ANC-STIC-100

Registre de Productes Certificats i Serveis de Seguretat de les T.I.C

(DOCUMENT SUBJECTE A MODIFICACIONS)

Fitxa del document

Títol	Registre de Productes i Serveis de Seguretat de les T.I.C

Versió	Redactat per	Aprovat per	Data aprovació	Data publicació
Versió Inicial	ANC-AD	ANC-AD	01/07/2024	

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi
1.0	375		

Propietari del document: ANC-AD

PRÒLEG

L'ús massiu de les tecnologies de la informació i les telecomunicacions (TIC), en tots els àmbits de la societat, ha creat un nou espai, el ciberespai, on es produiran conflictes i agressions, on hi ha ciberamenaces que atemptaran contra la seguretat nacional, l'estat de dret, la prosperitat econòmica, l'estat de benestar i el normal funcionament de la societat i de les administracions públiques i entitats privades.

El Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i la Comunicació (CPSTIC) és una eina d'alta importància elaborada pel Centre Criptològic Nacional (CCN) d'Espanya d'acord amb la directiva CCN-STIC 105. Aquest document proporciona una guia exhaustiva de productes i serveis en l'àmbit de les tecnologies de la informació i la comunicació amb un enfocament en la seguretat. Cal esmentar que l'ANC-AD té l'autorització expressa del CCN per utilitzar aquest catàleg i adaptar-lo a les seves necessitats específiques. Això proporciona a l'ANC-AD la capacitat flexible de realitzar les modificacions pertinents i replicar el contingut del document. Aquesta autorització ens permet orientar el catàleg d'acord amb les particularitats i necessitats del nostre entorn, assegurant que les directrius i recomanacions de seguretat estan adequadament alineades amb la nostra infraestructura i objectius. Per tant, l'ús i l'adaptació constant d'aquest catàleg reforcen la nostra posició a l'avantguarda en matèria de seguretat de les tecnologies de la informació i la comunicació.

Aquest document s'elabora seguint directrius de l'Agència Nacional de Ciberseguretat d'Andorra, el CSIRT-AD i el Comitè Especialitzat de Ciberseguretat. Per això, es reconeix la importància d'establir un marc de referència que recolzi a les entitats responsables de la seguretat dels sistemes de TIC sota la seva jurisdicció.

Marc Rossell i Soler
Secretari d´Estat de Transformació digital i Telecomunicacions

INDEX

1. INTRODUCCIÓ

1. L'adquisició d'un producte o la contractació d'un servei de seguretat TIC que ha de manejar informació nacional classificada o informació sensible ha d'estar precedida d'un procés de comprovació que els mecanismes de seguretat implementats en el producte o servei són adequats per protegir aquesta informació.
2. L'avaluació i certificació d'un producte o servei de seguretat TIC és l'únic mitjà objectiu que permet valorar i acreditar la seva capacitat per manejar informació de forma segura. Al Principat d'Andorra, aquesta responsabilitat està assignada a la Agència Nacional de Ciberseguretat d'Andorra (d'ara endavant, ANC-AD), sent l'autoritat de certificació de la seguretat de les tecnologies de la informació i la comunicació i autoritat de certificació criptològica.
3. El Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i la Comunicació (d'ara endavant, CPSTIC) es un document elaborat pel CCN d'Espanya (CCN-STIC 105), el qual l'ANC-AD té l'autorització per a utilitzar, modificar i replicar el document, com s'ha mencionat.
4. D'acord a aquestes competències, l'ANC-AD publica el **Registre de Productes i Serveis de Seguretat de les Tecnologies de la Informació i la Comunicació (d'ara endavant, RPSTIC)**. Aquest registre té com a finalitat oferir als organismes de l'Administració un conjunt de productes o serveis STIC de referència les funcionalitats de seguretat dels quals relacionades amb l'objecte de la seva adquisició han estat certificades.
5. D'aquesta manera, el RPSTIC permet proporcionar un nivell mínim de confiança a l'usuari final en els productes o serveis adquirits, en base a les millores de seguretat derivades del procés d'avaluació i certificació i a un procediment d'ocupació segur.
6. El RPSTIC consta de dos parts: **Productes Aprovats i Productes i Serveis Qualificats**. En l'apartat de **Productes Aprovats** es recullen aquells productes que es consideren adequats per al maneig d'informació classificada, mentre que en l'apartat de **Productes i Serveis Qualificats** s'inclouen aquells que compleixen els requisits de seguretat exigits per al maneig d'informació sensible en, en qualsevol de les seves categories (ALTA, MEDIA i BÀSICA).

TIPUS DE PRODUCTE O SERVEI	INFORMACIÓ QUE MANEJA
APROVAT	CLASSIFICAT
QUALIFICAT	SENSIBLE

Taula 1. Tipus de productes o serveis inclosos en el RPSTIC

2. OBJECTE DE LA PRESENT GUIA

7. L'objecte d'aquest document és el de presentar el Registre de Productes de Seguretat de les Tecnologies de la Informació i Comunicació que recull un llistat de productes aprovats per al maneig d'informació classificada i de productes i serveis qualificats per al maneig d'informació sensible, de manera que pugui servir de referència a l'Administració Pública.

3. ABAST

8. En l'apartat de Productes Qualificats d'aquest document s'inclouen tots aquells que han superat amb èxit el procés d'inclusió i que per tant es consideren qualificats per a ser utilitzats en sistemes crítics.
9. Aquest fet implica que tots ells posseeixen una certificació funcional Common Criteria en la qual s'inclouen els Requisits Fonamentals de Seguretat[1] (d'ara endavant, RFS) per a determinar la família en la qual es consideren o que, en absència de productes que posseeixin la certificació requerida.
10. En el cas de productes multipropòsit, aquests poden aparèixer en una o diverses famílies, sempre que s'hagi certificat que compleixen amb els RFS corresponents a cadascuna d'elles. En aquests casos, que un producte es consideri qualificat per a una determinada família de productes no implica que ho estigui per a la resta de les famílies en les quals pugui enquadrar-se, al marge que implementi la funcionalitat associada.
11. En l'apartat de Productes Aprovats s'inclouen tots aquells que han superat amb èxit el procés d'inclusió en el RPSTIC[2] i que per tant es consideren aprovats per manejar informació classificada. El nivell màxim de classificació de la informació per a la qual s'aprova el seu ús vindrà especificat en cada producte de manera individual.

4. INCLUSIÓ D'UN PRODUCTE DEL RPSTIC

12. Per a la inclusió d'un producte o servei en el catàleg, es tindrà en compte els següents criteris:
    a. En el cas de **Productes Aprovats** per al maneig d'informació classificada, el màxim nivell de classificació de la informació que pot manejar (DIFUSIÓ LIMITADA, CONFIDENCIAL, RESERVAT, SECRET).
    b. En el cas de **Productes i Serveis Qualificats**, la màxima categoria del sistema d'informació en el qual es pot emprar (ALTA, MITJANA, BÀSICA).

[1] Descripció de conformitat amb la guia CCN-STIC 140 (CCNCERT) Taxonomies de referència per a productes de seguretat TIC.

[2] Descrit en la guia CCN-STIC 140 (CCNCERT)Taxonomies de referència per a productes de seguretat TIC.

c. Les funcionalitats de seguretat que implementa el producte o servei i les certificacions aportades.

d. Altres aspectes com l'anàlisi de riscos del producte o servei, la necessitat operativa dins de l'Administració i totes les entitats que estan en l'abast de la Llei 22/2022, del 9 de juny, de mesures per la seguretat de les xarxes i dels sistemes d'informació, la disponibilitat o no d'altres productes o serveis certificats que satisfacin la mateixa funcionalitat, etc.

En funció d'aquesta informació, es determinaran les proves o avaluacions que haurà de superar el producte o servei de seguretat TIC corresponent.

5. REVISIÓ DE VALIDESA DE PRODUCTES STIC

13. Periòdicament, es realitzarà una revisió de validesa dels productes i serveis inclosos en el registre per tal de garantir que encara compleixen amb els requisits exigits per formar-ne part. La data de revisió de validesa s'indica en la fitxa corresponent a cada producte.

14. Per aquesta raó, després d'una revisió de validesa, un producte o servei inclòs en el registre pot baixar el màxim nivell de classificació que està autoritzat a processar en el cas dels productes aprovats i fins i tot pot ser exclòs quan es deixin de complir els requisits exigits per a la seva inclusió.

6. EXCLUSIÓ D'UN PRODUCTE O SERVEI DEL CPSTIC

15. Un producte o servei podrà ser exclòs del RPSTIC per qualsevol dels motius següents:

a. Caducitat del certificat de Producte o Servei Qualificat STIC. Tots els certificats seran emesos amb una data de revisió de validesa (que dependrà de la família considerada), a partir de la qual el sol·licitant haurà de remetre una nova sol·licitud d'inclusió seguint el procediment descrit anteriorment. En el cas que aquesta sol·licitud no es dugui a terme, es podrà excloure el producte o servei del RPSTIC.

b. Revocació o caducitat d'alguna de les certificacions requerides al producte o servei per accedir al catàleg: *Common Criteria*, LINCE, segons el cas.

c. Pèrdua de les condicions d'excepcionalitat. En el cas que el producte o servei hagi estat inclòs en el registre per algun dels supòsits d'excepcionalitat, podrà ser exclòs un cop deixi de complir-se algun d'ells: aparició de productes o serveis substitutius amb la certificació adequada, pèrdua de la consideració de producte o servei estratègic , etc.

d. Que no compleixi amb els RFS vigents en el moment de la revisió de validesa. Els avenços tecnològics poden deixar obsoleta la tecnologia

emprada en uns casos i en altres fer que es redueixi de forma considerable la seguretat d'aquest, la qual cosa implicarà una evolució dels RFS.

e. Que presenti vulnerabilitats crítiques no corregides. En aquest cas, es podrà demanar al fabricant un informe d'impacte d'aquestes vulnerabilitats. Si aquest informe determinés que la vulnerabilitat és explotable seguint el PES, aquest serà exclòs del registre.

7. PRODUCTES QUALIFICATS

7.1. EINES PER AL DESENVOLUPAMENT DE PRODUCTES DE SEGURETAT

Mòdul criptogràfic per a aplicacions mòbils Telcryp

Versió	1.11
Fabricant	Cryptographic ans Security System (CS2)
Família	-
Tipus	Producte
Data Inclusió	01/10/2023
Revisió de Validesa	31/10/2025

Descripció

Aquest mòdul proveeix els serveis de xifratge i seguretat per garantir la comunicació tant amb el servidor IMS com amb els terminals remots amb un xifratge extrem a extrem.

Aquest mòdul criptogràfic està dissenyat com una llibreria criptogràfica i incorporat a aplicacions de comunicacions en entorn de mobilitat degudament aprovades, i instal·lades en plataformes confiables.

Observacions

Procediment d'ocupació pendent de publicació

Biblioteca Criptogràfica BOTAN-CCN

Versió	2.19.3
Fabricant	Centre Criptològic Nacional
Família	-
Tipus	Producte
Data Inclusió	01/10/2020
Revisió de Validesa	31/12/2024

Descripció

La biblioteca criptogràfica BOTAN-CCN implementa els mecanismes criptogràfics acceptats pel CCN per al seu ús en el desenvolupament de productes de seguretat. Inclou codi font i binaris compatibles amb sistemes Windows i Linux. Inclou generadors de soroll i test de tots els mecanismes implementats

Observacions

No aplica

TRNG-P200 Physical True Random Number Generator	
Versió	1.11
Fabricant:	BERTEN DSP
Família	-
Tipus	Producte
Data Inclusió	01/10/2020
Revisió de Validesa	31/12/2024

Descripció

L'IP Core TRNG-P200 és un Generador de Números Aleatoris Veritables (TRNG, True Random Number Generator) implementable en qualsevol disseny criptogràfic basat en FPGA, SoC o ASIC. Utilitza una font física d'entropia no determinista basada en oscil·ladors multifase, que genera números aleatoris d'alta qualitat estadística en una àrea mínima. Genera simultàniament la seqüència aleatòria de la font d'entropia, i dues sortides postprocessades amb un filtre de paritat i un codificador polinòmic configurable. És portable a qualsevol dispositiu Xilinx, Intel o Microsemi i compleix amb els requisits definits en les bateries de test Diehard, NIST 800-22 i AIS-31 PTG.2. A més, implementa un conjunt de proves d'integritat (health tests), d'acord amb NIST 800-90B, FIPS 140-2 i AIS-31. La generació de seqüències és monitorada contínuament, activant alarmes en cas de fallades. El TRNG-P200 inclou interfícies AMBA-AXI i un mapa de registres amb paràmetres programables per configurar la velocitat de sortida, el codificador polinòmic, les proves d'integritat, i la gestió de les alarmes. El producte inclou funcions ANSI C per a la configuració d'aquests registres en el sistema criptogràfic. https:// www.bertendsp.com/products/trng-p200/

Observacions

No aplica

7.2. CONTROL D'ACCÉS

7.2.1. CONTROL D'ACCÉS A XARXA (NAC)

Aruba ClearPass Policy Manager	
Versió	6.11
Fabricant	HPE Aruba Networking
Família	Control d'accés a xarxa (NAC)
Tipus	Producte
Data Inclusió	06/05/2024
Revisió de Validesa	31/10/202
Descripció	
Pendent de descripció	
Observacions	
Procediment d'Ocupació Segura pendent de publicació	

Cisco Identity Services Engine (ISE) 3500 series (SNS-3595), 3600 series (SNS-3615, SNS-3655, SNS-3695), ISE-VM	
Versió	**V 3.1**
Fabricant	Cisco System
Família	Control d'accés a xarxa (NAC)
Tipus	Producte
Data Inclusió	01/03/2024
Revisió de Validesa	30/06/2024
Descripció	
Cisco® Identity Services Engine (ISE) és la solució integral per a optimitzar l'administració de les polítiques de seguretat. Amb ISE, pot veure els usuaris i els dispositius i controlar l'accés a la xarxa corporativa a través de connexions cablejades, sense fils, VPN i 5G. Cisco Identity Services Engine potencia la resiliència de la seguretat amb la flexibilitat i les opcions necessàries per a allotjar el programari de Cisco com a càrregues de treball en diversos núvols més enllà del suport local i mantenir la continuïtat empresarial enmig de la incertesa. Això permet als clients obtenir un enfocament més modernitzat per a implementar els serveis de NAC des del núvol. En passar d'administrar la infraestructura en una caixa a aprofitar la infraestructura com a codi (IaC) en lesimplementacions híbrides. Els equips guanyen agilitat amb l'aprovisionament Zero Trust i la flexibilitat a l'hora d'automatitzar el seu entorn durant tot el cicle de vida de l'administració de Cisco ISE. ISE és l'element central per a un accés de confiança zero al lloc de treball (infraestructura autogestionada)amb l'objectiu de reduir el risc, protegir la integritat i accelerar l'accés segur a la xarxa a través de la xarxa distribuïda	
Observacions	
Procediment d'Ocupació Segura pendent de publicació	

