF-30E, FWF-50E,FWF-51E, FWF-60E, FWF-60EDSL, FWF-61E	
Versión	FortiOS 5.6
Familia	Cortafuegos
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (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, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Junos 12.3X48 for SRX Platforms SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650, SRX5400, SRX5400E, SRX5600 y SRX5600E, SRX5800 y SRX5800E with SPC-4-15-320.

Versión	SW: Junos 12.3X48-D30
Familia	Cortafuegos
Fabricante	Juniper Networks
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 "Procedimiento de Empleo Seguro Plataformas SRX Juniper"

Junos 12.3X48-D30 for SRX XLR Platforms SRX1400, SRX3400 and SRX3600; SRX5400, SRX5400E, SRX5600, SRX5600E, SRX5800E with SPC-2-10-20.

Versión	SW: Junos 12.3X48-D30
Familia	Cortafuegos
Fabricante	Juniper Networks
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 "Procedimiento de Empleo Seguro Plataformas SRX Juniper"

Junos 15.1X49-D60 for SRX platforms
SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400E, SRX5400X, SRX5600E, SRX5600X, SRX5800E and SRX 5800X

Versión	SW: Junos 15.1X49-D60
Familia	Cortafuegos
Fabricante	Juniper Networks
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 "Procedimiento de Empleo Seguro Plataformas SRX Juniper"

PA-200 Series (PA-220, PA-220R), PA-500, PA-800 Series(820, PA-850)

Versión	PAN-OS v8.0.12 y v8.1.3
Familia	Cortafuegos
Fabricante	Palo Alto Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

Descripción

Firewalls de Nueva Generación orientados a pequeñas oficinas y sedes remotas, 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

Procedimiento de empleo seguro pendiente de publicación.

PA-3000 Series (PA-3020, PA-3050, PA-3060) y PA-3200 Series (PA-3220, PA-3250, PA-3260)	
Versión	PAN-OS v8.0.12 y v8.1.3
Familia	Cortafuegos
Fabricante	Palo Alto Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

Descripción

Firewalls de Nueva Generación orientados a empresas u organismos de tamaño medio, 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

Procedimiento de empleo seguro pendiente de publicación.

PA-5000 Series (PA-5020, PA-5050, PA-5060) y PA-5200 Series (PA-5220, PA-5250, PA-5260, PA-5280)	
Versión	PAN-OS v8.0.12 y v8.1.3
Familia	Cortafuegos
Fabricante	Palo Alto Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

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.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

PA-7000 Series (PA-7050, PA-7080)	
Versión	PAN-OS v8.0.12 y v8.1.3
Familia	Cortafuegos
Fabricante	Palo Alto Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

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.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

VM Series (VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000-HV)	
Versión	PAN-OS v8.0.12 y v8.1.3
Familia	Cortafuegos
Fabricante	Palo Alto Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

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.
ESon 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

Procedimiento de empleo seguro pendiente de publicación.

Serie SOHO (SOHOW)	
Versión	SonicOS 6.5.2
Familia	Cortafuegos
Fabricante	SonicWall
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	31/05/2020

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

Procedimiento de empleo seguro pendiente de publicación.

SonicWall NSA Serie (2650, 3600, 3650, 4600, 4650, 5600, 5650, 6600, 6650, 9250, 9450, 9650)	
Versión	SonicOS 6.5.2
Familia	Cortafuegos
Fabricante	SonicWall
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	30/01/2020

Descripción

Los firewall de la serie NSa de SonicWall están indicados para compañías medianas / grandes (de entre 50 y 3000 usuarios aprox), 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. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/mid-range

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

SonicWall SM Serie (9200, 9400, 9600, 9800)	
Versión	SonicOS 6.5.2
Familia	Cortafuegos
Fabricante	SonicWall
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	30/01/2020

Descripción

Diseñado 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. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/high-end

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

SonicWall TZ Serie (300/W, 400/W, 500/W, 600)	
Versión	SonicOS 6.5.2
Familia	Cortafuegos
Fabricante	SonicWall
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	30/01/2020

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

Procedimiento de empleo seguro pendiente de publicación.

7.4.4 FAMILIA: PROXIES

Blue Coat ProxySG S400 and S500

Versión	SW: SGOS v6.5
Familia	Proxies
Fabricante	Symantec Corporation
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	30/11/2019

Descripción

Los dispositivos Blue Coat ProxySG S400 y ProxySG S500 con la versión software SGOS v6.5 realizan la función de proxy multiprotocolo (http, https, ftp, DNS, MAPI, diversos protocols de streaming de contenido multimedia, webex, CIFS, RPC) y pueden funcionar tanto como proxies directos (para la protección y control de usuarios) como proxies inversos con firewall de aplicaciones web, para la protección de servidores de aplicaciones web. El propósito de estos dispositivos es proporcionar una capa de seguridadentre la red Interna y una o más redes externas (típicamente una red corporativa e Internet), aislando el tráfico de los usuarios a nivel de aplicación (torre OSI) y proporcionando demás diferentes mecanismos de optimización WAN para el tráfico que procesan.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Symantec SSL Visibility Appliance
SV1800-C, SV-1800-F, SV1800B-C, SV1800B-F, SV2800, SV2800B, SV3800, SV3800B, SV-3800B-20

Versión	SW: 3.10.2.1-21-FIPS140
Familia	Proxies
Fabricante	Symantec Corporation
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	30/11/2019

Descripción

El SSL Visibility Appliance permite detectar y bloquear amenazas de ciberseguridad contenidas en el tráfico cifrado mediante SSL/TLS. Para ello, realiza intercepción y descifrado selectivo de tráfico SSL/TLS y lo envía, junto con el tráfico no cifrado, auno o más dispositivos de seguridad de red de terceros fabricantes como pueden ser IPS/IDS, sistemas de Prevención de Pérdida de Datos (DLP) ó dispositivos de análisis forense de red. El SSL Visibility Appliance proporciona una versión no cifrada del tráfico SSL/TLS al dispositivo asociado sin requerir la remodelación de la infraestructura de la red, mientras mantiene una conexión SSL/TLS extremo a extremo entre el cliente y el servidor involucrados en la sesión.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

7.4.5 FAMILIA: DISPOSITIVOS DE RED INALÁMBRICOS

Aruba 7005, 7010, 7024, 7030, 7205, 7210, 7220, 7240 Mobility Controllers (FIPS)

Versión 6.5.4.13

Familia Dispositivos de Red Inalámbricos

Fabricante Aruba

Categoría ENS ALTO

Fecha Inclusión 01/06/2018

Revisión de Validez 31/05/2020

Descripción

Las controladoras Aruba junto con los puntos de acceso proporcionan autenticación, encriptación, servicios de túneles, servicios IPv4 y IPv6. Permite el despliegue de servicios inalámbricos con altos standards de seguridad. Ofrecen funcionalidades de monitorización inalámbricas para detección de amenazas inalámbricas, antes las cuales se pueden ejecutar funcionalidades de defensa activa.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Aruba AP-[204, 205, 214, 215, 224, 225, 274, 275, 277] Access Points

Versión 6.5.4.13

Familia Dispositivos de Red Inalámbricos

Fabricante Aruba

Categoría ENS ALTO

Fecha Inclusión 01/06/2018

Revisión de Validez 31/05/2020

Descripción

Las controladoras Aruba junto con los puntos de acceso proporcionan autenticación, encriptación, servicios de túneles, servicios IPv4 y IPv6. Permite el despliegue de servicios inalámbricos con altos standards de seguridad. Ofrecen funcionalidades de monitorización inalámbricas para detección de amenazas inalámbricas, antes las cuales se pueden ejecutar funcionalidades de defensa activa

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Aruba Mobility Controller Series (7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM) with ArubaOS and Access Points.

Versión	ArubaOS 8.2.
Familia	Dispositivos de Red Inalámbricos
Fabricante	Aruba
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

Aruba Mobility Controller Series funcionan como gateway entre redes cableadas e inalámbricas y proveen funciones de comando y control sobre los puntos de acceso de Aruba (APs) dentro de una red inalámbrica Aruba. Los Mobility Controllers (MC) y Virtual Mobility Controllers (VMC) de Aruba, son switches inalámbricos (Appliance físicos o virtuales) que proporcionan una amplia gama de servicios y características de seguridad que incluyen la movilidad de red inalámbrica y cableada, seguridad, administración centralizada, auditoría, autenticación, acceso remoto seguro, auto-chequeos de integridad y operación, filtrado de tráfico y funcionalidad de Gateway VPN. Los puntos de acceso (AP) de ARUBA compatibles con Aruba Mobility Controller son: AP-203R , AP-203RP ,AP-204 , AP-205 , AP-205H , AP-214 , AP-215 , AP-224 , AP-225 , AP-228 , AP-274 , AP-275 , AP-277 , AP-303H , AP-304 , AP-305 , AP-314 , AP-315 , AP-324 , AP-325 , AP-334 , AP-335.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Aruba Virtual Mobility Controller Series (MC-VA-50, MV-VA-250, MC-VA-1K) with ArubaOS and Access Points.