Forescout 8.3 (CT-R, CT-100, CT-1000, CT-2000, CT-4000, CT-10000, CEM-5, CEM-10, CEM-25, CEM 50, CEM-100, CEM-150, CEM-200, 4130, 5110, 5120, 5140, 5160)

Versió	8.4
Fabricant	Forescout
Família	Control d'accés a xarxa (NAC)
Tipus	Producte
Data Inclusió	01/05/2023
Revisió de Validesa	01/04/2025

Descripció

La plataforma Forescout és una plataforma unificada de seguretat que permet a les empreses i organismes oficials obtenir informació completa sobre l'estat dels seus entorns empresarials ampliats i orquestrar mesures destinades a reduir el risc operatiu i de ciberseguretat. Es desplega de forma ràpida i segura en entorns de campus, centres de dades, el núvol i xarxes d'OT. Ofereix descobriment, classificació en temps real i avaluació contínua d'estat, sense necessitat d'agents. Per a més informació, vegeu: https://forescouttechnologies.es

Observacions

CCN-STIC-1106 Procediment d'ocupació assegurança Forescout

EMMA / OpenNac Enterprise

Versió	1.2
Fabricant	OpenCloud Factory / CCN
Família	Control d'accés a xarxa (NAC)
Tipus	Producte
Data Inclusió	01/05/2020
Revisió de Validesa	31/01/2024

Descripció

EMMA és una solució de Visualització d'actius en una xarxa, la seva autenti aixi com l'automatització d'auditories de seguretat de la infraestructura. L'abast de la qualificació abasta els següents mòduls d'EMMA: Visibilitat, Control / Resposta, Segmentació, Compliment, BYOD i Gestió de convidats. Es registra l'inventari i perfilat de l'equip que es podrà utilitzar en les polítiques d'accés a la connexió remota. Addicionalment, permet definir i aplicar polítiques d'accés en funció d'una postura de seguretat basada en el nivell de bastionat, a més d'altres factors (horari de la connexió, característiques de l'equip, role d'usuari, etc.). EMMA s'integrarà amb solucions de l'ecosistema CCN-CERT: ROCIO i ANA. https:// www.ccn-cert.cni.es/pdf/documentos-publicos/4153- datasheet-emma/file.html

Observacions

CCN-STIC-1105 Procediment d'ocupació assegurança EMMA

ClearPass Policy Manager (C100, C200, C3000)	
Versió	6.9
Fabricant	Aruba
Família	Control d'accés a xarxa (NAC)
Tipus	Producte
Data Inclusió	01/07/2019
Revisió de Validesa	31/05/2024

Descripció

La família de productes ClearPass de seguretat per al control d'accés a la xarxa ofereix elaboració de perfils, autenticació i autorització per a usuaris, sistemes i dispositius que intenten accedir als recursos de TI. ClearPass s'ha dissenyat per abordar els reptes de seguretat associats amb una organització TI: Accés segur a la xarxa (802.1X i Radius), funcions de NAC, Implementació de portal de Convidats i intern, suport de funcionalitats BYOD, integració amb Firewalls (PaloAlto, CheckPoint, Forninet i més) tot això mitjançant la integració múltiples fonts d'autenticació (Directoris actius, LDAP, BBDD i provedors externs d'identitat)

Observacions

CCN-STIC-1103 Procediment d'ocupació assegurança ClearPass 6.9

7.2.2. SERVIDORS D'AUTENTICACIÓ

Aruba ClearPass Policy Manager	
Versió	6.11
Fabricant	Aruba
Família	Servidores d'autenticació
Tipus	Producte
Data Inclusió	06/05/2024
Revisió de Validesa	31/10/2024
Descripció	
Pendent de descripció	
Observacions	
Procediment d'Ocupació Segura pendent de publicació	

Location-Based Identity Platform

Versió	N/A
Fabricant	Ironchip Telco, S.L.
Família	Servidors d'Autenticació
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	30/04/2024

Descripció

La solució d'Ironchip Location-Based Identity Platform (LBAuth) representa una avançada plataforma de gestió d'accessos i protecció d'identitats basada en intel·ligència artificial de localització. Aquesta plataforma permet la configuració de polítiques de seguretat innovadores, amb l'objectiu d'evitar la suplantació d'identitats i l'accés no autoritzat als serveis protegits.

La plataforma centralitzada Ironchip LBAuth inclou integracions preconfigurades que l'administrador pot completar seguint passos senzills, protegint d'aquesta manera tots els serveis de tecnologia de la informació de l'empresa.

Els usuaris són integrats dinàmicament a la plataforma, la qual cosa possibilita la gestió de permisos tant individuals com grupals, mitjançant l'aplicació de diversos mètodes d'accés i polítiques de seguretat. Això assegura una protecció sòlida per als serveis més crítics de l'organització.

Les característiques clau d'aquesta solució inclouen:

- Gestió de privilegis basada en rols: Aquesta característica permet establir diferents nivells de privilegis d'usuari, prevenint així l'accés no autoritzat a la resta del sistema.
- Restricció d'accés des de llocs no autoritzats: La plataforma genera accés habilitat únicament des d'àrees autoritzades, portant la seguretat de l'empresa al següent nivell i garantint que només persones autoritzades tinguin accés als recursos protegits.
- Monitoratge d'accessos en temps real: La plataforma documenta l'activitat dels usuaris, permetent als administradors visualitzar l'accés en una línia de temps. A més, ofereix la possibilitat de generar informes detallats que poden ser descarregats per a un control complet del sistema.

Observacions

Procediment d'ocupació assegurança pendent de publicació

ClearPass Policy Manager (C1000, C2000, C3000)

Versió	6.9
Fabricant	Aruba
Família	Servidors d'Autenticació
Tipus	Producte
Data Inclusió	01/07/2019
Revisió de Validesa	31/05/2024

Descripció

La família de productes ClearPass de seguretat per al control d'accés a la xar[illegible]ió de perfils, autenticació i autorització per a usuaris, sistemes i dispositius que intenten accedir als recursos de TI. ClearPass s'ha dissenyat per abordar els reptes de seguretat associats amb una organització TI: Accés segur a la xarxa (802.1X i Radius), funcions de NAC, Implementació de portal de Convidats i intern, suport de funcionalitats BYOD, integració amb Firewalls (PaloAlto, CheckPoint, Forninet i més) tot això mitjançant la integració múltiples fonts d'autenticació (Directoris actius, LDAP, BBDD i provedors externs d'identitat)

Observacions

CCN-STIC-1103 Procediment d'ocupació assegurança ClearPass 6.9

7.2.3. GESTIÓ D'ACCÉS PRIVILEGIAT (PAM)

CyberArk Privileged Account Security Solution	
Versió	10.10
Fabricant	CyberArk
Família	Gestió d'accés privilegiat (PAM)
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	24/06/2024

Descripció

CyberArk Core PAS és una solució de seguretat que permet protegir, controlar i monitorar l'accés privilegiat a infraestructura locals, en el núvol i híbrides. Permet a les organitzacions administrar i protegir les credencials dels comptes privilegiats i els drets d'accés, monitorar i controlar l'activitat dels comptes privilegiats, identificar les activitats sospitoses i respondre a les amenaces.

Permet:

- Assegurar i controlar centralment l'accés a les credencials privilegiades basades en polítiques de seguretat definides administrativament
- Aïllar i assegurar sessions d'usuaris privilegiats. Les capacitats de monitoratge i gravació permeten als equips de seguretat veure sessions privilegiades en temps real, suspendre automàticament i acabar remotament les sessions sospitoses.
- Detectar, alertar i respondre a activitats privilegiades anòmales.
- Controlar l'accés de privilegis mínims per a NIX i Windows. La solució permet als usuaris amb privilegis executar comandos administratius autoritzats des de les seves sessions natives d'Unix o Linux, alhora que s'eliminen els privilegis d'arrel innecessaris.
- Protegir els controladors de domini de Windows.

No s'inclou en la qualificació els connectors basats en Internet Explorer.

Observacions

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

Safeguard for Priviledge Passwords

Versió	7.0
Fabricant	One Identity
Família	Gestió d'accés privilegiat (PAM)
Tipus	Producte
Data Inclusió	01/02/2024
Revisió de Validesa	31/04/2025

Descripció

Safeguard for Privileged Passwords (SPP) és una solució de seguretat de gestió de comptes privilegiats la funció principal de les quals és prevenir el mal ús potencial dels comptes privilegiats en els sistemes IT locals, híbrids o al núvol, així com les aplicacions de les organitzacions, permetent emmagatzemar, gestionar i monitoritzar l'ús d'aquests comptes per part dels usuaris. SPP automatitza, controla i assegura la gestió de credencials privilegiades amb un accés basat en rols i fluxos automatitzats.

- Arquitectura escalable basada en dispositius físics o virtuals en alta disponibilitat escalable en model Actiu-Actiu-Actiu.
- Gestió de l'accés basat en un motor de polítiques, fluxos d'aprovació i revisió, etc.
- Informes d'auditoria de l'activitat registrada en els dispositius.
- Importar, descobrir i trencat automàtic de comptes privilegiats i contrasenyes dels sistemes i aplicacions.
- Gestió de comptes de servei, IIS, tasques programades i COM + en entorns Microsoft.
- Integració amb Safeguard for Sessions per estendre les capacitats del SPP per a la gravació de sessions, anàlisi de comportament i detecció.
- Gestió de secrets en entorns DevOps i RPA.
- Integració amb sistemes externs mitjançant RestAPI

Observacions

CCN-STIC-1110 Procedimiento de Empleo Seguro Safeguard for Privileged Passwords (SPP)

7.2.4. GESTIÓ D'IDENTITATS (IM)

AWS IAM Identity Center	
Versió	
Fabricant	AWS
Família	Gestió d'identitats (IM)
Tipus	Servei
Data Inclusió	01/06/2023
Revisió de Validesa	30/06/2024

Descripció

AWS IAM Identity Center (successor d'AWS Single Sign-On) és un servei al núvol que facilita-la l'administració centralitzada de l'accés a diversos comptes d'AWS i aplicacions empresarials.

Amb AWS IAM Identity Center, pot administrar fàcilment l'accés centralitzat i els permisos d'usuari per a tots els seus comptes d'AWS Organizations. AWS IAM Identity Center també inclou integracions incorporades amb aplicacions d'AWS, i moltes aplicacions empresarials, com Salesforce, Box i Microsoft Office 365. A més, mitjançant l'assistent de configuració d'aplicacions d'AWS IAM Identity Center, pot crear integracions de Security Assertion Markup Language (SAML) 2.0 i ampliar l'accés SSO a qualsevol de les seves aplicacions compatibles amb SAML.

Els seus usuaris només han d'iniciar sessió en un portal d'usuari amb les credencials que configurin en AWS IAM Identity Center o utilitzant les seves credencials corporatives existents per accedir a tots els seus comptes i aplicacions assignades des d'un únic lloc.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació.

AWS Identity Access Management (IAM) + AWS STS

Versió

Fabricant AWS

Família Gestió d'identitats (IM)

Tipus Servei

Data Inclusió 01/08/2022

Revisió de Validesa 30/06/2024

Descripció

AWS Identity and Access Management (IAM) permet controlar de forma segura l'accés als serveis i recursos d'AWS per als seus usuaris, grups i rols d'AWS. Es poden crear i administrar controls d'accés de gra fi amb permisos, especificar qui pot accedir a quins serveis i recursos, i sota quines condicions.

Subministra la capacitat d'administrar els permisos d'AWS per als seus usuaris i càrregues de treball al Centre d'Identitat d'AWS IAM. Permet administrar l'accés dels usuaris en diversos comptes d'AWS, habilitar un servei d'alta disponibilitat, gestionar fàcilment l'accés a diversos comptes i els permisos de tots els seus comptes en les organitzacions d'AWS de forma centralitzada. El Centre d'Identitats de IAM inclou integracions SAML incorporades a moltes aplicacions empresarials, com Salesforce, Box i Microsoft Office 365.

Permet especificar l'accés als recursos d'AWS mitjançant permisos. Les entitats de IAM (usuaris, grups i rols) comencen per defecte sense permisos. A aquestes identitats se'ls poden concedir permisos adjuntant una política de IAM que especifiqui el tipus d'accés, les accions que es poden realitzar i els recursos en els quals es poden realitzar les accions.

Els rols de IAM permeten delegar l'accés a usuaris o serveis que normalment no tenen accés als recursos d'AWS de la seva organització. Els usuaris de IAM o els serveis d'AWS poden assumir un rol per obtenir una credencial de seguretat temporal que s'utilitzarà per fer trucades a l'API d'AWS. AWS Security Token Service (STS) s'integra al costat d'AWS IAM per proporcionar un servei web que permet sol·licitar credencials temporals (tokens) amb privilegis limitats als usuaris. Aquests tokens són els encarregats de proporcionar a les identitats d'AWS IAM els diferents permisos d'accés als recursos d'AWS.

Per a més informació: https://aws.amazon.com/iam/?nc1=h_ls

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

One Identity Manager

Versió	v9.0
Fabricant	One Identity
Família	Gestió d'identitats
Tipus	
Data Inclusió	
Revisió de Validesa	

Descripció

One Identity Manager és una solució de govern i gestió d'identitats (IAM) que permet automatitzar la gestió dels accessos dels usuaris, permetent que accedeixin a les aplicacions i a les dades estrictament necessàries per a exercir el seu treball. La solució permet que l'administració dels usuaris, les seves identitats digitals i els seus accessos puguin ser impulsades per altres departaments com a RH.

Permet:

- Gestionar l'accés a recursos en les instal·lacions, en el núvol i híbrids des de qualsevol departament de l'organització.
- Reduir el risc en assegurar-se que els usuaris tinguin només els accessos que necessiten.
- Satisfer auditories i iniciatives de compliment amb polítiques de confirmació/recertificació.
- Atorgar drets d'accés en funció de rols, regles i polítiques definides.
- Establir processos estàndard d'aprovisionament i desaprovisionament per als seus empleats i proveïdors.
- Administrar de manera ràpida i fàcil l'accés a recursos a mesura que les responsabilitats de l'usuari evolucionin amb l'empresa.