Versión	ArubaOS 8.2.
Familia	Dispositivos de Red Inalámbricos
Fabricante	Aruba
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

Aruba Mobility Controller Series funcionan como gateway entre redes cableadas e inalámbricas y proveen funciones de comando y control sobre los puntos de acceso de Aruba (APs) dentro de una red inalámbrica Aruba. Los Mobility Controllers (MC) y Virtual Mobility Controllers (VMC) de Aruba, son switches inalámbricos (Appliance físicos o virtuales) que proporcionan una amplia gama de servicios y características de seguridad que incluyen la movilidad de red inalámbrica y cableada, seguridad, administración centralizada, auditoría, autenticación, acceso remoto seguro, auto-chequeos de integridad y operación, filtrado de tráfico y funcionalidad de Gateway VPN. Los puntos de acceso (AP) de ARUBA compatibles con Aruba Mobility Controller son: AP-203R , AP-203RP ,AP-204 , AP-205 , AP-205H , AP-214 , AP-215 , AP-224 , AP-225 , AP-228 , AP-274 , AP-275 , AP-277 , AP-303H , AP-304 , AP-305 , AP-314 , AP-315 , AP-324 , AP-325 , AP-334 , AP-335.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

RAP-3WN Access Point, RAP-108 Remote Access Point, RAP-109 Remote Access Point	
Versión	6.5.4.13
Familia	Dispositivos de Red Inalámbricos
Fabricante	Aruba
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	31/05/2020

Descripción

Las controladoras Aruba junto con los puntos de acceso proporcionan autenticación, encriptación, servicios de túneles, servicios IPv4 y IPv6. Permite el despliegue de servicios inalámbricos con altos standards de seguridad. Ofrecen funcionalidades de monitorización inalámbricas para detección de amenazas inalámbricas, antes las cuales se pueden ejecutar funcionalidades de defensa activa

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

7.4.6 PASARELAS SEGURAS DE INTERCAMBIO DE DATOS

PSTfile	
Versión	v4.4.2
Familia	Pasarelas seguras de intercambio de datos
Fabricante	Autek Ingeniería
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

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
Familia	Pasarelas seguras de intercambio de datos
Fabricante	Autek Ingeniería
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

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

7.4.7 FAMILIA: DIODOS DE DATOS

PSTdiode	
Versión	v1.0.0
Familia	Diodos de datos
Fabricante	Autek Ingeniería
Categoría	TODOS LOS NIVELES
Fecha Inclusión	01/09/2019
Revisión de Validez	28/02/2022

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 esla 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

7.4.8 FAMILIA: REDES PRIVADAS VIRTUALES: IPSEC

Aruba Mobility Controller Series (7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM) with ArubaOS and Access Points.

Versión	ArubaOS 8.2.
Familia	Redes privadas virtuales: IPSec
Fabricante	Aruba
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

Aruba Mobility Controller Series funcionan como gateway entre redes cableadas e inalámbricas y proveen funciones de comando y control sobre los puntos de acceso de Aruba (APs) dentro de una red inalámbrica Aruba. Los Mobility Controllers (MC) y Virtual Mobility Controllers (VMC) de Aruba, son switches inalámbricos (Appliance físicos o virtuales) que proporcionan una amplia gama de servicios y características de seguridad que incluyen la movilidad de red inalámbrica y cableada, seguridad, administración centralizada, auditoría, autenticación, acceso remoto seguro, auto-chequeos de integridad y operación, filtrado de tráfico y funcionalidad de Gateway VPN. Los puntos de acceso (AP) de ARUBA compatibles con Aruba Mobility Controller son: AP-203R , AP-203RP ,AP-204 , AP-205 , AP-205H , AP-214 , AP-215 , AP-224 , AP-225 , AP-228 , AP-274 , AP-275 , AP-277 , AP-303H , AP-304 , AP-305 , AP-314 , AP-315 , AP-324 , AP-325 , AP-334 , AP-335.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Aruba Virtual Mobility Controller Series (MC-VA-50, MV-VA-250, MC-VA-1K) with ArubaOS and Access Points.	
Versión	ArubaOS 8.2.
Familia	Redes privadas virtuales: IPSec
Fabricante	Aruba
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

Aruba Mobility Controller Series funcionan como gateway entre redes cableadas e inalámbricas y proveen funciones de comando y control sobre los puntos de acceso de Aruba (APs) dentro de una red inalámbrica Aruba. Los Mobility Controllers (MC) y Virtual Mobility Controllers (VMC) de Aruba, son switches inalámbricos (Appliance físicos o virtuales) que proporcionan una amplia gama de servicios y características de seguridad que incluyen la movilidad de red inalámbrica y cableada, seguridad, administración centralizada, auditoría, autenticación, acceso remoto seguro, auto-chequeos de integridad y operación, filtrado de tráfico y funcionalidad de Gateway VPN. Los puntos de acceso (AP) de ARUBA compatibles con Aruba Mobility Controller son: AP-203R , AP-203RP ,AP-204 , AP-205 , AP-205H , AP-214 , AP-215 , AP-224 , AP-225 , AP-228 , AP-274 , AP-275 , AP-277 , AP-303H , AP-304 , AP-305 , AP-314 , AP-315 , AP-324 , AP-325 , AP-334 , AP-335.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Check Point Security Gateway Serie 15000 (CPAP-SG15400-NGTX, CPAP-SG15600-NGTX)	
Versión	R77.30
Familia	Redes privadas virtuales: IPSec
Fabricante	Check Point Software Technologies
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 76Gbps de inspección Firewall, 18Gbps de IPS y 13,11Gbps para protección ante amenazas avanzadas. Un máximo de 12.8 millones de conexiones concurrentes y 185.000 nuevas por segundo.
https://www.checkpoint.com/products/15000-security-appliances/

Observaciones

CCN-STIC 653 Seguridad en Check Point

Check Point Security Gateway Serie 23000 (CPAP-SG23500-NGTX, CPAP-SG23800-NGTX)

Versión	R77.30
Familia	Redes privadas virtuales: IPSec
Fabricante	Check Point Software Technologies
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Son dispositivos dedicados y 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, 30Gbps de IPS y 18,6 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 200.000 nuevas por segundo.
https://www.checkpoint.com/products-solutions/next-generation-firewalls/enterprise-firewall/check-point-security-appliances-comparison/

Observaciones

CCN-STIC 653 Seguridad en Check Point

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

Versión	R77.30
Familia	Redes privadas virtuales: IPSec
Fabricante	Check Point Software Technologies
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 4 Gbps de inspección Firewall, 1,44 Gbps de IPS y 740 Mbps para protección ante amenazas avanzadas. Un máximo de 3,2 millones de conexiones concurrentes y 48.000 nuevas por segundo.
https://www.checkpoint.com/products/3000-security-appliances/

Observaciones

CCN-STIC 653 Seguridad en Check Point

Check Point Security Gateway Serie 5000 (CPAP-SG5100-NGTX, CPAP-SG5200-NGTX, CPAP-SG5400-NGTX, CPAP-SG5600-NGTX, CPAP-SG5800-NGTX, CPAP-SG5900-NGTX)

Versión	R77.30
Familia	Redes privadas virtuales: IPSec
Fabricante	Check Point Software Technologies
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 52Gbps de inspección Firewall, 13,5Gbps de IPS y 6,75 Gbps para protección ante amenazas avanzadas. Un máximo de 12,8 millones de conexiones concurrentes y 185.000 nuevas por segundo.
https://www.checkpoint.com/products/5000-security-appliances/

Observaciones

CCN-STIC 653 Seguridad en Check Point

Licencias Check Point Open Server (CPSG-2C-NGTX, CPSG-4C-NGTX, CPSG-8C-NGTX, CPSG-16C-NGTX, CPSG-24C-NGTX, CPSG-32C-NGTX)

Versión	R77.30
Familia	Redes privadas virtuales: IPSec
Fabricante	Check Point Software Technologies
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Las licencias de Open Server ofrecen la posibilidad de instalar el software de Check Point en un appliance no propietario en base una lista certificada y probada por Check Point. Las funcionalidades serán las mismas que si de un hardware dedicado se tratase. Dependiendo del número de cores del gateway software, ofrece capacidades que van de 22Gbps a 128 Gbps de inspección Firewall, de 3,9 a 30 Gbps de IPS y de 1,745 a 18,6 Gbps para protección ante amenazas avanzadas.
https://www.checkpoint.com/products/next-generation-threat-prevention/

Observaciones

Únicamente con las plataformas HW descritas en la declaración de seguridad de la certificación del producto.
CCN-STIC 653 Seguridad en Check Point

ASA 5500 Series (5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40, 5585X SSP-60) con FireSIGHT Series (FCM) with FirePOWER

Versión	ASA 9.6.2 , ASDM 7.6 and FirePOWER 6.1
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/09/2018
Revisión de Validez	28/02/2020

Descripción

Los dispositivos de seguridad adaptables de Cisco con FirePOWER (FP) Services están diseñados para trabajar como
plataforma de firewall con capacidades VPN e IPS. Los dispositivos FMC proporcionan un sistema centralizado,
consola de administración y basede datos de eventos para los Servicios de FirePOWER, y agregados y correlaciona los datos de intrusión, descubrimiento y conexión de los Servicios de FirePOWER. En esta implementación, ASA proporciona VPN, filtro de firewall y pasa el tráfico al FirePOWER.
Dispositivos FirePOWER Management Center (FMC) compatibles: FireSIGHT (FS750, FS1500, FS2000, FS3500, FS4000)

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA 5500 Series (5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X, 5525-X, 5545-X, 5555-X) con FireSIGHT (FMC) y FMCv

Versión	FTD 6.2
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	31/12/2019

Descripción

Cisco Firepower Threat Defense (FTD) es un appliance, virtual o físico, con capacidades de firewall, VPN e IPS. Ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).
Cisco FireSIGHT, también conocido como Cisco Firepower Management Center (FMC), es una appliance, virtual o físico, que proporciona una consola de gestión centralizada y una base de datos de eventos centralizados para el FTD y FTDv, con capacidades de agregación y correlación.
Cisco ASA, son firewalls de nueva generación que soportan el servicio Cisco Firepower para ofrecer conjuntamente los servicios de firewall, VPN e IPS.
Compatible con:
- FireSIGHT Series (FMC) FS750, FS1000, FS2000, FS2500, FS4000, FS4500
- FMCv running on ESXi 5.5 or 6.0on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E160S-M3, and E180D-M2/K9 installed on ISR

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA 5500 Series (5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X) and (5512-X, 5515-X, 5525-X, 5545-X, 5555-X)

Versión	Platform version 9.6.2.
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

La serie Cisco ASA 5500-X Adaptative Security Appliance (Sw: ASA release 9.6.2) ofrece una gama de cortafuegos en formato de appliance físico. Con funcionalidades de cortafuegos stateful, capacidades VPN, mecanismos de alta disponibilidad y cluster.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA 5585 Series
(5585-X SSP-10, 5585-X SSP-20, 5585X-SSP-40, 5585X-SSP-60).