Observacions

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

SailPoint IdentityIQ	
Versió	V8.3p2
Fabricant de	Sailpoint
Família	Gestió d'identitats (IM)
Tipus	Producte
Data Inclusió	01/07/2023
Revisió de Validesa	31/12/2025

Descripció

Sailpoint és una pl s i Accessos que ofereix una àmplia gamma de funcionalitats, la qu ució integral per a la gestió de les identitats en les organitzacions.

- Provisionament: onboarding de nous usuaris, canvis i desnonament, automatització en processos. Per a usuaris interns, col·laboradors i/o proveïdors.
- Govern d'accés: Visibilitat completa dels accessos de l'organització, certificació d'accés, compliment d'accés segons polítiques d'usuaris a aplicacions i dades.
- Gestió de contrasenyes.
- Segregació de funcions.
- Govern de núvol.

Observacions

CCN-STIC-1111 SAILPOINT IdentityIQ

7.3. SEGURETAT DE L'EXPLOTACIÓ

7.3.1. ANTIVIRUS / EPP (ENDPOINT PROTECTION PLATFORM)

Deep Security (Manager i Agente/Relay Linux/Windows)	
Versió	11.0
Fabricant	Trend Micro
Família	Antivirus / EPP (Endpoint Protection Platform)
Tipus	Producte
Data Inclusió	01/12/2021
Revisió de Validesa	31/07/2024
Descripció	

Deep Security és la resposta de Trend Micro per protegir el cloud híbrid siguin servidors físics o virtuals.

Gràcies al seu agent lleuger, el qual incorpora funcionalitats: EDR (amb resposta enfront d'amenaces conegudes, zero-day), enviament de telemetria a la plataforma XDR de Trend Micro (VisionOne), reputació web, control d'aplicacions, supervisió de logs, Supervisió d'Integritat (FIM), Firewall de Host i Host IPS (que incorpora la tecnologia d'apedaçament virtual), ajuda a millorar la postura de seguretat proporcionant seguretat, visibilitat i control. La qualificació abasta els següents components: Manager, Agent/Relay Linux i l'Agent/Relay Windows. El Virtual Appliance no està qualificat.

Observacions

CCN-STIC-1216 PES Trendmicro Deep Security

Intercept X Advanced with EDR

Versió	2023.2.0.47/2023.1.1
Fabricant	Sophos
Família	Antivirus / EPP (Endpoint Protection Platform)
Tipus	Producte
Data Inclusió	01/03/2020
Revisió de Validesa	21/05/2024
Descripció	

Sophos Intercept X Advanced amb EDR és una solució que ofereix protecció avançada de lloc treball i servidors. Està especialment dissenyada per aturar la gran majoria d'atacs i fer front a noves amenaces com ransomware, fileless, o atacs zero-day. Amb diferents capes de protecció, les primeres estan dissenyades per reduir la superfície d'atac a través del control d'USBs, control d'aplicacions, control de navegació i DLP. Posteriorment té capes que detecten, primer el mal conegut a través de les firmes que desenvolupen els Sophos LABS i, segon, el mal desconegut, com el ransomware, gràcies al monitoratge de processos, el control de comportament, utilitzant la tecnologia única de Deep Learning que permet detectar malware no identificat prèviament, i la detecció de tècniques d'explotació/atac i de post compromís. A més, la solució compta amb capacitats avançades de detecció i resposta intel·ligents (EDR) que permeten a l'organització fer investigacions i threat hunting per ser proactiu a l'hora d'identificar amenaces i investigar possibles esdeveniments maliciosos, així com comprendre l'abast i l'impacte o buscar els indicadors d'amenaces a tota la xarxa. Tot això des d'una única consola de gestió al núvol i un únic agent.

Observacions

CCN-STIC 1207 Procediment d'Ocupació Segur Sophos Central Intercept X

WatchGuard EPDR/Advanced EPDR

Versió 4.2 (Protection Agent v8.0)
Fabricante WatchGuard Tecnologies
Família Antivirus / EPP (Endpoint Protection Platform)
Tipus Servei
Data Inclusió 01/03/2023
Revisió de Validesa 31/05/2024
Descripció

WatchGuard EDR/EPP integra en una única solució un conjunt complet de tecnologies preventives en l'endpoint, amb capacitats EDR i el Servei Zero-Trust Application. Estén les capacitats de prevenció, detecció i resposta amb una gamma completa de capacitats de protecció de l'endpoint necessàries per evitar que les amenaces arribin als dispositius i servidors i reduir la superfície d'atac. Les seves capacitats de protecció avançada cobreixen totes fases de la Seguretat Adaptativa: Prevenció, Detecció, Resposta i Remediació, gràcies als serveis gestionats: servei de classificació del 100% dels programes, processos i executables en els endpoints i els serveis de Threat Hunting i Anàlisi Forense, que permet un reforçament de la seguretat corporativa contínua.

Observacions

CCN-STIC-1213 PES Panda Adaptative Defense 360

Cytomic EDR/EPDR

Versió 4.2 (Protection Agentr v8.0)
Fabricant Panda Security
Família Antivirus / EPP (Endpoint Protection Platform)
Tipus Producte
Data Inclusió 01/09/2020
Revisió de Validesa 31/05/2024
Descripció

Cytomic EPDR integra en una única solució un conjunt complet de tecnologies preventives en l'endpoint, amb capacitats EDR i el Servei Zero-Trust Application. Estén les capacitats de prevenció, detecció i resposta amb una gamma completa de capacitats de protecció de l'endpoint necessàries per evitar que les amenaces arribin als dispositius i servidors i reduir la superfície d'atac. Les seves capacitats de protecció avançada cobreixen totes fases de la Seguretat Adaptativa: Prevenció, Detecció, Resposta i Remediació, gràcies als serveis gestionats: servei de classificació del 100% dels programes, processos i executables en els endpoints i el servei de Threat Hunting i Anàlisi Forense, que permet un reforçament de la seguretat corporativa contínua.

Observacions

CCN-STIC-1211 Procediment d'ocupació assegurança Cytomic EPDR

Autonomous AI Endpoint Security Platform

Versión	Console Tokyo#19, agent 23.1.1
Fabricant	SentinelOne
Família	Antivirus / EPP (Endpoint Protection Platform)
Tipus	Servei
Data Inclusió	01/05/2023
Revisió de Validesa	30/06/2024

Descripció

SentinelOne és una plataforma de ciberseguretat que utilitza intel·ligència artificial i aprenentatge automàtic per detectar i prevenir amenaces avançades i malware. La plataforma proporciona una visibilitat completa de la xarxa i és capaç d'analitzar el comportament del sistema en temps real per detectar patrons anòmals. També ofereix característiques de gestió de punts finals i una resposta automatitzada a les amenaces. La plataforma és fàcil d'implementar i personalitzar, escalable i s'adapta a empreses de qualsevol mida. SentinelOne també ofereix serveis de suport tècnic i gestió d'incidents.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

Kaspersky Endpoint Security for Windows

Versió	12.1.0.506 AES256
Fabricant	KASPERSKY LAB, S.L.U.
Família	Antivirus / EPP (Endpoint Protection Platform)
Tipus	Producte
Data Inclusió	01/01/2024
Revisió de Validesa	30/06/2026

Descripció

Kaspersky Endpoint Security és una solució de protecció avançada que proporciona una protecció integral mitjançant components de control (Control de dispositius, Control Web, Control d'anomalies adaptable) i de protecció (Detecció de comportament, Prevenció de vulnerabilitats, Prevenció d'intrusions en el host, Motor de reparació, Protecció enfront d'amenaces en arxius, Protecció enfront d'amenaces web, Protecció davant amenaces en el correu, Protecció davant amenaces a la xarxa, Firewall, Prevenció d'atacs de BadUSB, Proveïdor de protecció AMSI). Aquest enfocament de protecció multicapa permet detectar i bloquejar amenaces com Ransomware, atacs sense arxius (Fileless), atacs de dia zero, atacs de xarxa o atacs mitjançant l'ús d'Exploits o tècniques Phishing. Les seves capacitats de protecció avançada cobreixen les fases de Seguretat Adaptativa de Prevenció, Detecció i Resposta (Remediació). Compta amb capacitats avançades de detecció i resposta intel·ligents que permeten fer investigacions, anàlisis forenses i Threat Hunting per ser proactiu a l'hora d'identificar amenaces i investigar esdeveniments maliciosos, així com buscar els indicadors d'amenaces a tota la xarxa. Tot això des d'una única consola de gestió.

La integració amb Karspersky Security Center (KSC) està exclosa de la qualificació.

Observacions

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

Cortex XDR Agente Windows

Versió	7.5CE
Fabricant	Palo Alto
Família	Antivirus / EPP (E atform)
Tipus	Producte
Data Inclusió	01/07/2022
Revisió de Validesa	31/12/2024

Descripció

Cortex XDR és una solució de prevenció, detecció i resposta que integra de forma nativa la telemetria des de la xarxa, els endpoints i el núvol per aturar els atacs més sofisticats. L'agent Windows, que és el component qualificat, es fonamenta en una estratègia de detecció, prevenció i aprenentatge continu.

És capaç de detectar les amenaces amb precisió gràcies a l'anàlisi de comportament, revelant la causa original de cada incident per accelerar les investigacions. A més, s'integra perfectament amb les diferents solucions de seguretat que apliquen les polítiques, de manera que es posin en marxa els mecanismes de contenció al més aviat possible.

Pel que fa a la prevenció, ofereix una estratègia multidisciplinària per tal de prevenir no només les amenaces conegudes, sinó també les que no ho són. En el cas dels exploits, és possible prevenir els dies zero d'acord amb la detecció de les tècniques que s'utilitzen per aprofitar-se de les vulnerabilitats. Pel que fa al malware, cada arxiu s'examina amb un motor d'anàlisi local adaptatiu, basat en intel·ligència artificial, que aprèn constantment per combatre les noves tècniques. A més, un motor d'anàlisi dinàmica observa com es comporten els processos per detectar a l'instant qualsevol atac.

Cortex XDR permet que els equips de seguretat puguin aturar ràpidament la propagació del malware tant a l'endpoint com a la xarxa, habilitant-los a més per a les tasques de rènting o resposta a incidents.

Observacions

CCN-STIC-1222 Procediment d'ocupació assegurança Agente Cortex XDR

Falcon Sensor con Falcon Console Cloud

Versió	6.49
Fabricant	CrowdStrike
Família	Antivirus / EPP (Endpoint Protection Platform)
Tipus	Producte
Data Inclusió	01/09/2022
Revisió de Validesa	30/04/2024

Descripció

La plataforma CrowdStrike Falcon®, construïda sobre coneixement d'adversaris (intel·ligència d'amenaces) ofereix i unifica la higiene de TI, l'antivirus de nova generació, la detecció i resposta de punts finals (EDR), threat hunting i la intel·ligència d'amenaces, tot això a través d'un únic agent lleuger de desplegament ràpid i senzill sense requerir reinici ni impacte significatiu en el rendiment dels sistemes protegits. L'agent de Falcon registra totes les activitats d'interès en un punt final (llocs de treball, servidors, mobilitat i cloud) per a una inspecció més profunda, fins i tot aquelles que evadeixen les mesures de prevenció estàndard, aplicant tècniques de Deep Machine Learning i IA, Protecció basada en el comportament de l'Indicador d'Atac (IOA), protecció antiexploit i gestió de IOCs.

Observacions

CCN-STIC-1217 PES FALCON SENSOR

Panda Adaptive Defense 360

Versió	4.2 (Protection Agent v8.0)
Fabricant	Panda Security
Família	Antivirus / EPP (Endpoint Protection Platform)
Tipus	Producte
Data Inclusió	01/09/2020
Revisió de Validesa	31/05/2024

Descripció

Panda Adaptive Defense 360 és una solució de seguretat completa per als llocs de treball, portàtils i servidors que a més de protegir contra amenaces conegudes, avançades i zero-day, ransomware i atacs de seguretat fileless (en memòria) i malwareless, inclou firewall personal, IPS/IDS, anti-spam, anti-spam en correu, filtratge i categorització en navegació web i control de dispositius, entre altres tècniques de seguretat i control de productivitat. Les seves capacitats de protecció avançada cobreixen totes fases de la Seguretat Adaptativa: Prevenció, Detecció, Resposta i Remediació, gràcies als serveis gestionats: servei de classificació del 100% dels programes, processos i executables en els endpoints i els serveis de Threat Hunting i Anàlisi Forense, que permet un reforçament de la seguretat corporativa contínua.

Observacions

CCN-STIC-1213 PES Panda Adaptative Defense 360

7.3.2. EDR (ENDPOINT DETECTION AND RESPONSE)

Deep Security (Manager i Agente/Relay Linux/Windows)	
Versió	11.0
Fabricant	Trend Micro
Família	Antivirus / EPP (Endpoint Protection Platform)
Tipus	Producte
Data Inclusió	01/12/2021
Revisió de Validesa	31/07/2024
Descripció	

Deep Security és la resposta de Trend Micro per protegir el cloud híbrid siguin servidors físics o virtuals.

Gràcies al seu agent lleuger, el qual incorpora funcionalitats: EDR (amb resposta enfront d'amenaces conegudes, zero-day), enviament de telemetria a la plataforma XDR de Trend Micro (VisionOne), reputació web, control d'aplicacions, supervisió de logs, Supervisió d'Integritat (FIM), Firewall de Host i Host IPS (que incorpora la tecnologia d'apedaçament virtual), ajuda a millorar la postura de seguretat proporcionant seguretat, visibilitat i control. La qualificació abasta els següents components: Manager, Agent/Relay Linux i l'Agent/Relay Windows. El Virtual Appliance no està qualificat.

Observacions

CCN-STIC-1216 PES Trendmicro Deep Security

Microsoft Defender for Endpoint

Versió

Fabricante Microsoft Iberica SRL

Família EDR (Endpoint Dete e)

Tipus Servei

Data Inclusió 01/12/2022

Revisió de Validesa 30/11/2024

Descripció

Microsoft Defender for Endpoint és una solució EDR al núvol que protegeix les organitzacions públiques i/o privades contra amenaces en línia i en tota classe de dispositius. Utilitza tecnologies en temps real per prevenir, detectar, investigar i respondre a amenaces avançades. Entre les seves funcionalitats proporciona tècniques per a la reducció de la superfície d'atac, protecció contra amenaces i vulnerabilitats incloent l'ús d'Intel·ligència Artificial, detecció i resposta mitjançant el monitoratge de comportaments i tècniques dels atacants, capacitats d'investigació avançada i automatització de respostes, així com accés als experts en ciber-amenaces de Microsoft.

Microsoft Defender for Endpoint pot controlar i monitorar l'accés a tots els recursos d'una organització pública o privada de forma centralitzada, la qual cosa permet detectar i resoldre problemes de seguretat de manera ràpida i eficient a més d'estar integrada amb altres productes de Microsoft, com Office 365 i Azure.

Observacions

CCN-STIC-885E Guia de configuració segura per a Microsoft Defender for Endpoint

Intercept X Advanced with EDR

Versió	2023.2.0.47/2023.1.1
Fabricant	Sophos
Família	EDR (Endpoint Detection and Response)
Tip	Producte
Da	01/03/2020
Re	31/05/2024
De	

Sophos Intercept X Advanced amb EDR és una solució que ofereix protecció avançada de lloc treball i servidors. Està especialment dissenyada per aturar la gran majoria d'atacs i fer front a noves amenaces com ransomware, fileless, o atacs zero-day. Amb diferents capes de protecció, les primeres estan dissenyades per reduir la superfície d'atac a través del control d'USBs, control d'aplicacions, control de posteriorment té capes que detecten, primer el mal conegut a través de les firmes que Sophos LABS i, segon, el mal desconegut, com el ransomware, gràcies al monitoratge de processos, el control de comportament, utilitzant la tecnologia única de Deep Learning que permet detectar malware no identificat prèviament, i la detecció de tècniques d'explotació/atac i de post compromís. A més, la solució compta amb capacitats avançades de detecció i resposta intel·ligents (EDR) que permeten a l'organització fer investigacions i threat hunting per ser proactiu a l'hora d'identificar amenaces i investigar possibles esdeveniments maliciosos, així com comprendre l'abast i l'impacte o buscar els indicadors d'amenaces a tota la xarxa. Tot això des d'una única consola de gestió al núvol i un únic agent.

Observacions

CCN-STIC 1207 Procediment d'Ocupació Segur Sophos Central Intercept X

WatchGuard EPDR/Advanced EPDR

Versió	4.2 (Protection Agent v8.0)
Fabricante	WatchGuard Tecnologies
Família	EDR (Endpoint Detection and Response
Tipus	Servei
Data Inclusió	01/03/2023
Revisió de Validesa	31/05/2024

Descripció

WatchGuard EDR/EPP integra en una única solució un conjunt complet de tecnologies preventives en l'endpoint, amb capacitats EDR i el Servei Zero-Trust Application. Estén les capacitats de prevenció, detecció i resposta amb una gamma completa de capacitats de protecció de l'endpoint necessàries per evitar que les amenaces arribin als dispositius i servidors i reduir la superfície d'atac. Les seves capacitats de protecció avançada cobreixen totes fases de la Seguretat Adaptativa: Prevenció, Detecció, Resposta i Remediació, gràcies als serveis gestionats: servei de classificació del 100% dels programes, processos i executables en els endpoints i els serveis de Threat Hunting i Anàlisi Forense, que permet un reforçament de la seguretat corporativa contínua.

Observacions

CCN-STIC-1213 PES Panda Adaptative Defense 360

Cytomic EDR/EPDR

Versió	4.2 (Protection Agent v8.0)
Fabricant	Panda Security
Família	EDR (Endpoint Detection and Response)
Tipus	Producte
Data Inclusió	01/09/2020
Revisió de Validesa	31/05/2024

Descripció

Cytomic EPDR integra en una única solució un conjunt complet de tecnologies preventives en l'endpoint, amb capacitats EDR i el Servei Zero-Trust Application. Estén les capacitats de prevenció, detecció i resposta amb una gamma completa de capacitats de protecció de l'endpoint necessàries per evitar que les amenaces arribin als dispositius i servidors i reduir la superfície d'atac. Les seves capacitats de protecció avançada cobreixen totes fases de la Seguretat Adaptativa: Prevenció, Detecció, Resposta i Remediació, gràcies als serveis gestionats: servei de classificació del 100% dels programes, processos i executables en els endpoints i el servei de Threat Hunting i Anàlisi Forense, que permet un reforçament de la seguretat corporativa contínua.

Observacions

CCN-STIC-1211 Procediment d'ocupació assegurança Cytomic EPDR

Autonomous AI Endpoint Security Platform

Versión	Console Tokyo#19, agent 23.1.1
Fabricant	SentinelOne
Família	EDR (Endpoint Detection and Response)
Tipus	Servei
Data Inclusió	01/05/2023
Revisió de Validesa	30/06/2024

Descripció

SentinelOne és una plataforma de ciberseguretat que utilitza intel·ligència artificial i aprenentatge automàtic per detectar i prevenir amenaces avançades i malware. La plataforma proporciona una visibilitat completa de la xarxa i és capaç d'analitzar el comportament del sistema en temps real per detectar patrons anòmals. També ofereix característiques de gestió de punts finals i una resposta automatitzada a les amenaces. La plataforma és fàcil d'implementar i personalitzar, escalable i s'adapta a empreses de qualsevol mida. SentinelOne també ofereix serveis de suport tècnic i gestió d'incidents.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

Kaspersky Endpoint Security for Windows

Versió	11.6.0.395 AES256
Fabricant	KASPERSKY LAB, S.L.U.
Família	EDR (Endpoint Detection and Response)
Tipus	Producte
Data Inclusió	01/02/2024
Revisió de Validesa	30/06/2026

Descripció

Kaspersky Endpoint Security és una solució de protecció avançada que proporciona una protecció integral mitjançant components de control (Control de dispositius, Control Web, Control d'anomalies adaptable) i de protecció (Detecció de comportament, Prevenció de vulnerabilitats, Prevenció d'intrusions en el host, Motor de reparació, Protecció enfront d'amenaces en arxius, Protecció enfront d'amenaces web, Protecció davant amenaces en el correu, Protecció davant amenaces a la xarxa, Firewall, Prevenció d'atacs de BadUSB, Proveïdor de protecció AMSI). Aquest enfocament de protecció multicapa permet detectar i bloquejar amenaces com Ransomware, atacs sense arxius (Fileless), atacs de dia zero, atacs de xarxa o atacs mitjançant l'ús d'Exploits o tècniques Phishing. Les seves capacitats de protecció avançada cobreixen les fases de Seguretat Adaptativa de Prevenció, Detecció i Resposta (Remediació). Compta amb capacitats avançades de detecció i resposta intel·ligents que permeten fer investigacions, anàlisis forenses i Threat Hunting per ser proactiu a l'hora d'identificar amenaces i investigar esdeveniments maliciosos, així com buscar els indicadors d'amenaces a tota la xarxa. Tot això des d'una única consola de gestió.

La integració amb Karspersky Security Center (KSC) està exclosa de la qualificació.

Observacions

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

Cortex XDR Agente Windows

Versió	7.5CE
Fabricant	Palo Alto
Família	EDR (Endpoint Detection and Response)
Tipus	Producte
Data Inclusió	01/07/2022
Revisió de Validesa	31/12/2024

Descripció

Cortex XDR és una solució de prevenció, detecció i resposta que integra de forma nativa la telemetria des de la xarxa, els endpoints i el núvol per aturar els atacs més sofisticats. L'agent Windows, que és el component qualificat, es fonamenta en una estratègia de detecció, prevenció i aprenentatge continu.

És capaç de detectar les amenaces amb precisió gràcies a l'anàlisi de comportament, revelant la causa original de cada incident per accelerar les investigacions. A més, s'integra perfectament amb les diferents solucions de seguretat que apliquen les polítiques, de manera que es posin en marxa els mecanismes de contenció al més aviat possible.

Pel que fa a la prevenció, ofereix una estratègia multidisciplinària per tal de prevenir no només les amenaces conegudes, sinó també les que no ho són. En el cas dels exploits, és possible prevenir els dies zero d'acord amb la detecció de les tècniques que s'utilitzen per aprofitar-se de les vulnerabilitats. Pel que fa al malware, cada arxiu s'examina amb un motor d'anàlisi local adaptatiu, basat en intel·ligència artificial, que aprèn constantment per combatre les noves tècniques. A més, un motor d'anàlisi dinàmica observa com es comporten els processos per detectar a l'instant qualsevol atac.

Cortex XDR permet que els equips de seguretat puguin aturar ràpidament la propagació del malware tant a l'endpoint com a la xarxa, habilitant-los a més per a les tasques de rènting o resposta a incidents.

Observacions

CCN-STIC-1222 Procediment d'ocupació assegurança Agente Cortex XDR

Falcon Sensor amb Falcon Console Cloud

Versió 7.05 (Falcon Sensor)

Fabricant CrowdStrike

Família EDR (Endpoint Detection and Response)

Tipus Producte

Data Inclusió 01/09/2022

Revisió de Validesa 30/04/2024

Descripció

La plataforma CrowdStrike Falcon®, construïda sobre coneixement d'adversaris (Intel·ligència d'amenaces) ofereix i unifica la higiene de TI, l'antivirus de nova generació, la detecció i resposta de punts finals (EDR), threat hunting i la intel·ligència d'amenaces, tot això a través d'un únic agent lleuger de desplegament ràpid i senzill sense requerir reinici ni impacte significatiu en el rendiment dels sistemes protegits. L'agent de Falcon registra totes les activitats d'interès en un punt final (llocs de treball, servidors, mobilitat i cloud) per a una inspecció més profunda, fins i tot aquelles que evadeixen les mesures de prevenció estàndard, aplicant tècniques de Deep Machine Learning i IA, Protecció basada en el comportament de l'Indicador d'Atac (IOA), protecció antiexploit i gestió de IOCs.

Observacions

CCN-STIC-1217 PES FALCON SENSOR

Sandblast (Harmony) Mobile per a iOS i Android

Versió 3.8

Fabricant Check Point Software Technologies

Familia EDR (Endpoint Detection and Response)

Tipus Producte

Data Inclusió 01/04/2021

Revisió de Validesa 31/12/2024

Descripció

Harmony Mobile és una completa solució de defensa contra amenaces mòbils per a les plataformes d'iOS i Android. Manté les seves dades corporatives segures perquè protegeix els dispositius mòbils dels empleats de tots els vectors d'atac: aplicacions, xarxa i sistema operatiu. Dissenyada per reduir les despeses generals dels administradors i augmentar l'adopció de l'usuari, s'adapta perfectament al seu entorn mòbil existent, s'implementa i escala ràpidament, i protegeix els dispositius sense afectar l'experiència ni la privacitat de l'usuari.

Observacions

CCN-STIC-1212 Procediment d'ocupació assegurança Harmony Sandblast Mobile

Panda Adaptive Defense 360

Versió	4.2 (Protection Agent v8.0)
Fabricant	Panda Security
Família	EDR (Endpoint Detection and Response)
Tipus	Producte
Data Inclusió	01/09/2020
Revisió de Validesa	31/05/2024

Descripció

Panda Adaptive Defense 360 és una solució de seguretat completa per als llocs de treball, portàtils i servidors que a més de protegir contra amenaces conegudes, avançades i zero-day, ransomware i atacs de seguretat fileless (en memòria) i malwareless, inclou firewall personal, IPS/IDS, anti-spam, anti-spam en correu, filtratge i categorització en navegació web i control de dispositius, entre altres tècniques de seguretat i control de productivitat. Les seves capacitats de protecció avançada cobreixen totes fases de la Seguretat Adaptativa: Prevenció, Detecció, Resposta i Remediació, gràcies als serveis gestionats: servei de classificació del 100% dels programes, processos i executables en els endpoints i els serveis de Threat Hunting i Anàlisi Forense, que permet un reforçament de la seguretat corporativa contínua.

Observacions

CCN-STIC-1213 PES Panda Adaptative Defense 360

7.3.3. EINES DE FILTRATGE DE NAVEGACIÓ

FortiManager (FMG-300Fi FMG-1000F)	
Versió	6.4
Fabricant	Fortinet
Família	Eines de filtratge de navegació
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	09/10/2024
Descripció	

Gestió centralitzada mitjançant interfície gràfica de dispositius Fortinet incloent: FortiGate, FortiSwitches, FortiAP, FortiClient. Facilita la descàrrega de signatures FortiGuard per a entorns estancs sense connexió a internet. Revisió, aprovació i auditoria de polítiques de seguretat i/o gestió de les comunicacions, procés automatitzat per a facilitar el compliment de les polítiques i gestió del cicle de vida d'aquestes. Disseny de fluxos de treball per a reduir el risc o impacte sobre el servei. API per a l'automatització i orquestració. Capacitat de configuració col·lectiva dels dispositius, els objectes i les polítiques des d'una única interfície d'usuari, amb possibilitat de creació de diferents rols de gestió o aprovació, arribant a poder distingir perfils o grau d'aplicació en funció de les garanties de seguretat, accés, moment o ubicació d'aquest. Agrupació i gestió flexible lògica o geogràfica de dispositius. Facilita el desplegament i acte-provisió en mode ""Zero Touch".

Observacions

CCN-STIC-1443 Procedimiento de empleo seguro FortiManager

FortiManager (FMG-200G, FMG-400G, FMG-3000G, FMG-3700G, FMG-VM)

Versió	6.4
Fabricant	Fortinet
Família	Eines de filtratge de navegació
Tipus	Producte
Data Inclusió	01/03/2024
Revisió de Validesa	09/10/2024

Descripció

Gestió centralitzada mitjançant interfície gràfica de dispositius Fortinet incloent: FortiGate, FortiSwitches, FortiAP, FortiClient. Facilita la descàrrega de signatures FortiGuard per a entorns estancs sense connexió a internet. Revisió, aprovació i auditoria de polítiques de seguretat i/o gestió de les comunicacions, procés automatitzat per a facilitar el compliment de les polítiques i gestió del cicle de vida d'aquestes. Disseny de fluxos de treball per a reduir el risc o impacte sobre el servei. API per a l'automatització i orquestració. Capacitat de configuració col·lectiva dels dispositius, els objectes i les polítiques des d'una única interfície d'usuari, amb possibilitat de creació de diferents rols de gestió o aprovació, arribant a poder distingir perfils o grau d'aplicació en funció de les garanties de seguretat, accés, moment o ubicació d'aquest. Agrupació i gestió flexible lògica o geogràfica de dispositius. Facilita el desplegament i acte-provisió en mode ""Zero Touch".

Observacions

CCN-STIC-1443 Procedimiento de empleo seguro FortiManager

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

Versió	AsyncOS 11.8
Fabricant	Cisco Systems
Família	Eines de filtratge de navegació
Tipus	Producte
Data Inclusió	01/12/2022
Revisió de Validesa	31/05/2025

Descripció

Cisco Secure Web Appliance proxy protegeix les organitzacions quant a navegació es refereix, avaluant les webs desconegudes abans de permetre que els usuaris hi accedeixin i bloquejant automàticament les pàgines de risc. Utilitzant funcions d'alt rendiment, Cisco Secure Web Appliance manté segurs els usuaris.