Versión	Platform version 9.6.2.
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

La serie ASA 5585-X Adaptative Security Appliance (Sw: ASA release 9.6.2) ofrece una gama de cortafuegos en formato de appliance físico. Con funcionalidades de cortafuegos stateful, capacidades VPN, mecanismos de alta disponibilidad y cluster.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA Firepower 2100 Series: 2110, 2120, 2130, 2140

Versión	FXOS 2.2, ASA 9.8.2 and ASDM 7.8
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/04/2019
Revisión de Validez	31/03/2020

Descripción

Los dispositivos de seguridad Cisco Firepower 2100 son plataformas escalables especialmente diseñadas con funciones de firewall y VPN provistas por el software Adaptive Security Appliances (ASA).

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA Firepower 4100 Series (4110, 4120, 4140, y 4150) and ASA Firepower 9300.

Versión	ASA 9.6.2
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	31/05/2020

Descripción

Los dispositivos de seguridad Cisco Firepower 4100 y 9300 son plataformas escalables especialmente diseñadas con funciones de firewall y VPN provistas por el software Adaptive Security Appliances (ASA).

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA Firepower 4100 Series (4110, 4120, 4140, y 4150) and ASA Firepower 9300.	
Versión	FXOS 2.2, ASA 9.8 and ASDM 7.8
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2018
Revisión de Validez	31/05/2020

Descripción

Los dispositivos de seguridad Cisco Firepower 4100 y 9300 son plataformas escalables especialmente diseñadas con funciones de firewall y VPN provistas por el software Adaptive Security Appliances (ASA).

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASA Services Module (ASA-SM)	
Versión	Platform version 9.6.2.
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

ASA-SM ofrece un módulo de cortafuegos para la serie Cisco Catalyst 6500. Con funcionalidades de cortafuegos stateful, capacidades VPN, mecanismos de alta disponibilidad y cluster.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASAv running on ESXi 5.5 or 6.0 (E140S M1, E140S M2, E140D M1, E160D M2, E160D M1, E180D M2, E140DP M1, E160DP M1) installed on ISR

Versión	Platform version 9.6.2.
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Cisco ASAv (ASA Virtual Appliance, release 9.6.2) es una plataforma de firewall virtual que ofrece funcionalidades de cortafuegos stateful, capacidades VPN y mecanismos de alta disponibilidad y cluster. Puede correr en hipervisores Vmware, KVM, Hiper-V yCitrix Xen

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASAv running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) B22 M3, B200 M3, B200 M4, B230 M2, B260 M4, B420 M3, B420 M4, B440 M2, B460 M4, C22 M3, C24 M3, C220 M3, C220 M4, C240 M3, C240 M4, C260 M2 and C460 M4, C240 M3, C240 M4, C260 M2, and C

Versión	Platform version 9.6.2.
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Cisco ASAv (ASA Virtual Appliance, release 9.6.2) es una plataforma de firewall virtual que ofrece funcionalidades de cortafuegos stateful, capacidades VPN y mecanismos de alta disponibilidad y cluster. Puede correr en hipervisores Vmware, KVM, Hiper-V yCitrix Xen

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASR 1000 Series: 1001-X, 1001-HX, 1002-HX, 1006-X, 1009-X, 1013.	
Versión	IOS XE 16.3
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	31/05/2020

Descripción

La serie Agregation Services Router (ASR) 1000 de CISCO es una plataforma de enrutamiento que entrega aceleración de hardware integrada para múltiples servicios de software Cisco IOS-XE. En apoyo a las capacidades de enrutamiento, Cisco ASR1K proporcionacapacidades de conexión IPsec para facilitar la seguridad comunicaciones con entidades externas, según sea necesario. Los Cisco ASR1kK son soluciones de enrutamiento y seguridad de dispositivo único para proteger la red.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ASR1K-1004	
Versión	IOS XE 16.3
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	31/05/2020

Descripción

La serie ASR1K de Cisco ofrece aceleración de hardware integrada para múltiples servicios de Cisco IOS-XE Software. Además, los enrutadores de Cisco de la serie ASR1K presentan enrutado redundante y procesadores de servicios integrados, así como redundancia basada en software. Cisco ASR1K proporciona capacidades de conexión IPsec para comunicaciones seguras.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Firepower 2100 Series: FP2110, FP2120, FP2130, FP2140 con FireSIGHT (FMC) y FMCv

Versión	FTD 6.2, FXOS 2.2 y FMC/FCMv 6.2
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Cisco Firepower Threat Defense (FTD) es un appliance, virtual o físico, que tiene las 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:
-FireSIGHT Series (FMC) FS750, FS1000, FS2000, FS3500, FS4000, FS4500
- FMCv: running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E180D-M2/K9and E160S-M3

Observaciones

Procedimiento de empleo seguro pendiente de publicación.
Los dispositivos deben trabajar en "CC mode"

FP 4100 Series: FP4110, FP4120, FP4140, FP4150 con FireSIGHT (FMC) y FMCv

Versión	FTD 6.2, FXOS 2.2 y FMC/FCMv 6.2
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Cisco Firepower Threat Defense (FTD) es un appliance, virtual o físico, que tiene las 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:
-FireSIGHT Series (FMC) FS750, FS1000, FS2000, FS3500, FS4000, FS4500
- FMCv: running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E180D-M2/K9and E160S-M3

Observaciones

Procedimiento de empleo seguro pendiente de publicación.
Los dispositivos deben trabajar en "CC mode"

FTDv running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E160S-M3, and E180D-M2/K9 installed on ISR con FireSIGHT (FMC) y FMCv

Versión	FMC/FCMv 6.2
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/07/2019
Revisión de Validez	31/12/2019

Descripción

Cisco Firepower Threat Defense (FTD) es un appliance, virtual o físico, con capacidades de firewall, VPN e IPS. Ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).
Cisco FireSIGHT, también conocido como Cisco Firepower Management Center (FMC), es una appliance, virtual o físico, que proporciona una consola de gestión centralizada y una base de datos de eventos centralizados para el FTD y FTDv, con capacidades de agregación y correlación.
Cisco ASA, son firewalls de nueva generación que soportan el servicio Cisco Firepower para ofrecer conjuntamente los servicios de firewall, VPN e IPS.
Compatible con:
- FireSIGHT Series (FMC) FS750, FS1000, FS2000, FS2500, FS4000, FS4500
- FMCv running on ESXi 5.5 or 6.0on the Unified Computing System (UCS) B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, E140S-M2/K9, E160S-M3, and E180D-M2/K9 installed on ISR

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ISR 1100 Series: C1111-8P, C1111-4P, C1112-8P, C1113-8P, C1114-8P, C1115-8P, C1116-4P, C1117-4P.

Versión	IOS XE 16.6
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/04/2019
Revisión de Validez	31/03/2020

Descripción

Cisco ISR 1100 es una plataforma de enrutamiento que brinda conectividad y servicios de seguridad. Cisco ISR ejecuta el software modular Cisco IOS-XE. En apoyo de las capacidades de enrutamiento, Cisco ISR 1100 proporciona capacidades de conexión IPsec para clientes habilitados para VPN.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

ISR 4000 Series: 4321, 4331, 4351, 4431, 4451-X	
Versión	IOS XE 16.3
Familia	Redes privadas virtuales: IPSec
Fabricante	Cisco Systems
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	31/05/2020

Descripción

Cisco ISR4K es una plataforma de enrutamiento que
ofrece aceleración de encriptación y brinda conectividad y servicios de seguridad. Cisco ISR ejecuta el software modular Cisco IOS-XE. En apoyo de las capacidades de enrutamiento, Cisco ISR4K proporciona capacidades de conexión IPsec para clientes habilitados para VPN.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

FG-1000D, FG-1200D, FG-1500D, FG-2000E, FG-2500E	
Versión	FortiOS 5.6
Familia	Redes privadas virtuales: IPSec
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos que incluyen diferentes procesadores de seguridad para proporcionar mayor rendimiento en entornos grandes, tanto para protección perimetral como para centro de proceso de datos o segmentación interna. Las funcionalidades de seguridad son similares a las del resto de modelos (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, capacidades SDWAN, etc,, como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf)
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

FG-100E, FG-100EF, FG-101E, FG-140E, FG-140EPoE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG- 501E, FG-600D, FG-900D

Versión	FortiOS 5.6
Familia	Redes privadas virtuales: IPSec
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos que incluyen procesadores de seguridad para proporcionar mayor rendimiento en entornos de tamaño medio. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (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, capacidades SDWAN, etc.,como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf)
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

FG-3000D, FG-3100D, FG-3200D, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG- 3960E, FG-3980E