Observacions

CCN-STIC-1625 Procediment d'Ocupació Segur Cisco Web Security Appliance

7.3.4. SISTEMES DE GESTIÓ D'ESDEVENIMENTS DE SEGURETAT (SIEM)

FortiAnalyzer (FAZ-800F, FAZ-1000F, FAZ-2000E, FAZ-3000F, FAZ-3500G, FAZ-3700F, FAZ-3000G y FAZ-VM)	
Versió	6.4
Fabricant	Fortinet
Família	Sistemes de gestió d'esdeveniments de seguretat (SIEM)
Tipus	Producte
Data Inclusió	01/05/2024
Revisió de Validesa	09/10/2024
Descripció	

Consola web que ofereix visibilitat en temps real, informes baix demanda o programats per a ser exportats en diferents formats (PDF, Mail, etc) per a dispositius Fortinet (FortiGate, FortiDDoS, FortiClient, FortiCarrier, Forticlient EMS, FortiMail, FortiWeb, FortiCache, FortiSandbox, etc.). També,mitjançant Syslog, productes d'altres fabricants. Facilita la realització d'anàlisi forense, compliment legal, descobriment i recerca d'esdeveniments d'una manera centralitzada i correlada. Exploració multi-capa. Ús de plantilles predefinides (Revisió Seguretat 360è, Aplicacions, Amenaces, ús de Web, compliment normatiu, activitat Wifi, VPN, consumeixo amplada de banda, etc). Capacitat de creació de diferents perfils d'administració per a entorns concrets o capacitats d'escriptura o lectura configurades per entorn. Àmplia gamma de dispositius físics o virtuals que proporcionen solució escalable.

Observacions

CCN-STIC-1444 Procedimiento de empleo seguro FortiAnalyzer

MONICA

Versió	7.1
Fabricant	Grupo ICA Sistemas y Seguridad
Família	Sistemes de gestió d'esdeveniments de seguretat (SIEM)
Tipus	Producte
Data Inclusió	01/05/2024
Revisió de Validesa	30/06/2024

Descripció

La plataforma espanyola Mónica permet als analistes de ciberseguretat r rmació il·limitada de seguretat, detectar atacs basats en anomalies i comportaments desconeguts així com automatitzar la resposta davant incidents en entorns IT, OT i IoT. Mónica recopila informació de qualsevol font interna i externa a l'empresa (comercial, propietària, aplicacions, cloud), correlando i analitzant en temps real aquesta informació, permetent contextualitzar i prioritzar els incidents de seguretat tant interns com externs. Combina els casos d'ús de detecció més sofisticats amb la informació més precisa d'amenaces i vulnerabilitats zero day gràcies a la informació de fonts

Observacions

CCN-STIC-1206 PES NGSIEM LogICA

Microsoft Sentinel

Versió

Fabricante Microsoft Iberica SRL

Família Sistemes de gestió d'esdeveniments de uretat (SIEM)

vei

Data incl '02/2023

Revisió d '01/2025

Descripció

Microsoft Sentinel és una plataforma SIEM/SOAR de seguretat al núvol dissenyat per ajudar les organitzacions a detectar, investigar i respondre a amenaces de seguretat. Incorpora capacitats d'automatització i una visió completa de la seguretat d'una organització.

Permet agilitzar i modernitzar les operacions de qualsevol centre de seguretat (SOC) eliminant la configuració i el manteniment de la infraestructura de seguretat, aprofitant l'elasticitat i l'escalabilitat del núvol, alhora que redueix els costos. És una solució enfocada a detectar ràpidament les amenaces reals, reduint els falsos positius gràcies a l'ús de l'aprenentatge automàtic integrat i a coneixements basats en l'anàlisi diària de bilions de senyals.

Permet a més accelerar la recerca proactiva d'amenaces amb consultes predefinides basades en anys d'experiència en seguretat, disposa de llistes prioritzades d'alertes, anàlisis de correlacionats de milers d'esdeveniments de seguretat de forma ràpida i visualització de l'abast complet de cada atac. Permet simplificar les operacions de seguretat i accelerar la resposta a les amenaces amb l'automatització integrada i l'orquestració de tasques i fluxos de treball.

Pot connectar i recopilar dades de diferents fonts, inclosos usuaris, aplicacions, servidors i dispositius que s'executen en una infraestructura on-premise o en qualsevol núvol. I té la capacitat d'integrar-se amb eines existents, siguin aplicacions empresarials, o altres productes d'anàlisi de seguretat o eines pròpies, i crear i utilitzar els seus propis models d'aprenentatge automàtic.

Observacions

CCN-STIC 1229 Procedimiento de Empleo Seguro MS Sentinel

IBM QRadar Security Intelligence Platform	
Versió	7.5
Fabricant	IBM
Família	Sistemes de gestió d'esdeveniments de seguretat (SIEM)
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/12/2026

Descripció

La família de productes QRadar, plataforma de seguretat intel·ligent líder al mercat SIEM, ofereix una visibilitat absoluta i unificada de la seguretat en temps real. QRadar recol·lecta, consolida i correlaciona informació de tots els endpoints, dispositius de xarxa, entorns dels núvols, aplicacions i fins i tot de diferents data-lakes. Aplica anàlisi avançada per prioritzar les amenaces i classificar-les amb més precisió. Addicionalment, aquesta tecnologia ofereix capacitats de recerques avançades per ajudar a trobar noves amenaces de forma proactiva i proporciona totes les funcionalitats que una organització necessita per abordar els desafiaments de seguretat més importants.

Observacions

CCN-STIC-1203 Procediment d'ocupació segur IBM QRadar Security Intelligence Platform

Chronicle SIEM

Versió	**N/A**
Fabricant	Google
Família	Sistemes de gestió d'esdeveniments de seguretat (SIEM)
Tipus	Producte
Data Inclusió	16/02/2024
Revisió de Validesa	16/08/2024

Descripció

Chronicle SIEM, una solució de gestió d'esdeveniments i informació de segure[illegible]l núvol, permet als clients recopilar i analitzar la telemetria de seguretat de tota la seva empresa per a potenciar la detecció, recerca i remediació d'amenaces.

Com a part del servei, Chronicle SIEM normalitza, correlaciona i enriqueix les dades de seguretat per a proporcionar anàlisi i context sobre activitats sospitoses.

Chronicle SIEM inclou Google Cloud Threat Intelligence, que és un servei d'intel·ligència d'amenaces agregat per a clients de Chronicle SIEM que aprofita la intel·ligència d'amenaces de Google per a ressaltar amenaces en els seus entorns de núvol i on-premise.

Està recolzat per analistes d'amenaces de Google que verifiquen els indicadors maliciosos en la

telemetria de seguretat i revelen alertes contextualitzades als clients, la qual cosa els permet donar una resposta informada.

Observacions

Procediment d'Ocupació Segura pendent de publicació

ASIP (AIUKEN SECURITY INTELLIGENCE PLATFORM)

Versió	Delfos Linux Agent v0.8.10
Fabricant:	AIUKEN SOLUTIONS
Família	Sistemes de gestió d'esdeveniments de seguretat (SIEM)
Tipus	Servei
Data Inclusió	01/03/2023
Revisió de Validesa	**30**/06/2024

Descripció

ASIP (Aiuken Security Intelligence Platform), és una Plataforma completa de gestió SOC, que encara capacitats avançades de correlació i detecció primerenca d'esdeveniments de seguretat, millorant-les a través d'aprenentatge i Intel·ligència Artificial integració dels framework de seguretat MITRE Attack per a atacs, CAPEC per a detecció de vulnerabilitats i NIST per a la gestió dels controls de seguretat de les companyies, permetent no tenir una dependència tan alta del model tradicional de casos d'ús

Integra al seu torn, portal de servei, gestió de casos i ticketing, motor de generació de panells informatius i KPIs, Threat Intelligence pròpia i eines per a Threat Hunting i detecció primerenca. L'automatització és un altre dels avantatges d'ASIP, orquestració i SOAR per al modelatge de processos autogestionat i generació d'informes de servei de forma automàtica, permetent als tècnics enfocar-se en les tasques importants.

De la mateixa manera és possible integrar qualsevol font disponible a la companyia i fins i tot aprofitar les capacitats d'integració nativa de l'eina amb Azure, Google Cloud i AWS per poder tenir una visibilitat completa de totes les fonts de la companyia, tant externes com internes.

Observacions

Procediment d'Ocupació Segura pendent de publicació

MONSE	
Versió	Probe 1.0, Agent 8.3.2
Fabricant	GRUPO CIES
Família	Sistemes de gestió d'esdeveniments de seguretat (SIEM)
Tipus	Producte
Data Inclusió	01/11/2022
Revisió de Validesa	01/11/2024

Descripció

MONSE (MONitoratge de la SEguretat) és una solució SIEM que permet recopilar i correlacionar de forma centralitzada múltiples fonts d'esdeveniments de seguretat. La solució permet analitzar esdeveniments basats en logs, processos, comportament i IOCs. Disposa de tècniques d'Intel·ligència Artificial que faciliten la detecció d'anomalies, integració de fonts d'intel·ligència d'amenaces, possibilitat de definir regles d'alerta adaptades a la particularitat de cada organització, així com la possibilitat de crear quadres de comandament personalitzables. La plataforma permet un desplegament modular en funció del tipus de maduresa de l'organització. Disposa de múltiples funcionalitats orientades a la millora en el compliment de l'Esquema Nacional de Seguretat.

Observacions

CCN-STIC 1223 Procedimiento de empleo seguro MONSE

Splunk Enterprise

Versió	9.0.4
Fabricante	Splunk Inc.
Família	Sistemes de gestió d'esdeveniments de seguretat (SIEM)
Tipus	Producte
Data Inclusió	01/01/2024
Revisió de Validesa	14/06/2024

Descripció

Splunk Enterprise és una plataforma de gestió d'esdeveniments i informació de seguretat (SIEM) que proporciona una visibilitat completa de la seva postura de seguretat. Splunk Enterprise permet gestionar el cicle complet en una organització, incloent-hi capacitats de Detecció, Monitoratge, Recerca i Resposta davant incidents de Seguretat. Incorpora capacitats de cerca i generació d'informes sense precedents, anàlisis avançades, intel·ligència artificial integrada i contingut de seguretat predefinit i dinàmic per a accelerar la detecció i recerca d'amenaces. Splunk permet classificar per prioritat els incidents, prioritzant els incidents que afectin actius o identitats crítics. Permet generar alertes basades en risc, identificant anomalies i amenaces tant externes com internes. Les més de 2500 regles de detecció abasten tots els àmbits de seguretat: IT, OT, IoT, IoMT i els núvols públics en qualsevol dels seus formats.

Observacions

Procedimiento de empleo pendiente de actualización. Existe un PES de una versión anterior del producto:

CCN-STIC-1225

NetWitness Platform	
Versió	11.6
Fabricante	Netwitne
Família	Sistemes seguretat (SIEM)
Tipus	Producte
Data Inclusió	01/07/2022
Revisió de Validesa	31/12/2024

Descripció

La plataforma XDR de Netwitness (an RSA Business), és la solució de SIEM o XDR (eXtended Detection and Response), amb capacitats de visibilitat completa gràcies al seu model de dades unificat podent capturar logs, netflows, trànsit de xarxa, activitat en els end points, a més d'informació d'intel·ligència de seguretat, de forma integrada, sota un únic motor d'anàlisi i correlació avançada. A més, inclou funcionalitats necessàries per a un SOC per fer front a amenaces complexes. Netwitness Platform XDR compta a més amb components addicionals com UEBA (User and Entity Behaviour Analitics) i SOAR (Security Orchestration and Automation Response). La solució permet capturar tota mena d'informació, permetent l'anàlisi avançada d'amenaces, priorització d'acord amb el context de negoci i fent més eficient el treball de l'analista. És una plataforma que, gràcies a la seva capacitat d'anàlisi, mostra l'abast complet d'un atac als analistes. A més, gràcies a la seva estratègia Run Anywhere, la plataforma es pot desplegar en qualsevol entorn (virtual, cloud, físic o híbrid), així com fer front a arquitectures altament distribuïdes. RSA Netwitness inclou en tots els seus clients +50 feeds d'intel·ligència, agent per a endpoints il·limitats, així com el desplegament il·limitat de dispositius per cobrir qualsevol forma de desplegament. https:// www.netwitness.com/en- us/solutions/evolved-siem/

Observacions

CCN-STIC-1210 Procediment d'Ocupació Segur RSA Netwitness Platform

Gloria	
Versió	v5.8.1
Fabricant	S2 GRUPO / CCN
Família	Sistemes de gestió d'esdeveniments de seguretat (SIEM)
Tipus	Producte
Data Inclusió	01/01/2021
Revisió de Validesa	30/06/2024

Descripció

Glòria és una plataforma per a la gestió d'incidents i amenaces de ciberseguretat a través de tècniques de correlació complexa d'esdeveniments. Basat en els sistemes SIEM, va un pas més enllà de les capacitats de monitoratge, emmagatzematge i interpretació de les dades rellevants. Així, mitjançant tècniques de correlació complexa de diverses fonts d'esdeveniments o anàlisi de patrons per a la identificació d'anomalies, permet una orientació molt flexible cap a la vigilància del món IP. La plataforma permet les següents funcionalitats a través de diferents mòduls:

- Monitoratge d'entorns tecnològics (IT/OT).
- Intel·ligència.
- Gestió del servei.
- Automatització, orquestració i reducció de temps de resposta.

Per a més informació, (https://ccn-cert.cni.es/soluciones-seguridad/gloria.html)

Observacions

CCN-STIC-1215 Procediment d'ocupació segur GLORIA

LogICA5 Next Generation SIEM

Versió	v7.1
Fabricant	Grupo ICA Sistemas y Seguridad
Família	Sistemes de gestió d'esdeveniments de seguretat (SIEM)
Tipus	Producte
Data Inclusió	01/01/2020
Revisió de Validesa	30/06/2024

Descripció

La plataforma espanyola Next Generation SIEM LogICA permet als analistes de ciberseguretat recopilar logs i informació il·limitada de seguretat, detectar atacs basats en anomalies i comportaments desconeguts, així com automatitzar la resposta davant incidents en entorns IT, OT i IoT. LogICA NG SIEM recopila informació de qualsevol font interna i externa a l'empresa (comercial, propietària, aplicacions, cloud), correlant i analitzant en temps real aquesta informació, permetent contextualitzar i prioritzar els incidents de seguretat tant interns com externs. Combina els casos d'ús de detecció més sofisticats amb la informació més precisa d'amenaces i vulnerabilitats gràcies a la informació de fonts externes d'intel·ligència, threat hunting i anomalies de xarxa/usuari. Incorpora, a més, un quadre de comandament de gestió del servei, centralitzant la informació i facilitant el seu consum per part de l'organització. LogICA permet adaptar-se a les necessitats de desplegament de les organitzacions, en mode on-premise, virtual o entorn cloud.

Observacions

CCN-STIC-1206 PES NGSIEM LogICA

7.3.5. DISPOSITIUS PER A GESTIÓ DE CLAUS CRIPTOGRÀFIQUES

EP543N	
Versió	V.1.7
Fabricant:	Epicom
Família	Dispositius per a gestió de claus criptogràfiques
Tipus	Producte
Data Inclusió	27/12/2021
Revisió de Validesa	31/12/2024
Descripció	

Centre de Gestió de xifradors IP EP430GN sobre ordinador segur EP1140.

Observacions

Google KMS with EKM solution

Versió

Fabricant Google Cloud

Família Dispositius per a gestió de claus criptogràfiques

Tipus Servei

Data Inclusió 01/05/2023

Revisió de Validesa 30/04/2025

Descripció

Google Cloud External Key Manager (EKM) és un servei de Google Cloud que permet als clients generar i gestionar claus crip
xifrat nadiu d'informació al núvol a través d'un tercer, protegides a través d' está fora de les infra
núvol de Google. La protecció de la informació amb claus generades, proteg oveïdor de núvol, ha
de sobirania de la dada des del moment en què la informació emmagatzemada al núvol de Google Cloud només podrà ser desxif
extern de la clau, que podrà ser:

- El mateix usuari final mitjançant un mòdul EKM instal·lat en les seves pròpies infraestructures.
- Un soci de confiança de l'usuari final que hostatja i gestioni aquest mòdul EKM en les seves infraestructures.
- Un dels socis locals de Google Cloud (sotmesos exclusivament a legislació espanyola) amb la infraestructura ja pr preparada per oferir aquest servei des de la plataforma de Google Cloud, com a "Control de Sobirania" SIA/Minsait/Indra per a Espanya, Thales per a França o T-Systems per a Alemanya).

El servei EKM es presta des de múltiples regions de Google Cloud, inclosa la d'Espanya. Més info
https://cloud.google.com/kms/docs/ekm?hl=es-419

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

EP543X

Versió SW v 4.15

Fabricant: Epicom

Família Dispositius per a gestió de claus criptogràfiques

Tipus Producte

Data Inclusió 01/12/2017

Revisió de Validesa 31/12/2024

Descripció

Centre de Gestió sobre la plataforma EP1140, que dona suport als xifradors de la família EP430, inclosos els models EP430TX i EP430GX.

Observacions

Utilització segons PE-2012-49 Procediment d'Ocupació EP430GX v2

AWS Key Management Service (KMS)

Versió

Fabricant	AWS
Família	Dispositius per a gestió de claus criptogràfiques
Tipus	Servei
Data Inclusió	01/02/2022
Revisió de Validesa	30/06/2024

Descripció

AWS Key Management Service (KMS) facilita la creació i l'administració de claus criptogràfiques i el control del seu ús en una àmplia gamma de serveis d'AWS i en les seves aplicacions. Utilitza mòduls de seguretat de maquinari que s'han validat segons FIPS 140-2 per protegir les seves claus.

AWS KMS li proporciona un control centralitzat sobre les claus criptogràfiques que s'utilitzen per protegir les seves dades. El servei està integrat amb altres serveis d'AWS, la qual cosa facilita el xifrat de les dades que emmagatzema en aquests serveis i el control de l'accés a les claus que els desxifran. Els serveis integrats amb KMS es poden trobar en https://aws.amazon.com/kms/

Observacions

CCN-STIC-887A Guia de configuració segura AWS

7.4. MONITORATGE DE LA SEGURETAT

7.4.1. IDS, IPS I ANTIDDOS.

ASA 5500 Series (5508-X and 5516-X)	
Versió	7.0
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	30/04/2026
Descripció	

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
- FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observacions

CCN-STIC 651B Seguretat a Cortafocs Cisco Firepower

Cisco Firepower Threat Defense (FTD) en Firepower 1000 i 2100 Series (FP1010, FP1120, FP1140, FP2110, FP2120, FP2130, FP2140)	
Versió	FTD 6.4 i FMC/FCMv 6.4
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024
Descripció	

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Compatible amb:

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 i FMC4600-K9)
- FMCv executant-se en ESXi 6.0 o 6.5 en el Sistema Unificat de Computació (UCS) UCSB-B200-M4, UCSC-C220- M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S- M3 i UCS-E180D-M3

Observacions

CCN-STIC-651B Seguretat en tallafocs CISCO Firepower

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

Versió	6.5.4.4-44n-federal-12n
Fabricant	SonicWall
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	01/08/2021
Revisió de Validesa	28/02/2025
Descripció	

La Serie TZ de SonicWall ofereix seguretat i rendiment d'entorn Enterprise orientat a petites companyies. Enfocat a entorns departamentals o PIMES d'entre 5 i 100 usuaris (aprox), incorpora funcions de prevenció d'intrusions, antimalware, filtratge de continguts/URL i control d'aplicacions a través de xarxes i entorns sense fil. Proporciona inspecció profunda de paquets (DPI), SD-WAN i desplegament zero-touch. Opcions de ports PoE i wifi 802.11ac. Més info a: https:// www.sonicwall.com/es-mx/products/firewalls/entry-level

Observacions

CCN-STIC-1420 Procediment d'Ocupació Segur Sonicwall SonicOS

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

Versió	6.4
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	01/11/2022
Revisió de Validesa	30/04/2025
Descripció	

Sistema de Detecció i Prevenció d'Intrusions, que consisteix en una FMC i sensors.

La FMC proporciona una consola de gestió centralitzada i un sistema de base de dades d'esdeveniments, agrega i correlaciona dades d'intrusió, descobriment i connexió, recollides dels sensors gestionats.

Els sensors monitoritzen tot el trànsit de la xarxa a la recerca d'esdeveniments de seguretat i violacions i poden alertar o fins i tot bloquejar trànsit maliciós d'acord amb les regles definides per al control d'accés.

Observacions

CCN-STIC-651B Seguretat a Cortafocs Cisco Firepower

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

Versió	6.4
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	01/11/2022
Revisió de Validesa	30/04/2025
Descripció	

Sistema de Detecció i Prevenció d'Intrusions, que consisteix en una FMC i sensors.

La FMC proporciona una consola de gestió centralitzada i un sistema de base de dades d'esdeveniments, agrega i correlaciona dades d'intrusió, descobriment i connexió, recollits dels sensors gestionats.

Els sensors monitoritzen tot el trànsit de la xarxa a la recerca d'esdeveniments de seguretat i violacions i poden alertar o fins i tot bloquejar trànsit maliciós d'acord amb les regles definides per al control d'accés.

Observacions

CCN-STIC-651B Seguretat a Cortafocs Cisco Firepower

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

Versió	6.4
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	01/11/2022
Revisió de Validesa	30/04/2025
Descripció	

Sistema de Detecció i Prevenció d'Intrusions, que consisteix en una FMC i sensors.

La FMC proporciona una consola de gestió centralitzada i un sistema de base de dades d'esdeveniments, agrega i correlaciona dades d'intrusió, descobriment i connexió, recollits dels sensors gestionats.

Els sensors monitoritzen tot el trànsit de la xarxa a la recerca d'esdeveniments de seguretat i violacions i poden alertar o fins i tot bloquejar trànsit maliciós d'acord amb les regles definides per al control d'accés.

Observacions

CCN-STIC-651B Seguretat a Cortafocs Cisco Firepower

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

Versió	7.0
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	30/04/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Observacions

CCN-STIC 651B Seguretat a Cortafocs Cisco Firepower

Deep Discovery Inspector

Versió	6.5.1129
Fabricant	Trend Micro
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	N/A
Revisió de Validesa	16/05/2026

Descripció

Deep Discovery Inspector és una sonda de xarxa anti-APT dissenyada per detectar de manera primerenca ciberatacs al vector de xarxa (ex.: malware de dia 0, moviments laterals, comunicacions C&C, exfiltració de dades, explotació de vulnerabilitats etc.). Combinant tècniques de Reputació, Machine Learning i Sandboxing.

Disponible en format appliance físic o virtual, amb diferents nivells d'escalat d'ample de banda i configuració de ports, facilita la seva implementació en xarxes amb diferents nivells de complexitat. Integrada amb la plataforma XDR Trend Vision One, on aporta telemetria i deteccions, conforma la plataforma NDR perfecta per fer front als complexos atacs rebuts pel cibercrim modern.

Observacions

CCN-STIC 1227 Procedimiento de Empleo Seguro Deep Discovery Inspector

TippingPoint Threat Protection System

Fabricant	Trend Micro		
Família	IDS, IPS i AntiDDoS		
Tipus	Producte	**Versió**	5.4.1
Data Inclusió	01/02/2023		
Revisió de Validesa	31/07/2025		

Descripció

Trend Micro™ TippingPoint™ Threat Protection System (TPS) consisteix en un appliance IPS dedicat que ofereix protecció enfront d'un ampli catàleg d'amenaces: vulnerabilitats i malware tant coneguts com desconeguts, connexions sospitoses, geolocalització i filtres de protecció enfront de DDOS, suportant trànsit asimètric i inspecció SSL.

La combinació de la intel·ligència de la Smart Protection Network, Zero Day Initiative i un maquinari optimitzat proporciona nivells òptims de rendiment, baixa latència, gran efectivitat, escalabilitat i sota ràtio de falsos positius.

Aquesta tecnologia implementa interfícies de xarxa amb bypass amb l'objectiu d'evitar interrupcions de trànsit en el cas de fallada maquinari del dispositiu.

Addicionalment, compta amb la tecnologia eVR (Enterprise Vuln tzant integració amb tercers per importar vulnerabilitats i nous filtres.

Tipping Point s'integra dins de l'arquitectura Vision One XDR i la plataforma Deep Discovery de Trend Micro.

Observacions

CCN-STIC-1220 PES TIPPING POINT TRENDMICRO

FTD Virtual (FTDv) sobri ESXi 6.7 or 7.0 on Cisco Unified Computing System (UCS) - UCSC-C220-M5, UCSC-C240- M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3 installed on ISR	
Versió	7.0
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2024
Descripció	

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Observacions

Pendent de publicació de Procediment d'Ocupació Assegurança

Firepower 2100 Series (2120, 2120, 2130, 2140)	
Versió	FTD 7.0 y FMC 7.0
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	01/11/2022
Revisió de Validesa	30/04/2025
Descripció	

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Compatible amb:

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 i FMC4600-K9)
- FMCv executant-se en ESXi 6.0 o 6.5 en el Sistema Unificat de Computació (UCS) UCSB-B200-M4, UCSC-C220- M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S- M3 i UCS-E180D-M3

Observacions

CCN-STIC-651B Seguretat a Cortafocs Cisco Firepower

FMC (Firepower Management Center) Appliances: FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9	
Versió	6.4.0.17
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	01/11/2022
Revisió de Validesa	30/04/2025
Descripció	

Sistema de Detecció i Prevenció d'Intrusions, que consisteix en una FMC i sensors.

La FMC proporciona una consola de gestió centralitzada i un sistema de base de dades d'esdeveniments, agrega i correlaciona dades d'intrusió, descobriment i connexió, recollits dels sensors gestionats.

Els sensors monitoritzen tot el trànsit de la xarxa a la recerca d'esdeveniments de seguretat i violacions i poden alertar o fins i tot bloquejar trànsit maliciós d'acord amb les regles definides per al control d'accés.

La versió 6.4.0.17 corregeix una vulnerabilitat crítica [CVE-2023-20048] detectada en la versió 6.4 inicialment qualificada.

Observacions

CCN-STIC-651B Seguretat a Cortafocs Cisco Firepower

NGIPSv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S- M3 and UCS-E18	
Versió	6.4
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	01/11/2022
Revisió de Validesa	30/04/2025
Descripció	

Sistema de Detecció i Prevenció d'Intrusions, que consisteix en una FMC i se

La FMC proporciona una consola de gestió centralitzada i un sistema de base de dades d'esdeveniments, agrega i correlaciona dades d'intrusió, descobriment i connexió, recollides dels sensors gestionats.

Els sensors monitoritzen tot el trànsit de la xarxa a la recerca d'esdeveniments de seguretat i violacions i poden alertar o fins i tot bloquejar trànsit maliciós d'acord amb les regles definides per al control d'accés.

Observacions

CCN-STIC-651B Seguretat a Cortafocs Cisco Firepower

Cisco FTD (NGFW) 6.4 en Firepower Series 4100 i 9300 con FMC/FMCv	
Versió	6.4
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	01/11/2022
Revisió de Validesa	30/04/2025
Descripció	

Els equips de seguretat Cisco Firepower 4100 i 9300 són plataformes escalables i fetes a propòsit amb capacitats de Firewall proporcionades pel Software Firepower Threat Defense (FTD) que corre en el sistema operatiu FXOS.

Observacions

CCN-STIC-651B Seguretat a Cortafocs Cisco Firepower

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

Versió	7.0
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Compatible amb:

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 i FMC4600-K9)
- FMCv executant-se en ESXi 6.0 o 6.5 en el Sistema Unificat de Computació (UCS) UCSB-B200-M4, UCSC-C220- M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S- M3 i UCS-E180D-M3

Observacions

CCN-STIC 651B Seguretat a Cortafocs Cisco Firepower

FTD Virtual (FTDv) sobri NFVIS 4.4 en ENCS 5406, 5408, i 5412

Versió	FTDv 7.0 y FMC/FMCv 7.0
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2024

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Compatible amb:

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 i FMC4600-K9)
- FMCv executant-se en ESXi 6.0 o 6.5 en el Sistema Unificat de Computació (UCS) UCSB-B200-M4, UCSC-C220- M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S- M3 i UCS-E180D-M3

Observacions

Pendent de Publicació de Procediment d'ocupació assegurança

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

Versió	FTD 7.0, FXOS 2.10 y FMC/FMCv 7.0
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Compatible amb:

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 i FMC4600-K9)
- FMCv executant-se en ESXi 6.0 o 6.5 en el Sistema Unificat de Computació (UCS) UCSB-B200-M4, UCSC-C220- M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S- M3 i UCS-E180D-M3

Observacions

CCN-STIC 651B Seguretat a Cortafocs Cisco Firepower

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

Versió	FTD 7.0 i FMC 7.0
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2026
Descripció	

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Compatible amb:

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 i FMC4600-K9)
- FMCv executant-se en ESXi 6.0 o 6.5 en el Sistema Unificat de Computació (UCS) UCSB-B200-M4, UCSC-C220- M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S- M3 i UCS-E180D-M3

Observacions

CCN-STIC 651B Seguretat a Cortafocs Cisco Firepower

SonicWall SOHO Serie (250, 250W)

Versió	6.5.4.4-44n-federal-12n
Fabricant	SonicWall
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	01/08/2021
Revisió de Validesa	28/02/2025
Descripció	

Els tallafocs de la Serie TZ SOHO de Sonicwall són una solució adequada per a oficines petites i domèstiques, així com per a entorns distribuïts en ubicacions remotes. Despleguen funcionalitats per construir Secure SD-WAN i connectivitat WIFI (opcional). El SOHO 250 proporciona un 50% més de rendiment sobre el seu antecessor SOHO, així com accés als sandboxes avançats Capture ATP, amb la qual cosa es millora la seguretat en prevenció i detecció de malware desconegut en un entorn remot.