Versión	FortiOS 5.6
Familia	Redes privadas virtuales: IPSec
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos que incluyen diferentes procesadores de seguridad para proporcionar mayor rendimiento en entornos muy grandes, tanto para protección perimetral como para centro de proceso de datos o segmentación interna. Las funcionalidades de seguridad son similares a las del resto de modelos (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, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf)
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

FG-30E, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-PoE, FG-61E, FG-80E, FG-80E- PoE, FG-81E, FG-81E-PoE

Versión	FortiOS 5.6
Familia	Redes privadas virtuales: IPSec
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (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, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

FG-5001D, FG-5001E

Versión	FortiOS 5.6
Familia	Redes privadas virtuales: IPSec
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/09/2019
Revisión de Validez	29/02/2020

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC en formato chasis. Incluyen diferentes procesadores de seguridad para proporcionar mayor rendimiento en grandes centros de procesos de datos, proveedores de servicios de seguridad gestionada y compañías de telecomunicaciones. Las funcionalidades de seguridad son similares a las del resto de modelos (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadasy ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf)
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

FWF-30E, FWF-50E,FWF-51E, FWF-60E, FWF-60EDSL, FWF-61E

Versión FortiOS 5.6

Familia Redes privadas virtuales: IPSec

Fabricante Fortinet

Categoría ENS ALTO

Fecha Inclusión 01/09/2019

Revisión de Validez 29/02/2020

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (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, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

IS101

Versión 1.01

Familia Redes privadas virtuales: IPSec

Fabricante ISTRIA SOLUCIONES DE CRIPTOGRAFIA

Categoría ENS ALTO

Fecha Inclusión 01/07/2018

Revisión de Validez 31/12/2020

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"

Junos 12.3X48 for SRX Platforms SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650, SRX5400, SRX5400E, SRX5600 y SRX5600E, SRX5800 y SRX5800E with SPC-4-15-320.

Versión	SW: Junos 12.3X48-D30
Familia	Redes privadas virtuales: IPSec
Fabricante	Juniper Networks
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 "Procedimiento de Empleo Seguro Plataformas SRX Juniper"

Junos 15.1X49-D60 for SRX platforms SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400E, SRX5400X, SRX5600E, SRX5600X, SRX5800E and SRX 5800X

Versión	SW: Junos 15.1X49-D60
Familia	Redes privadas virtuales: IPSec
Fabricante	Juniper Networks
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 "Procedimiento de Empleo Seguro Plataformas SRX Juniper"

PA-200 Series (PA-220, PA-220R), PA-500, PA-800 Series(820, PA-850)	
Versión	PAN-OS v8.0.12 y v8.1.3
Familia	Redes privadas virtuales: IPSec
Fabricante	Palo Alto Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

Descripción

Firewalls de Nueva Generación orientados a pequeñas oficinas y sedes remotas, 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

Procedimiento de empleo seguro pendiente de publicación.

PA-3000 Series (PA-3020, PA-3050, PA-3060) y PA-3200 Series (PA-3220, PA-3250, PA-3260)	
Versión	PAN-OS v8.0.12 y v8.1.3
Familia	Redes privadas virtuales: IPSec
Fabricante	Palo Alto Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

Descripción

Firewalls de Nueva Generación orientados a empresas u organismos de tamaño medio, 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

Procedimiento de empleo seguro pendiente de publicación.

PA-5000 Series (PA-5020, PA-5050, PA-5060) y PA-5200 Series (PA-5220, PA-5250, PA-5260, PA-5280)	
Versión	PAN-OS v8.0.12 y v8.1.3
Familia	Redes privadas virtuales: IPSec
Fabricante	Palo Alto Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

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.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

PA-7000 Series (PA-7050, PA-7080)	
Versión	PAN-OS v8.0.12 y v8.1.3
Familia	Redes privadas virtuales: IPSec
Fabricante	Palo Alto Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

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.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

VM Series (VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000-HV)	
Versión	PAN-OS v8.0.12 y v8.1.3
Familia	Redes privadas virtuales: IPSec
Fabricante	Palo Alto Networks
Categoría	ENS ALTO
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

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.
ESon 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

Procedimiento de empleo seguro pendiente de publicación.

Serie SOHO (SOHOW)	
Versión	SonicOS 6.5.2
Familia	Redes privadas virtuales: IPSec
Fabricante	SonicWall
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	31/05/2020

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

Procedimiento de empleo seguro pendiente de publicación.

SonicWall NSA Serie (2650, 3600, 3650, 4600, 4650, 5600, 5650, 6600, 6650, 9250, 9450, 9650)	
Versión	SonicOS 6.5.2
Familia	Redes privadas virtuales: IPSec
Fabricante	SonicWall
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	31/05/2020

Descripción

Los firewall de la serie NSa de SonicWall están indicados para compañías medianas / grandes (de entre 50 y 3000 usuarios aprox), 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. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/mid-range

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

SonicWall SM Serie (9200, 9400, 9600, 9800)	
Versión	SonicOS 6.5.2
Familia	Redes privadas virtuales: IPSec
Fabricante	SonicWall
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	31/05/2020

Descripción

Diseñado 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. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/high-end

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

SonicWall TZ Serie (300/W, 400/W, 500/W, 600)	
Versión	SonicOS 6.5.2
Familia	Redes privadas virtuales: IPSec
Fabricante	SonicWall
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	31/05/2020

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

Procedimiento de empleo seguro pendiente de publicación.

7.4.9 FAMILIA: REDES PRIVADAS VIRTUALES: SSL

Pulse Connect Secure (PSA-300, PSA-3000, PSA-5000, PSA-7000c, PSA-7000f)	
Versión	v8.2R12.1
Familia	Redes privadas virtuales: SSL
Fabricante	Pulse Secure
Categoría	ENS ALTO
Fecha Inclusión	01/12/2018
Revisión de Validez	31/05/2020

Descripción

La solución de acceso remoto Pulse Connect Secure (PCS) en la versión actual prevé una solución adaptativa para el acceso remoto corporativo a través de VPN SSL. Con capacidad de integración de elementos de terceros, como pueden ser soluciones de MDM, firewalls y soluciones de doble factor de autenticación.

Incorpora mecanismos de seguridad como Host Checker, para evaluar el cumplimiento de las normas de seguridad de los entes que se conectan de forma remota a la organización (patrones actualizados de AV, elementos en clave de registro, parcheado del sistema, firewall activo en el host, etc.).

Ofrece la posibilidad de prever el acceso a través de cliente pesado, que al mismo tiempo es capaz de actuar como cliente de la solución de NAC (PCS), o a través de acceso vía Navegador (HTML5) a los diferentes recursos corporativos (Aplicaciones, RDP, SSH, etc.)

Incluye capacidades añadidas para la federación con aplicativos de terceros en la Nube (SaaS), como pueden ser Office365, Salesforce, etc. y la habilidadde interactuar como iDP exclusivo o intermedio a través de la federación con SAML 2.0 con estos mismos servicios u otros proveedores de servicio como pueden ser Okta, Ping One, MS AD FS, etc.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

7.4.10 FAMILIA: HERRAMIENTAS PARA COMUNICACIONES MÓVILES SEGURAS

COMSec

Versión	v3.1
Familia	Herramientas para comunicaciones móviles seguras
Fabricante	Indra
Categoría	ENS ALTO
Fecha Inclusión	01/10/2018
Revisión de Validez	31/03/2021

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.

Observaciones

CCN-STIC-1407 Procedimiento de Empleo Seguro de COMSec

7.4.11 FAMILIA: CIFRADORES IP

EP430GN

Versión	1.08.29
Familia	Cifradores IP
Fabricante	Epicom
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2022

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.

EP430GX	
Versión	v.1.07
Familia	Cifradores IP
Fabricante	Epicom
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2021

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.

EP430TX	
Versión	1.04
Familia	Cifradores IP
Fabricante	Epicom
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	30/06/2020

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.

IS101	
Versión	1.01
Familia	Cifradores IP
Fabricante	ISTRIA SOLUCIONES DE CRIPTOGRAFIA
Categoría	ENS ALTO
Fecha Inclusión	01/07/2018
Revisión de Validez	31/12/2020

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

Procedimiento de empleo seguro pendiente de publicación.

7.5 CATEGORÍA: PROTECCIÓN DE LA INFORMACIÓN Y SOPORTES DE INFORMACIÓN

7.5.1 FAMILIA: ALMACENAMIENTO CIFRADO DE DATOS

Dell Data Protection | Encryption Personal Edition	
Versión	8.14.0
Familia	Almacenamiento cifrado de datos
Fabricante	Dell Computer
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	30/11/2019

Descripción

Esta herramienta software permite el cifrado de datos almacenados en estaciones de trabajo u ordenadores portátiles. Permite:
- Cifrado de datos por tipos de fichero o directorios específicos.
- Integración con los procesos existentes de identificación.
- Capacidad de cifrar basándose en perfiles de usuario, datos y grupos dentro de la organización.

Corre sobre Windows 8.1 (Entreprise, Pro) y Windows 10 (Enterprise, Pro).

Observaciones

Debe ejecuntarse sobre plataformas Dell Precision, Latitude o Optiplex. Procedimiento de empleo pendiente de publicación.

7.5.2 FAMILIA. CIFRADO OFFLINE

EP851	
Versión	2.02 y 2.03
Familia	Cifrado offline
Fabricante	Epicom
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2020

Descripción

Dispositivo portatil USB de cifrado "off-line":
• Compatible con Crypto Token USB de la empresa Datatech.
• Cifrado de ficheros para su posterior envío.
• Almacenamiento interno de la datos cifrados para su transporte.

Observaciones

Utilización según el PE-2008-01 Procedimiento de Empleo TOKEN USB.

7.5.3 FAMILIA: BORRADO SEGURO

Erase IT Core	
Versión	V1.0.3
Familia	Herramientas de borrado seguro
Fabricante	Recovery Labs
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

EraseIT Loop es el software que borra de forma segura, definitiva e irreversible todos los datos almacenados en los discos duros de un equipo informático, incluido el disco de sistema, permitiendo su reciclaje o reutilización.
Después de cada proceso de borrado, la aplicación genera un informe de borrado seguro, en base al cual Recovery Labs emite un Certificado de Borrado Seguro reflejando el método de borrado seleccionado.
Entre los estándares de sobreescritura más reconocidos hay que destacar: DoD 5220.22-M, NATO Standard, USNavy, NAVSO P-5239-26 –RLL,…

Observaciones

Procedimiento de empleo seguro: CCN-STIC 1501 Configuración segura de Herramienta de Borrado Seguro EraseIT Loop

7.5.4 FAMILIA: PREVENCIÓN DE FUGAS DE DATOS

Forcepoint On-Premise Security	
Versión	8.5
Familia	Sistemas para prevención de fugas de datos
Fabricante	Forcepoint
Categoría	ENS ALTO
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2020

Descripción

Forcepoint On-Premise Security 8.5 es una solución de prevención de fuga de datos en un organismo.Esta solución ofrece una alta escalabilidad de acuerdo con la estrategia del cliente para abordar el robo y la pérdida de datos.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Symantec Data Loss Prevention	
Versión	14.5
Familia	Sistemas para prevención de fugas de datos
Fabricante	Symantec Corporation
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	30/11/2019

Descripción

Symantec ™ Data Loss Prevention 14.5 es un producto utilizado por las organizaciones para proteger datos confidenciales como información de la empresa, datos de clientes, datos regulados y propiedad intelectual. Proporciona esta funcionalidad mediante eldescubrimiento, la supervisión y la protección de información confidencial sobre recursos de red dentro de la infraestructura de TI de una organización. La información confidencial puede incluir números de tarjetas de crédito, nombres, direcciones, números de identificación o cualquier dato que una compañía considere de propiedad y puede estar tanto en datos estructurados como no estructurados.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

7.5.5 FAMILIA. HERRAMIENTAS PARA FIRMA ELECTRÓNICA

ADSS Server SAM Appliance	
Versión	6.0
Familia	Herramientas para firma electrónica
Fabricante	ASCERTIA
Categoría	ENS ALTO
Fecha Inclusión	01/10/2019
Revisión de Validez	31/03/2020

Descripción

El ADSS Server SAM 6.0 es un dispositivo de creación de Firma Remota (rQSCD) de la empresa Ascertia, que cuenta con un certificado Common Criteria EAL4+ que cumple con la regulación Protection Profile EN 419241-2 con Level 2 Sole Control y que, junto a laaplicación de móviles Go>Sign de Ascertia, proporciona a sus usuarios la firma Remota Avanzada y Cualificada.

Observaciones

Procedimiento de empleo pendiente de publicación.

SIAVAL Safecert Server Signing Sistema	
Versión	v.2.4.02
Familia	Herramientas para firma electrónica
Fabricante	Sistemas Informáticos Abiertos
Categoría	ENS ALTO
Fecha Inclusión	01/12/2018
Revisión de Validez	31/05/2021

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.

7.6 CATEGORÍA: PROTECCIÓN DE EQUIPOS Y SERVICIOS

7.6.1 FAMILIA: DISPOSITIVOS MÓVILES

GALAXY Note 8 (SM-N950F)	
Versión	Android 8
Familia	Dispositivos móviles
Fabricante	Samsung Electronics
Categoría	ENS ALTO
Fecha Inclusión	01/04/2019
Revisión de Validez	30/07/2021

Descripción

Galaxy Note 8 es un Smartphone Samsung con Sistema operativo Android. Destaca por su pantalla de 6,3''. En su interior cuenta con procesador de 10nm, almacenamiento interno de 64GB que puede extenderse hasta los 256GB a través de microSD, y RAM de 6GB. Todo ello protegido con su plataforma Samsung Knox, certificación IP68.

Observaciones

Procedimiento de empleo: CCN-STIC 1604 Configuración segura de dispositivos Samsung Galaxy S9 con Android 8.

GALAXY Note 8 (SM-N950F)

Versión	Android 7
Familia	Dispositivos móviles
Fabricante	Samsung Electronics
Categoría	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

Galaxy Note 8 es un Smartphone Samsung con Sistema operativo Android. Destaca por su pantalla de 6,3''. En su interior cuenta con procesador de 10nm, almacenamiento interno de 64GB que puede extenderse hasta los 256GB a través de microSD, y RAM de 6GB. Todo ello protegido con su plataforma Samsung Knox, certificación IP68.

Observaciones

Procedimiento de empleo seguro: CCN-STIC 1601 Configuración Segura Samsung Galaxy S8/S8+

Galaxy Note 9 (SM-N960)

Versión	Android 8
Familia	Dispositivos móviles
Fabricante	Samsung Electronics
Categoría	ENS ALTO
Fecha Inclusión	01/10/2019
Revisión de Validez	31/07/2021

Descripción

Galaxy Note9 ofrece una experiencia PC permitiendo el trabajo con su función touchpad gracias a su S Pen. Cuenta con sistema operativo Android, pantalla de 6,4" con resolución Quad HD+.
Sus datos estarán protegidos con la plataforma de seguridad Samsung Knox
Memoria: interna 512 GB, externa hasta 512GB. RAM: 8GB

Observaciones

Procedimiento de empleo: CCN-STIC 1604 Configuración segura de dispositivos Samsung Galaxy S9 con Android 8.

GALAXY S8 (SM-G950F), GALAXY S8+ (SM-G955F)	
Versión	Android 7
Familia	Dispositivos móviles
Fabricante	Samsung Electronics
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Galaxy S8/S8+ es un smartphone Samsung con Sistema operativo Android. Destaca por su diseño curvo simétrico, con acabados en cristal y aluminio, con una pantalla inmersiva Infinity Display. En su interior cuenta con procesador de 10nm, almacenamiento interno de 64GB que puede extenderse hasta los 320GB a través de microSD, y RAM de de 4GB. Todo ello protegido con su plataforma Samsung Knox, certificación IP68.

Observaciones

Procedimiento de empleo seguro: CCN-STIC 1601 Configuración Segura Samsung Galaxy S8/S8+

GALAXY S8 (SM-G950F), GALAXY S8+ (SM-G955F)	
Versión	Android 8
Familia	Dispositivos móviles
Fabricante	Samsung Electronics
Categoría	ENS ALTO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

Descripción

Galaxy S8/S8+ es un smartphone Samsung con Sistema operativo Android. Destaca por su diseño curvo simétrico, con acabados en cristal y aluminio, con una pantalla inmersiva Infinity Display. En su interior cuenta con procesador de 10nm, almacenamiento interno de 64GB que puede extenderse hasta los 320GB a través de microSD, y RAM de de 4GB. Todo ello protegido con su plataforma Samsung Knox, certificación IP68.

Observaciones

Procedimiento de empleo: CCN-STIC 1604 Configuración segura de dispositivos Samsung Galaxy S9 con Android 8.

GALAXY S9 (SM-G960F), GALAXY S9+ (SM-G965F)

Versión	Android 8
Familia	Dispositivos móviles
Fabricante	Samsung Electronics
Categoría	ENS ALTO
Fecha Inclusión	01/02/2019
Revisión de Validez	31/07/2021

Descripción

Su diseño con pantalla infinita, su avanzada cámara o la certificación IP68, permite trabajar de forma más productiva, manteniendo al mismo tiempo lo estándares más altos de seguridad gracias a Samsung Knox. La plataforma de seguridad Samsung Knox está integrada en el hardware y operativa desde que enciende su smartphone. Ofrece múltiples capas de seguridad en tiempo real para mantener sus datos a salvo dentro de una carpeta segura. Dispone de una memoria de almacenamiento de 64 GB ampliables mediante microSD hasta 512GB más.

Observaciones

Procedimiento de empleo: CCN-STIC 1604 Configuración segura de dispositivos Samsung Galaxy S9 con Android 8.

Galaxy Tab S4 (SM-T830 / SM-T835)

Versión	Android 8
Familia	Dispositivos móviles
Fabricante	Samsung Electronics
Categoría	ENS ALTO
Fecha Inclusión	01/10/2019
Revisión de Validez	31/07/2021

Descripción

Galaxy Tab S4 viene equipado con un procesador Qualcomm MSM8998 AP para una ejecución más rápida y 4 GB de memoria RAM para un rendimiento más suave, ayudando a completar más tareas a la vez. Incorpora la plataforma de alta seguridad Samsung Knox con baseen el propio chip desde el primer momento en que enciende su tablet. Pantalla sAMOLED de 10.5". Incorpora un S Pen.

Observaciones

Procedimiento de empleo: CCN-STIC 1604 Configuración segura de dispositivos Samsung Galaxy S9 con Android 8.

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

Versión Android 9

Familia Dispositivos móviles

Fabricante Samsung Electronics

Categoría ENS ALTO

Fecha Inclusión 01/11/2019

Revisión de Validez 30/04/2022

Descripción

Los dispositivos Galaxy Note10, Note10+ y Note10+ 5G, incorporan el procesador Exynos 9825, permitiendoles ofrecer un mayor rendimiento y seguridad.
La familia de productos Galaxy Note10 protegen sus datos sensibles de ataques maliciosos y malware graciasa la plataforma de alta seguridad Samsung Knox que comienza en el propio chip desde el momento en que enciende su dispositivo, preservando los datos más sensibles de sus clientes y evitando posibles fugas de información.