Observacions

CCN-STIC-1420 Procediment d'Ocupació Segur Sonicwall SonicOS

7.4.2. CAPTURA, MONITORATGE I ANÀLISI DE TRÀNSIT

CloudWatch

Versió

Fabricant AWS

Família Captura, Monitoratge i Anàlisi de Trànsit

Tipus Producte

Data Inclusió 01/07/2022

Revisió de Validesa 30/06/2024

Descripció

Amazon CloudWatch és un servei de monitoratge i administració creat per a desenvolupadors, operadors de sistemes, enginyers de fiabilitat (SRE), i administradors d'IT. CloudWatch proporciona dades i coneixements pràctics per monitoritzar les seves aplicacions, comprendre i respondre als canvis d'acompliment de tot el sistema, optimitzar la utilització dels recursos i obtenir una visió unificada de l'estat operatiu. Amazon CloudWatch recopila dades operatives i de monitoratge en forma de registres, mètriques i esdeveniments, proporcionant-li una visió unificada dels recursos d'AWS, les aplicacions i els serveis que s'executen en AWS i els servidors on-premise.

Pot utilitzar CloudWatch per establir alarmes d'alta resolució, visualitzar els registres i les mètriques de forma paral·, realitzar accions automatitzades, solucionar problemes i descobrir informació per optimitzar les seves aplicacions i assegurar-se que funcionen correctament.

Per a més informació sobre Amazon CloudWatch, per favor visiteu https://aws.amazon.com/es/cloudwatch/

https://docs.aws.amazon.com/whitepapers/latest/aws-overview/managementgovernance.html#amazon-cloudwatch

Observacions

CCN-STIC-887A Guía de configuración segura AWS

CARMEN

Versió Versió 7.16.2

Fabricant S2 GRUPO / CCN

Família Captura, Monitoratge i Anàlisi de Trànsit

Tipus Producte

Data Inclusió 01/04/2021

Revisió de Validesa 30/06/2024

Descripció

CARMEN (Centre d'Anàlisi de Registres i Mineria d'EveNtos) és una solució uisició, processament i anàlisi d'informació per suportar el procés d'identificació d'Amenaces Persistents Avançades (APT) a partir del trànsit de xarxa intern i sortint d'una forma eficient, donant suport a la presa de decisions a partir de la informació generada i processada. Es compon d'agents que recopilen els fluxos de trànsit, un motor d'emmagatzematge en el qual s'insereix la informació, un sistema de detecció d'anomalies que s'encarrega de processar la informació emmagatzemada i una aplicació web que permet la representació i consulta tant de la informació obtinguda com de la processada. Per a més informació, es pot consultar el web del CCN-CERT (https://ccn- cert.cni.es/soluciones-seguridad/carmen.html)

Observacions

CCN-STIC-1304 Procediment d'ocupació assegurança CARMEN

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

Versió 6.1

Fabricant Gigamon

Família Captura, Monitoratge i Anàlisi de Trànsit

Tipus Producte

Data Inclusió 28/06/2023

Revisió de Validesa 30/06/2024

Descripció

Network Packet Brokers HC Series. Network Packet Brokers d'alt rendiment amb suport de ports 1g/10g/25g/40g/100g en fibra multimode o/i monomode i 100m/1g/10g en coure i funcionalitats de filtratge de tràfic L2-3-4-7 amb motor de DPI, generació de Netflow/IPFix/Metadatos, Xifrat/Desxifrat de SSL/TLS (incloent-hi protocols RSA, DHE, ECC, i PFS), Terminació de túnels (GRE, VXLAN, ERSPAN, GMIP), Truncat de paquets, Eliminació de capçaleres, Emmascarat, De-Duplicació, Clustering, Balanceig, Captura de trànsit per a entorns virtuals (VMWare ESX/NSX, Openstack, Kubernetes, AWS, GCP, Azure, Nutanix), simetrització de trànsit per a arquitectura HA, Inline Bypass amb Heartbeat positiu i negatiu, Canvi de mitjà i velocitat, Bypass HW, TAPs integrats.

Observacions

CCN-STIC-1301 Procediment d'Ocupació Segur GigaVUE-OS

GigaVUE (GVS-TAX21-HW, GVS-TAX22-HW, GVS-TAX21A-HW, GVS-TAX22A-HW, GVS-TAC21, GVS-TAC22, GTP-ATX21, GTP-ASF21)	
Versió	6.1
Fabricant	Gigamon
Família	Captura, Monitoratge i Anàlisi de Trànsit
Tipus	Producte
Data Inclusió	28/06/2023
Revisió de Validesa	30/06/2024
Descripció	

Network Packet Brokers HC Series. Network Packet Brokers d'alt rendiment amb suport de ports 1g/10g/25g/40g/100g en fibra multimode o/i monomode i 100m/1g/10g en coure i funcionalitats de filtratge de tràfic L2-3-4-7 amb motor de DPI, generació de Netflow/IPFix/Metadatos, Xifrat/Desxifrat de SSL/TLS (incloent-hi protocols RSA, DHE, ECC, i PFS), Terminació de túnels (GRE, VXLAN, ERSPAN, GMIP), Truncat de paquets, Eliminació de capçaleres, Emmascarat, De-Duplicació, Clustering, Balanceig, Captura de trànsit per a entorns virtuals (VMWare ESX/NSX, Openstack, Kubernetes, AWS, GCP, Azure, Nutanix), simetrització de trànsit per a arquitectura HA, Inline Bypass amb Heartbeat positiu i negatiu, Canvi de mitjà i velocitat, Bypass HW, TAPs integrats.

Observacions

CCN-STIC-1301 Procediment d'Ocupació Segur GigaVUE-OS

7.4.3. EINES DE SANDBOX

8.	Deep Discovery Inspector
Versió	6.5.1129
Fabricant	Trend Micro
Família	Eines de Sandbox
Tipus	Producte
Data Inclusió	N/A
Revisió de Validesa	16/05/2024
Descripció	

Deep Discovery Inspector és una sonda de xarxa anti-APT dissenyada per detectar de manera primerenca ciberatacs al vector de xarxa (ex.: malware de dia 0, moviments laterals, comunicacions C&C, exfiltració de dades, explotació de vulnerabilitats, etc.). Combinant tècniques de Reputació, Machine Learning i Sandboxing.

Disponible en format appliance físic o virtual, amb diferents nivells d'escalat d'amplada de banda i configuració de ports, facilita la seva implementació en xarxes amb diferents nivells de complexitat. Integrada amb la plataforma XDR Trend Vision One, on aporta telemetria i deteccions, conforma la plataforma NDR perfecta per fer front als complexos atacs rebuts pel cibercrim modern.

Observacions

CCN-STIC 1227 Procedimiento de Empleo Seguro Deep Discovery Inspector

7.5. PROTECCIÓ DE LES COMUNICACIONS

7.5.1. ENRUTADORS

Dell EMC Networking SmartFabric OS10.5.4en Switches de les series N, S i Z (N3248TE, S41xx, S52xx, S54xx, Z91xx, Z92xx, Z93xx, Z94xx, Z96xx)	
Versió	OS10.5.4
Fabricant	DELL COMPUTER, S.A.
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/10/2023
Revisió de Validesa	31/03/2026

Descripció

Dell EMC Smart Fabric OS10 és el sistema operatiu de xarxa (NOS) que s'utilitza en les famílies d'enrutadors i commutadors de les Serie N (alguns models), Serie S, Serie Z i Serie MX de Dell EMC Networking (les plataformes HW que actualment suporten OS10 són N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n i MX9116n). Dell EMC SmartFabric OS10 és un sistema operatiu de xarxa (NOS) que admet múltiples arquitectures i entorns. La solució SmartFabric OS10 permet la desagregació en diverses capes de la funcionalitat de xarxa. SmartFabric OS10 comprèn l'administració, monitoratge i funcionalitat completa i estàndard de la indústria de xarxes de nivell 2 i nivell 3 a través de CLI, SNMP i REST. Els usuaris poden triar les seves pròpies aplicacions d'organització, gestió, supervisió i xarxes de tercers. Per desenvolupar xarxes escalables L2 i L3, SmartFabric OS10 ofereix una solució modular i desagregada en una única imatge binària.

Observacions

CCN-STIC-1429 PES DELL EMC Networking

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

Versió	SAR OS v6.1
Fabricant	NOKIA
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	30/06/2025

Descripció

La família d'encaminadors d'agregació de serveis 7705 SAR de Nokia, ofereix capacitats IP/MPLS i interfícies legacy (sèrie i TDM) líders en la indústria. A més proporciona plataformes compactes amb la capacitat de preparar i agregar de manera fiable i eficient múltiples continguts a través de diferents protocols de transport. La gamma 7705 SAR de Nokia està optimitzada per a l'adaptació, agregació i encaminament multiservei, especialment en modernes infraestructures Ethernet i IP/MPLS. Gràcies al "Service Encaminador Operating System (SR US)", i a la capacitat de gestió de xarxa que aporta la solució de "Network Service Platform (NSP)", tots dos productes de Nokia, els encaminadors ofereixen serveis d'alta disponibilitat a través de topologies de xarxa flexibles i resistents estant disponible en plataformes compactes i de baix consum d'energia. La família 7705 SAR resulta adequada tant per a l'agregació del trànsit de xarxa com per a la implementació del "backhaul" de l'accés radio 3G, LTE i 5G i la connexió d'aquests serveis a xarxes IP/MPLS.

EL 7705 SAR de Nokia proporciona una fàcil integració dels dispositius TDM a les xarxes IP/MPLS. Lafamília de 7705 SAR ofereix un ampli conjunt d'interfícies incloent OC-12/STM-4, OC-3/ STM-1, T1/E1, serveis de Teleprotecció C37.94 de sistemes elèctrics així com interfícies de veu per a telefonia analògica, juntament amb característiques de programari per a retard asimètric i compensació per fluctuació. Aquestes interfícies i les seves característiques garanteixen que les aplicacions incorporades des d'aquests dispositius funcionin exactament com ho fan en les xarxes TDM.

Per a garantir el rendiment de les aplicacions de missió crítica, el trànsit s'accelera quan s'utilitza qualsevol de les diferents velocitats Ethernet o enllaços TDM de baixa amplada de banda. Les característiques de migració d'aquest encaminador permeten als operadors de xarxa migrin de manera eficient aplicacions a l'entorn IP/MPLS.

Observacions

Procediment d'ocupació pendent de publicació.

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

Versió	IOS-XE 17.9 (amb 17.9.4a)
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	13/11/2023
Revisió de Validesa	30/04/2026

Descripció

Els Cisco Catalyst 9400 9500 i 9600 són equips de xarxa d'alt rendiment. Ofereixen alta densitat de ports Ethernet per mòdul, amb opcions de 10 Gbps, 25 Gbps i 40 Gbps. Estan equipats amb un processador que proporciona una alta capacitat de processament i seguretat avançada.

Observacions

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

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

Versió	IOS-XE 17.9 (con fix 17.9.a)
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	14/11/2023
Revisió de Validesa	30/04/2026

Descripció

Els equips Cisco Catalyst 9200 i 9200L són switches d'alt rendiment i seguretat reforçada, ideals per a empreses que requereixen solucions de xarxa segures i escalables. Amb models que varien des de 24 fins a 48 ports, proporciona una gran flexibilitat per adaptar-se a qualsevol mida de xarxa. Ofereixen gestió avançada i detecció d'amenaces millorada.

Els Cisco Catalyst 9200L són la variant de la Serie 9200, mantenint les mateixes característiques de seguretat i rendiment. Són ideals per a petites i mitjanes empreses que busquen una xarxa segura i escalable.

Observacions

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

RUCKUS FastIron series ICX8200, ICX7550 e ICX7850 Switch/Router

Versió	10.0.10c
Fabricant	CommScope Technologies
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	31/12/2026

Descripció

La família RUCKUS ICX de commutadors de nivell 2 i 3 disposa d'una gamma de models tant per a campus i xarxes empresarials de 2 i 3 nivells com per a Data Center, cobrint tot el rang de velocitats de port des de 1G fins a 100G.

Inclou tecnologies com Stacking a tala i llarga distància, fonts d'alimentació redundants, nivell 3 avançat, protocols d'alta disponibilitat, microsegmentació i automatització, entre altres.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

Junos OS 22.4R1 MX304

Versió	22.2R1
Fabricant	Juniper Networks
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2024

Descripció

Les plataformes d'encaminament universal MX304 brinden un rendiment de gran escalabilitat en un factor de forma optimitzat per al núvol i les economies de cost per port o bit més exigents. Es poden utilitzar tant en xarxes de tipus operador, com a node de vora en xarxes MPLS, en entorns de mobilitat convergent, IoT, empresarial i també en arquitectures de Core convergent i de bord multiservei. També suporta l'ús com a encaminador de commutació d'etiquetes (LSR), provider Edge, equip d'intercanvi d'Internet i xarxa troncal per a implementacions en xarxes de caràcter metropolitanes, regionals o nacionals, o terminador de túnels IPSEC o Firewall de capa 4. La sèrie MX admet un ampli conjunt de funcionalitats IPoDWDM, L2, L3, IP/MPLS, SR, SRv6, o terminador de túnels IPSEC per a permetre xarxes de transport a gran escala amb operacions i aprovisionament de serveis simplificats, mantenint simplicitat en la xarxa. Gràcies al tipus de chipsets implementats, tenen una capacitat de programació en el pla de dades gairebé infinita, la qual cosa li brinda la llibertat d'implementar noves innovacions de xarxa. Amb tecnologia de silici TRIO, la família MX304 és altament escalable des dels 1.6Tbps, passant per 3.2 Tbps fins als 4.8 Tbps en 2U depenent del número de slots utilitzats.