Observaciones

CCN-STIC 1606 Configuración segura de dispositivos Samsung Galaxy S10 con Android 9

Samsung Galaxy S10 (SM-G973F), S10e (SM-G970F), S10+ (SM-G975F), S10 5G (SM-G977B)

Versión Android 9

Familia Dispositivos móviles

Fabricante Samsung Electronics

Categoría ENS ALTO

Fecha Inclusión 01/08/2019

Revisión de Validez 30/01/2022

Descripción

Los dispositivos de la Gama S10 son el fruto de 10 años de innovación en smartphones, y están preparados para afrontar los desafíos de cualquier sector empresarial. Toda la gama S10 cuenta con las mismas características a nivel empresarial: seguridad garantizada gracias a Samsung Knox, pantalla Infinita para una mejor experiencia de trabajo, un potente procesador, carga rápida e inalámbrica, sensor de huella (ultrasónico en el caso de S10+ y S10), y unas capacidades de altas prestaciones.

Observaciones

CCN-STIC 1606 Configuración segura de dispositivos Samsung Galaxy S10 con Android 9

Samsung Galaxy Tab Active2 4G (SM-T395), Tab Active2 Wi-Fi (SM-T390)	
Versión	Android 9
Familia	Dispositivos móviles
Fabricante	Samsung Electronics
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Galaxy Tab Active2 dispone de certificación MIL-STD 810G, está diseñada para soportar caídas de hasta 1,2 metros.
Para hacer frente a los entornos más extremos de trabajo, donde se requiere resistencia al agua y al polvo, tanto Galaxy Tab Active2 como su S Pen cuentan con certificado IP68.
El conector POGO pin integrado elimina la necesidad de emparejar dispositivos, y mejora la carga a través de docking stations.
Incorpora la plataforma de alta seguridad Samsung Knox que comienza en el propio chip desde el primer momento en que enciende su tableta, preservando los datos más sensibles de sus clientes y evitando posibles fugas de información.

Observaciones

CCN-STIC 1606 Configuración segura de dispositivos Samsung Galaxy S10 con Android 9

7.6.2 FAMILIA: SISTEMAS OPERATIVOS

Windows 10	
Versión	1709 Enterprise Edition
Familia	Sistemas Operativos
Fabricante	Microsoft Corporation
Categoría	ENS ALTO
Fecha Inclusión	01/12/2018
Revisión de Validez	14/04/2020

Descripción

Sistema Operativo para estaciones de trabajo, tanto en entornos reales como virtualizados.

Observaciones

CCN-STIC-599A18 Anexo A y CCN-STIC-599B18 Anexo A

Windows 10	
Versión	1809 Enterprise Edition
Familia	Sistemas Operativos
Fabricante	Microsoft Corporation
Categoría	ENS ALTO
Fecha Inclusión	01/10/2019
Revisión de Validez	11/05/2021
Descripción	
Sistema Operativo para estaciones de trabajo, tanto en entornos reales como virtualizados.	
Observaciones	
Procediminento de empleo: CCN-STIC-599A19 y CCN-STIC-599B19	

Windows Server 2012 R2	
Versión	Standard Edition, Datacenter Edition
Familia	Sistemas Operativos
Fabricante	Microsoft Corporation
Categoría	ENS ALTO
Fecha Inclusión	01/12/2018
Revisión de Validez	31/05/2021
Descripción	
Sistema Operativo para servidores	
Observaciones	
CCN-STIC-870A y CCN-STIC-870B	

Windows Server 2016	
Versión	Standard Edition, Datacenter Edition
Familia	Sistemas Operativos
Fabricante	Microsoft Corporation
Categoría	ENS ALTO
Fecha Inclusión	01/12/2018
Revisión de Validez	31/05/2021
Descripción	
Sistema Operativo para servidores	
Observaciones	
CCN-STIC-570A, CCN-STIC-570B Anexo A	

7.6.3 FAMILIA: ANTI-SPAM

FortiMail Appliances FML-2000E, FML-3000E, FML-3200E	
Versión	Firmware 6.0.2
Familia	anti-spam
Fabricante	Fortinet
Categoría	ENS ALTO
Fecha Inclusión	01/06/2019
Revisión de Validez	31/05/2020

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.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.
Requiere Fortinet Entropy Token V1

7.6.4 FAMILIA: TARJETAS INTELIGENTES

Pendiente de publicación los Requisitos Fundamentales de Seguridad (RFS) de esta familia.

7.6.5 FAMILIA: COPIAS DE SEGURIDAD

Familia hardware R6000

Versión	V. 4.1.2
Familia	Copias de seguridad
Fabricante	Rubrik
Categoría	ENS ALTO
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2021

Descripción

Rubrik es una plataforma convergente de gestión del dato en Cloud, Pública o Privada, que ofrece disponibilidad instantánea de la información para recuperación ante desastre, ataque Ransomware o pruebas de desarrollo. Solución definida por software que permite una operación sencilla, construida con arquitectura scale-out, basada en sistemas distribuidos, que reparten de forma inteligente y autónoma los datos, metadatos y tareas entre todos los nodos y miembros del clúster, permitiendo realizar búsquedas globales, indexadas y predictivas "google-like". Diseño API RESTful nativo 100%, que ofrece máxima integración, automatización y orquestación con la Cloud, para archivado a largo plazo, instanciación de máquinas virtuales o explotación de los metadatos. Permite el cumplimiento GDPR en el tratamiento de la información, certificado por metodología Common Criteria EAL2+. Cada appliance tiene tres o cuatro nodos, cada uno tiene su propio cómputo, discos SATA y discos SSD y se pueden combinar cualquiera de loscuatro modelos de appliance en un mismo cluster
-> https://www.rubrik.com/wp-content/uploads/2018/11/Rubrik-r6000-Specs-Sheet.pdf

Observaciones

CCN-STIC-1606 Procedimiento de Empleo Seguro Rubrik

Familia hardware R6000f

Versión	V. 4.1.2
Familia	Copias de seguridad
Fabricante	Rubrik
Categoría	ENS ALTO
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2021

Descripción

Appliance certificado FIPS 140-2 Level 2. Cada appliance tiene cuatro nodos y cada uno tiene su propio cómputo, discos SATA y discos SSD
https://www.rubrik.com/wp-content/uploads/2018/11/Rubrik-r6000-Specs-Sheet.pdf

Observaciones

CCN-STIC-1606 Procedimiento de Empleo Seguro Rubrik

Familia Software Edge	
Versión	V. 4.1.2
Familia	Copias de seguridad
Fabricante	Rubrik
Categoría	ENS ALTO
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2021

Descripción

Modelo de despliegue del software basado en máquina virtual. Las funcionalidades aportadas son las mismas que en el despliegue basado en appliances de Rubrik. Esta solución está pensada para entornos de oficinas remotas. Siempre tendrá como respaldo pararéplica un sistema Rubrik basado en appliance o Cloud Cluster y puede archivar directamente a nube pública https://www.rubrik.com/solutions/remote-branch-office/

Observaciones

CCN-STIC-1606 Procedimiento de Empleo Seguro Rubrik

Rubrik Cloud Data Management	
Versión	V. 4.1.2
Familia	Copias de seguridad
Fabricante	Rubrik
Categoría	ENS ALTO
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2021

Descripción

Modelo de despliegue del software basado en hardware de terceros. Las funcionalidades aportadas son las mismas que en el despliegue con appliances de Rubrik. El hardware certificado para el despliegue de Rubrik CDM se puede consultar a través del equipo comercial de Rubrik España o en la siguiente web: https://www.rubrik.com/product/rubrik-industry-platforms/

Observaciones

CCN-STIC-1606 Procedimiento de Empleo Seguro Rubrik

7.6.6 FAMILIA: PLATAFORMAS CONFIABLES

Pendiente de publicación los Requisitos Fundamentales de Seguridad (RFS) de esta familia.

7.6.7 FAMILIA: VIRTUALIZACIÓN

Pendiente de publicación los Requisitos Fundamentales de Seguridad (RFS) de esta familia.

7.6.8 FAMILIA: BALANCEADORES DE CARGA

Pendiente de publicación los Requisitos Fundamentales de Seguridad (RFS) de esta familia.

PRODUCTOS APROBADOS

8 PRODUCTOS APROBADOS

8.1 CATEGORÍA: SEGURIDAD EN LA EXPLOTACIÓN

8.1.1 FAMILIA: DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS

EP543N

Versión	V.1.2
Familia	Dispositivos para gestión de claves criptográficas
Fabricante	Epicom
Clasificación	RESERVADO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2021

Descripción

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

Observaciones

EP543X

Versión	SW v 4.15
Familia	Dispositivos para gestión de claves criptográficas
Fabricante	Epicom
Clasificación	SECRETO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2021

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

8.2 CATEGORÍA: PROTECCIÓN DE LAS COMUNICACIONES

8.2.1 FAMILIA: ENRUTADORES

Aruba 8320 Switch Series

Versión	Aruba OS-CX version 10.03
Familia	Enrutadores
Fabricante	Aruba
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. 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.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Aruba 8325 Switch Series

Versión	Aruba OS-CX version 10.03
Familia	Enrutadores
Fabricante	Aruba
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. 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.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Aruba 8400 Switch Series	
Versión	Aruba OS-CX version 10.03
Familia	Enrutadores
Fabricante	Aruba
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. 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.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

8.2.2 FAMILIA: SWITCHES

Aruba 2930F y 2930M Switch Series	
Versión	Aruba OS version 16.04
Familia	Switches
Fabricante	Aruba
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

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

Aruba 3810M Switch Series

Versión Aruba OS version 16.04

Familia Switches

Fabricante Aruba

Clasificación TODOS LOS NIVELES

Fecha Inclusión 01/03/2019

Revisión de Validez 31/08/2021

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

Aruba 5400R Switch Series

Versión Aruba OS version 16.04

Familia Switches

Fabricante Aruba

Clasificación TODOS LOS NIVELES

Fecha Inclusión 01/03/2019

Revisión de Validez 31/08/2021

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

Aruba 8320 Switch Series

Versión	Aruba OS-CX version 10.03
Familia	Switches
Fabricante	Aruba
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. 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.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Aruba 8325 Switch Series

Versión	Aruba OS-CX version 10.03
Familia	Switches
Fabricante	Aruba
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. 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.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Aruba 8400 Switch Series

Versión	Aruba OS-CX version 10.03
Familia	Switches
Fabricante	Aruba
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

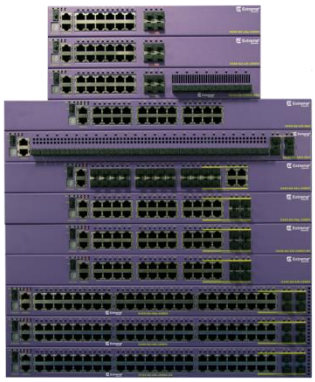
Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. 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.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

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 v22.3.1.4-patch1CC-2
Familia	Switches
Fabricante	Extreme Networks
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	31/08/2021

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 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

Versión EXOS v22.3.1.4-patch1CC-2

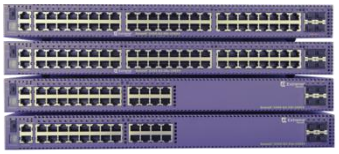
Familia Switches

Fabricante Extreme Networks

Clasificación TODOS LOS NIVELES

Fecha Inclusión 01/06/2019

Revisión de Validez 31/08/2021



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 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 v22.3.1.4-patch1CC-2

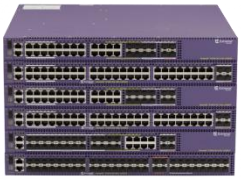
Familia Switches

Fabricante Extreme Networks

Clasificación TODOS LOS NIVELES

Fecha Inclusión 01/06/2019

Revisión de Validez 31/08/2021



Descripción

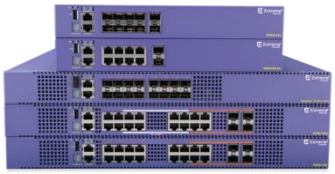
Conmutador apilable de alta rendimiento, posicionado como equipo de acceso de altas prestaciones y backbone de redes medias. Proporciona conmutación avanzada de Nivel 2 y de Nivel 3, con soporte de protocolos de alta complejidad (BGP, MPLS, etc). con interfaces 10/100/1000 Mbps, así como 10Gb y 40 Gb. 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

Summit X620 Series:
X620–16x, X620–16t, X620–10x, X620–8t-2x

Versión	EXOS v22.3.1.4-patch1CC-2
Familia	Switches
Fabricante	Extreme Networks
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	31/08/2021



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 x670-G2 Series:
X670-G2-72x, X670-G2-48x-4q, X670-G2-48x-4q-FB-AC-TAA

Versión	EXOS v22.3.1.4-patch1CC-2
Familia	Switches
Fabricante	Extreme Networks
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	31/08/2021

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 X690 Series:
(X690-48x-2q-4c, X690-48t-2q-4c)

Versión	EXOS v22.3.1.4-patch1CC-2
Familia	Switches
Fabricante	Extreme Networks
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	31/08/2021

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 X870 Series:
(X870-32c, X870-96x-8c)

Versión	EXOS v22.3.1.4-patch1CC-2
Familia	Switches
Fabricante	Extreme Networks
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	31/08/2021

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 hacenideal 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

8.2.3 FAMILIA: PASARELAS DE INTERCAMBIO DE DATOS

PSTfile	
Versión	v4.4.2
Familia	Pasarelas seguras de intercambio de datos
Fabricante	Autek Ingeniería
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

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
Familia	Pasarelas seguras de intercambio de datos
Fabricante	Autek Ingeniería
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2020

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

8.2.4 FAMILIA: DIODOS DE DATOS

PSTdiode	
Versión	v1.0.0
Familia	Diodos de datos
Fabricante	Autek Ingeniería
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2019
Revisión de Validez	28/02/2022

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 esla 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

8.2.5 FAMILIA: HERRAMIENTAS PARA COMUNICACIONES MÓVILES SEGURAS

COMSec Admin +	
Versión	v3.1
Familia	Herramientas para comunicaciones móviles seguras
Fabricante	Indra
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	21/09/2018
Revisión de Validez	21/09/2020

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 yel país donde se encuentre.

Observaciones

Utilización según el PE-2018-24 Procedimiento de empleo COMSec Admin + v1
Para su empleo en entornos tácticos o desplegables, este producto deberá emplearse sobre un dispositivo móvil perteneciente a la familia “plataformas y dispositivos tácticos confia

8.2.6 FAMILIA: CIFRADORES IP

EP430GN	
Versión	1.08.29
Familia	Cifradores IP
Fabricante	Epicom
Clasificación	RESERVADO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2022

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.

EP430GX	
Versión	v.1.07
Familia	Cifradores IP
Fabricante	Epicom
Clasificación	SECRETO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2021

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.

EP430TX	
Versión	1.04
Familia	Cifradores IP
Fabricante	Epicom
Clasificación	SECRETO
Fecha Inclusión	01/12/2017
Revisión de Validez	30/06/2020

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.

8.3 CATEGORÍA: PROTECCIÓN DE LA INFORMACIÓN Y SOPORTES DE INFORMACIÓN

8.3.1 FAMILIA. CIFRADO OFFLINE

EP851

Versión	2.02 y 2.03
Familia	Cifrado offline
Fabricante	Epicom
Clasificación	CONFIDENCIAL
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2020

Descripción

Dispositivo portatil USB de cifrado "off-line":
• Compatible con Crypto Token USB de la empresa Datatech.
• Cifrado de ficheros para su posterior envío.
• Almacenamiento interno de la datos cifrados para su transporte.

Observaciones

Utilización según el PE-2008-01 Procedimiento de Empleo TOKEN USB.

8.3.2 FAMILIA. HERRAMIENTAS PARA FIRMA ELECTRÓNICA

Keyone

Versión	v 4.0
Familia	Herramientas para firma electrónica
Fabricante	Safelayer
Clasificación	Conf. DL Int. Res.
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.

8.4 CATEGORÍA: PROTECCIÓN DE EQUIPOS Y SERVICIOS

8.4.1 FAMILIA. DISPOSITIVOS MÓVILES

Färist Mobile System

Versión	V4, Dispositivo: BQ Aquaris X
Familia	Dispositivos móviles
Fabricante	Tutus
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/12/2018
Revisión de Validez	31/12/2020

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 (BQ Aquaris X) para almacenar información clasificada hasta el grado de Difusión Limitada.

Observaciones

Utilización según PE-2018-19 Operational Doctrine Farist Mobile v4. v1 DL Rel to EU.
Comercializado en España por la empresa Epicom.

8.4.2 FAMILIA: SISTEMAS OPERATIVOS

Windows 10

Versión	Enterprise LTSC 2019
Familia	Sistemas Operativos
Fabricante	Microsoft Corporation
Clasificación	ENS ALTO
Fecha Inclusión	01/10/2019
Revisión de Validez	09/01/2029

Descripción

Sistema Operativo para estaciones de trabajo, tanto en entornos reales como virtualizados.

Observaciones

Procediminento de empleo: CCN-STIC-599A19 y CCN-STIC-599B19

Windows 10	
Versión	Enterprise 2015 LTSB
Familia	Sistemas Operativos
Fabricante	Microsoft Corporation
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2018
Revisión de Validez	14/10/2025

Descripción

Sistema Operativo para estaciones de trabajo, tanto en entornos reales como virtualizados.

Observaciones

CCN-STIC-599A Anexo B
CCN-STIC-599B Anexo B

Windows 10	
Versión	Enterprise 2016 LTSB
Familia	Sistemas Operativos
Fabricante	Microsoft Corporation
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2018
Revisión de Validez	13/10/2026

Descripción

Sistema Operativo para estaciones de trabajo, tanto en entornos reales como virtualizados.

Observaciones

CCN-STIC-599A18 Anexo B
CCN-STIC-599B18 Anexo B

Windows Server 2012 R2	
Versión	Standard Edition, Datacenter Edition
Familia	Sistemas Operativos
Fabricante	Microsoft Corporation
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2018
Revisión de Validez	31/05/2021

Descripción

Sistema Operativo para servidores

Observaciones

CCN-STIC-870A y CCN-STIC-870B

Windows Server 2016	
Versión	Standard Edition, Datacenter Edition
Familia	Sistemas Operativos
Fabricante	Microsoft Corporation
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2018
Revisión de Validez	31/05/2021

Descripción

Sistema Operativo para servidores

Observaciones

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

8.4.3 FAMILIA: COPIAS DE SEGURIDAD

Familia hardware R6000	
Versión	V. 4.1.2
Familia	Copias de seguridad
Fabricante	Rubrik
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2021

Descripción

Rubrik es una plataforma convergente de gestión del dato en Cloud, Pública o Privada, que ofrece disponibilidad instantánea de la información para recuperación ante desastre, ataque Ransomware o pruebas de desarrollo. Solución definida por software que permite una operación sencilla, construida con arquitectura scale-out, basada en sistemas distribuidos, que reparten de forma inteligente y autónoma los datos, metadatos y tareas entre todos los nodos y miembros del clúster, permitiendo realizar búsquedas globales, indexadas y predictivas "google-like". Diseño API RESTful nativo 100%, que ofrece máxima integración, automatización y orquestación con la Cloud, para archivado a largo plazo, instanciación de máquinas virtuales o explotación de los metadatos. Permite el cumplimiento GDPR en el tratamiento de la información, certificado por metodología Common Criteria EAL2+. Cada appliance tiene tres o cuatro nodos, cada uno tiene su propio cómputo, discos SATA y discos SSD y se pueden combinar cualquiera de loscuatro modelos de appliance en un mismo cluster
https://www.rubrik.com/wp-content/uploads/2018/04/Spec-Sheet-Rubrik-Appliance-Specs-r6000.pdf

Observaciones

CCN-STIC-1606 Procedimiento de Empleo Seguro Rubrik

Familia hardware R6000f	
Versión	V. 4.1.2
Familia	Copias de seguridad
Fabricante	Rubrik
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2021

Descripción

Appliance certificado FIPS 140-2 Level 2. Cada appliance tiene cuatro nodos y cada uno tiene su propio cómputo, discos SATA y discos SSD
https://www.rubrik.com/wp-content/uploads/2018/11/Rubrik-r6000-Specs-Sheet.pdf

Observaciones

CCN-STIC-1606 Procedimiento de Empleo Seguro Rubrik

Familia Software Edge	
Versión	V. 4.1.2
Familia	Copias de seguridad
Fabricante	Rubrik
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2021

Descripción

Modelo de despliegue del software basado en máquina virtual. Las funcionalidades aportadas son las mismas que en el despliegue basado en appliances de Rubrik. Esta solución está pensada para entornos de oficinas remotas. Siempre tendrá como respaldo pararéplica un sistema Rubrik basado en appliance o Cloud Cluster y puede archivar directamente a nube pública https://www.rubrik.com/solutions/remote-branch-office/

Observaciones

CCN-STIC-1606 Procedimiento de Empleo Seguro Rubrik

Rubrik Cloud Data Management	
Versión	V. 4.1.2
Familia	Copias de seguridad
Fabricante	Rubrik
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2021

Descripción

Modelo de despliegue del software basado en hardware de terceros. Las funcionalidades aportadas son las mismas que en el despliegue con appliances de Rubrik. El hardware certificado para el despliegue de Rubrik CDM se puede consultar a través del equipo comercial de Rubrik España o en la siguiente web: https://www.rubrik.com/product/rubrik-industry-platforms/

Observaciones

CCN-STIC-1606 Procedimiento de Empleo Seguro Rubrik

8.5 CATEGORÍA: COMUNICACIONES TÁCTICAS SEGURAS

8.5.1 FAMILIA. PLATAFORMAS Y DISPOSITIVOS TÁCTICOS CONFIABLES

BITTIUM TOUGH MOBILE C	
Versión	HW version: 9304809A03 SW version: Android 5.1.1 Kernel version: 3.4.0 Build: S2_BSOS_1.1.5C_MR22_sapphire2
Familia	Plataformas y dispositivos tácticos confiables
Fabricante	BITIUM
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/06/2019
Revisión de Validez	30/11/2020

Descripción

Teléfono móvil rugerizado (IP67, MIL-STD- 810G) basado en S.O. Android diseñado para dar soporte a usuarios civiles y militares. Cubre 9 bandas LTE, incluida la Banda 14 para seguridad pública. Dual-sim para redes LTE privadas y públicas. Este dispositivose considera una plataforma confiable donde ejecutar aplicaciones software de forma protegida.

Observaciones

procedimiento de configuración y empleo seguro pendiente de publicación.
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
Familia	Plataformas y dispositivos tácticos confiables
Fabricante	GETAC
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/06/2019
Revisión de Validez	30/11/2020

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".

8.5.2 FAMILIA. SOLUCIONES PARA PROTECCIÓN DE LAS COMUNICACIONES TÁCTICAS

COMSec Admin +	
Versión	v3.1
Familia	Soluciones para protección de las comunicaciones tácticas
Fabricante	Indra
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	21/09/2018
Revisión de Validez	21/09/2020

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 yel país donde se encuentre.

Observaciones

Utilización según el PE-2018-24 Procedimiento de empleo COMSec Admin + v1
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".

8.6 CATEGORÍA: TEMPEST

8.6.1 FAMILIA. ARMARIOS APANTALLADOS

P.AT-02D

Versión

Familia Armarios apantallados

Fabricante CONSUEGRA S. COOP.

Clasificación Apto ZONA 0

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2020

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 deZONA 0 con equipos clasificados ZONA 2.

Observaciones

P.AT-06D

Versión

Familia Armarios apantallados

Fabricante CONSUEGRA S. COOP.

Clasificación Apto ZONA 0

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2020

Descripción

Armario apantallado ciego de 25U. Dimensiones 1524x625x1000 mm. Ventilación a través de 2 ventiladores con termostatos independientes con caudal de hasta 2.700 m3/h. Distribuidor interno con diferencial y automático. Apto para instalación en locales con clasificación de ZONA 0.

Observaciones

P.AT-06E

Versión

Familia Armarios apantallados

Fabricante CONSUEGRA S. COOP.

Clasificación Apto ZONA 0

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2020

Descripción

Armario apantallado ciego de 38U. Dimensiones 2102x625x1000 mm. Ventilación a través de 2 ventiladores con termostatos independientes con caudal de hasta 2.700 m3/h. Distribuidor interno con diferencial y automático. Apto para instalación en locales con clasificación de ZONA 0.

Observaciones

P.AT-07

Versión

Familia Armarios apantallados

Fabricante CONSUEGRA S. COOP.

Clasificación Apto ZONA 0

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2020

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

P.AT07D

Versión

Familia Armarios apantallados

Fabricante CONSUEGRA S. COOP.

Clasificación Apto ZONA 0

Fecha Inclusión 01/04/2019

Revisión de Validez 30/09/2021

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

SHATEM - SHELTER ARPA TEMPEST MULTIPROPOSITO

Versión

Familia Armarios apantallados

Fabricante ARPA, EQUIPOS MÓVILES DE CAMPAÑA S.A.U.

Clasificación Apto ZONA 0

Fecha Inclusión 01/01/2020

Revisión de Validez 31/05/2022

Descripción

Contenedor shelter para alojamiento y/o operación de equipos informáticos, electrónicos, optrónicos de telecomunicaciones y asimilables para entornos CIS. Equipado con los elementos de filtrado y protección EMI necesarios en acometidas de potencia, datos y servicios para disponer de apantallamiento intergral TEMPEST frente a emanaciones comprometedoras radiadas y conducidas.

Observaciones

8.6.2 FAMILIA. MONITORES

P.MONT0-04

Versión

Familia Monitores

Fabricante CONSUEGRA S. COOP.

Clasificación SDIP-27 Level A

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2020

Descripción

Monitor LCD de 19" con formato panorámico.

Observaciones

8.6.3 FAMILIA. PERIFÉRICOS

P.CTTDB9-02

Versión

Familia Periféricos

Fabricante CONSUEGRA S. COOP.

Clasificación SDIP-27 Level A

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2020

Descripción

Teclado QWERTY español. Conexión USB.

Observaciones

P.KVMT0-01

Versión

Familia Periféricos

Fabricante CONSUEGRA S. COOP.

Clasificación SDIP-27 Level A

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2020

Descripción

Conmutador KVM para dos sistemas. Basado en BELKIN SECURE OMNIVIEW F1DN102Uea con certificación NIAP EAL 4+.

Observaciones

P.TECT0-07

Versión

Familia Periféricos

Fabricante CONSUEGRA S. COOP.

Clasificación SDIP-27 Level A

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2020

Descripción

Teclado QWERTY español. Conexión USB.

Observaciones

P-RATT0-04

Versión

Familia Periféricos

Fabricante CONSUEGRA S. COOP.

Clasificación SDIP-27 Level A

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2020

Descripción

Ratón óptico USB

Observaciones

8.6.4 FAMILIA. CPU

P.COMT0-01

Versión

Familia CPU

Fabricante CONSUEGRA S. COOP.

Clasificación SDIP-27 LEVEL A

Fecha Inclusión 01/06/2018

Revisión de Validez 30/11/2020

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

8.6.5 FAMILIA. IMPRESORAS

P.IMPT0-03

Versión

Familia Impresoras

Fabricante CONSUEGRA S. COOP.

Clasificación SDIP-27 Level A

Fecha Inclusión 01/07/2018

Revisión de Validez 31/12/2020

Descripción

Impresora tempestizada del modelo comercial HP Laserjet Pro 400 M451dn. Aprobado para su uso en locales con clasificación ZONING de ZONA 0.

Observaciones

9 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] PO-09 Procedimiento de cualificación de productos STIC en el ENECSTI.

[6] CCN-STIC-105 Catálogo de Productos de Seguridad TIC (CPSTIC).

[7] CCN-STIC-151 Evaluación y Clasificación TEMPEST de equipos.

10 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*
RFS	*Requisitos Fundamentales de Seguridad*
STIC	*Seguridad de las Tecnologías de la Información y la Comunicación*
TIC	*Tecnologías de la Información y la Comunicación*