Observacions

Procediment d'ocupació assegurança pendent de publicació

ACX5448-M

Versió	Junos OS 22.3R1
Fabricant	Juniper Networks
Família	Enrutadors
Tipus	Producte
Data Inclusió	07/05/2024
Revisió de Validesa	31/10/2024

Descripció

La línia Juniper Networks® ACX5000 sorgeix com a resposta a un canvi en les arquitectures de xarxes metropolitanes on les capes d'accés i agregació estan estenent la intel·ligència operativa des de l'extrem del proveïdor de serveis fins a la xarxa d'accés. La línia ACX5000 simplifica les arquitectures d'accés i agregació en eliminar capes innecessàries i superposicions de xarxa, la qual cosa redueix dràsticament CapEx i OpEx. Està basada en la simplificació de l'arquitectura i en la reducció de costos, la línia ACX5000 brinda als proveïdors de serveis i empreses la capacitat d'adoptar un veritable paradigma de metre universal.

Així mateix, proporciona alta capacitat, escalabilitat i una capa de transport òptic de paquets, al mateix temps que ofereix un rendiment líder en la indústria amb una àmplia gamma de densitats de ports i tipus d'interfície.

La sèrie ACX presenta el lideratge IP/MPLS de Juniper des del core i el perímetre de la xarxa fins a les capes d'accés. La sèrie ACX admet un ampli conjunt de funcionalitats L2, L3 i IP/MPLS per a permetre xarxes MPLS transparents a gran escala amb operacions i aprovisionament de serveis simplificats mantenint simplicitat en la xarxa.

ACX5448-M: L'ACX5448-M té 44 ports 1GbE/10GbE i 6 ports 40GbE/100GbE, així com capacitats de seguretat avançades com such as Mitjana Access Control Security (MACsec) on all 1GbE/10GbE ports.

Observacions

CCN-STIC-1445 PES Router_Juniper_ACX5448-M_JunOS 20.3R1

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

Versió	09.0.10
Fabricant	CommScope Technologies
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	30/09/2025

Descripció

La família RUCKUS ICX de commutadors de nivell 2 i 3 disposa d'una gamma de models tant per a campus i xarxes empresarials de 2 i 3 nivells com per a Data Center, cobrint tot el rang de velocitats de port des de 1G fins a 100G.

Inclou tecnologies com Stacking a tala i llarga distància, fonts d'alimentació redundants, nivell 3 avançat, protocols d'alta disponibilitat, microsegmentació i automatització, entre altres.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

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

Versió	IOS-XE 17.6
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	07/03/2024
Revisió de Validesa	31/08/2024

Descripció

Els encaminadors Cisco Catalyst 8200 i 8500 Sèries són part de la cartera de solucions de Cisco per a xarxes de vores de l'empresa, dissenyats per a oferir una connectivitat segura i d'alt rendiment per a sucursals i serveis de xarxa en el núvol. Aquests encaminadors estan especialment dissenyats per a suportar la creixent demanda d'aplicacions en el núvol, mobilitat i augment en el trànsit de dades. Totes dues sèries s'integren sense problemes amb l'arquitectura de xarxa de Cisco, oferint una gestió simplificada i una operativitat millorada a través d'eines com Cisco SD-WAN i Cisco DNA Center, permetent a les organitzacions modernitzar la seva infraestructura de xarxa i optimitzar l'experiència d'usuari final.

La sèrie 8200 és ideal per a sucursals mitjanes a grans, oferint una plataforma optimitzada per a la integració de serveis de xarxa, seguretat avançada i capacitats d'encaminament flexibles. Amb opcions de rendiment modular, aquests encaminadors permeten a les empreses escalar segons les seves necessitats específiques.

Per part seva, la sèrie 8500 està orientada a entorns empresarials d'alta densitat i centres de dades, proporcionant una solució robusta per a l'encaminament de vores amb capacitats d'agregació. Aquests encaminadors d'alt rendiment són adequats per a aplicacions intensives en amplada de banda i per a manejar grans volums de trànsit de dades amb una seguretat integrada de grau empresarial.

Observacions

Procediment d'Ocupació Segura pendent de publicació

NE40E 8000 Series Routers running VRP software

Versió V800R012C00SPC300

Fabricant Huawei Technologies Espanya

Família Enrutadors

Tipus Producte

Data Inclusió 01/07/2022

Revisió de Validesa 31/12/2024

Descripció

Els routers NE40E i NetEngine 8000 equipats amb els xipsets NP i la plataforma VRP compleixen amb els requisits de baixa latència i alta fiabilitat tant dels serveis crítics per al negoci com de les solucions SDN-WAN avançades. Funcionen com a nodes core WAN, nodes d'accés en xarxes de gran escala, nodes d'agregació i interconnexió en xarxes de campus i nodes edge en xarxes IDC de gran escala, oferint un elevat rendiment (fins a 14.4 tbit/s per stolt), alta fiabilitat, baix consum energètic i una densitat de ports per sobre de la mitjana. Amb un disseny compacte, dissipació de la calor optimitzada i un consum energètic molt baix, permet construir xarxes ultra-broadband simplificades i convergents.

Observacions

CCN-STIC-1419 Procediment d'ocupació assegurança Routers Huawei NE40E Series

RouterTeldat-M1 Series

Versió	11.01.09
Fabricant	TELDAT, S.A.
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/05/2023
Revisió de Validesa	31/10/2025

Descripció

Es tracta d'una família de routers compactes orientats a oficines petites i mitjanes, però que requereixen connexió d'alta velocitat. El seu disseny compacte i sense ventiladors, per no generar soroll, permeten instal·lar-lo en àrees de treball, una cosa molt útil en petites oficines, botigues o despatxos professionals. A més, en aquests entorns aquesta família de routers afavoreix l'ús de connexions 3G/4G per la disponibilitat més gran de cobertura que en instal·lacions realitzades en sales o armaris tècnics. Tot i ser routers compactes, alguns models poden assolir velocitats de fins a 600 Mbps simètrics, i són molt escalables gràcies a un slot i una àmplia varietat de targetes. Integren connectivitat Ethernet WAN i commutador Ethernet de 4 ports LAN, a més d'un punt d'accés Wi-Fi i connectivitat 3G/4G. A més d'un sofisticat maquinari, inclouen un avançat Software adaptat a xarxes professionals que inclou totes les funcionalitats demandades a un router professional com routing (RIP, OSPF, BGP, VRF, PolicyRouting,...), seguretat (ACLs, Firewall, IPSec, 802.1X, ...), qualitat de servei (CBWFQ, PQ, perfilat, ...), o gestió (CLI, SNMPv3, RADIUS, TACACS+, Syslog, Netflow, Mirroring,...).

Observacions

CCN-STIC-1455 Procediment d'ocupació assegurança Teldat M1 Series

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

Versió	IOS-XE 16.9
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/11/2022
Revisió de Validesa	30/04/2025

Descripció

Les famílies ASR900 i NCS4200 són equips fets a propòsit com plataformes de routing, suportant addicionalment xifrat MACsec.

Observacions

CCN-STIC 1454 Procediment d'Ocupació Assegurança Routers CISCO ASR9000 i NCS4200 Series

ASR1000 (ASR1001-X, ASR1001-HX, ASR1002-HX, ASR1006-X, ASR1009-X, ASR1013, MACsec EPAs: ASR1000-MIP100, 18X1GE, 10X10GE, 1X100GE, CPAK-2X40GE, 1X100GE QSFP +, 2X40GE QSFP +, 1X40GE QSFP +)	
Versió	IOS-XE 17.3 (amb 17.3.8a)
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/06/2022
Revisió de Validesa	30/11/2024

Descripció

Els routers de Cisco permeten el seu desplegament en xarxes WAN, LAN i el núvol. Proporcionen una solució completa i provada a través d'anàlisis avançades, optimització d'aplicacions, aprovisionament automatitzat i seguretat integrada.

Observacions

CCN-STIC-1461 PES Cisco ISR 4000 Series - ASR 1000 Series - Catalyst 8300-8500 running IOS-XE 17

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

Versió	SR OSv12.0
Fabricant	NOKIA
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	01/01/2024

Descripció

La plataforma d'encaminament Core 7950 XRS de Nokia proporciona l'escalabilitat, l'eficiència i la versatilitat necessàries a les demandes de servei impulsades pel núvol, el 5G i la Internet de les coses. El 7950 XRS s'ha implementat per operadors de telecomunicacions, cable, mòbils, serveis públics i xarxes privades de qualsevol grandària, així com pels principals operadors d'escala web i proveïdors d'intercanvi d'Internet.

El disseny de maquinari modular i extensible impulsat pel microprocessador de silici d'encaminament FP4 de Nokia garanteix un escalat granular i econòmic de la capacitat de commutació i la densitat de ports amb un rendiment de reexpedició determinista. Un sol xassís 7950 XRS-20e equipat amb maquinari FP4 ofereix una capacitat de commutació dúplex completa de fins a 48 Tb/s i admet densitats de ports de fins a 160 ports d'interfície 400GE, 800 100GE o 4800 10GE.

La família 7750 Service Encaminador (SR) de Nokia ofereix encaminadors de bord multiservei d'alt rendiment dissenyats per al suport simultani de serveis avançats d'usuari final, empresarials i mòbils en una plataforma de borda IP comuna.

La família d'encaminadors 7750 SR permet la creació d'una àmplia gamma de serveis IP disponibles per a les grans empreses i operadors amb requisits excepcionals de rendiment, escalabilitat i intel·ligència de servei. La família 7750 SR utilitza el Sistema Operatiu de l'encaminador de serveis de Nokia (SR US) i suporta la gestió dels serveis per a millorar l'eficiència operativa.

La família 7750 SR disposa de la capacitat de servei per a admetre múltiples aplicacions i funcions en una plataforma comuna. L'innovador disseny de refrigeració tèrmica “front-to-back” compatible amb NEBS dels 7750 SR base per a un creixement futur. La família 7750 SR-e ofereix densitat Gigabit Ethernet (GE) d'alta densitat i 10GE,100GE i 400GE per a la distribució de 10GE i 100GE en xarxes d'accés i agregació.

Observacions

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

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

Versió	10.11
Fabricant	HPE Aruba Networking
Família	Enrutadors
Tipus	Producte
Data Inclusió	20/03/2024
Revisió de Validesa	31/08/2024

Descripció

La família Aruba CX implementen solucions de switching i routing per a xarxes de sucursals, campus i datacenter. Els equips 10000, 8320, 8325, 8360, i 8400 són idonis per a Datacenter i equips nucli (core) de la xarxa de campus. Els equips 6400 es posicionen com a equips nucli (core) de la xarxa de campus, mentre els 6300 i 6200 estan orientats per a xarxes d'accés. Implementen funcionalitats multicapa, implementen múltiples mecanismes de seguretat en l'accés i administració. Orientat a la segmentació dinàmica i a implementar entorns Zero Trust. Permet el desplegament automàtic desatès (ZTP) Aruba CX disposa d'una arquitectura interna de Sistema Operatiu que proporciona una manera de treballar amb el completament programable. El seu motor d'analítiques (NAE) permet la inserció de scripts de per a l'execució de tasques avançades de monitoratge i respostes a esdeveniments.Els equips 4100i són equips amb protecció mediambientals i de format industrial.

Observacions

Procediment d'Ocupació Segura pendent de publicació

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	10/04/2025

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	IOS-XE 17.9 (amb 17.9.4a)
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	14/11/2023
Revisió de Validesa	30/04/2026

Descripció

Els Cisco Catalyst 9300y 9300L són switches de xarxa que ofereixen una alta densitat ports Ethernet per mòdul, incloent opcions de PoE+. Estan dissenyats amb un potent processador i ofereixen serveis de xarxa avançats per a empreses que necessiten una xarxa segura i escalable. Els Cisco Catalyst 9300L, la variant compacta de la Serie 9300, ideals per a petites i mitjanes empreses.

Observacions

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

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

Versió	22.2R1
Fabricant	Juniper Networks
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/02/2024
Revisió de Validesa	31/07/2024

Descripció

Les plataformes d'encaminament universal MX240/MX480/MX960 brinden un rendiment de gran escalabilitat en un factor de forma optimitzat per al núvol i les economies de cost per port o bit més exigents. Es poden utilitzar tant en xarxes de tipus operador, com a node de vora en xarxes MPLS, en entorns de mobilitat convergent, IoT, empresarial i també en arquitectures de Core convergent i de bord multiservei. També suporta l'ús com a encaminador de commutació d'etiquetes (LSR), provider Edge, equip d'intercanvi d'Internet i xarxa troncal per a implementacions en xarxes de caràcter metropolitanes, regionals o nacionals, o terminador de túnels IPSEC o Firewall de capa 4. La sèrie MX admet un ampli conjunt de funcionalitats IPoDWDM, L2, L3, IP/MPLS, SR, SRv6, erminador de túnels IPSEC o CGNAT per a permetre xarxes de transport a gran escala amb operacions i aprovisionament de serveis simplificats, mantenint simplicitat en la xarxa. Gràcies al tipus de chipsets implementats, tenen una capacitat de programació en el pla de dades gairebé infinita, la qual cosa li brinda la llibertat d'implementar noves innovacions de xarxa. Amb tecnologia de silici TRIO, la família MX és altament escalable des dels 3Tbps en 3U, passant per 38,4 Tbps en 5 slots i fins a un rendiment de 12 Tbps en 16 slots.

Observacions

Procediment d'ocupació segura pendent de publicació

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

Versió	ArubaOS 16.08
Fabricant	Aruba
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/12/2021
Revisió de Validesa	31/05/2024

Descripció

Equips dissenyats per utilitzar-se en tasques d'accés i agregació, o nucli de xarxa d'accés. Són equips que proporcionen connexions de totes les velocitats i tipus de mitjans. Equips amb capacitat de commutació sense bloqueig (non-blocking). Segons la família, ofereixen solucions escalables mitjançant constitució de stacks via port de xarxa, port dedicat així com existeixen models de xassís. Totes les funcions del sistema operatiu s'ofereixen amb l'equip. Ofereixen diversos tipus d'interfícies i velocitats. Ofereixen PoE en alguns models, a diferents potències.

Poden ser gestionables, tan localment (gestió on-premise) com poden arribar a administrar-se en modalitat Software-as-a-Service

Observacions

CCN-STIC-647C Seguretat en commutadors HPE Aruba

MX10003

Versió Junos OS 22.2R1

Fabricant Juniper Networks

Família Enrutadors

Tipus Producte

Data Inclusió 01/08/2023

Revisió de Validesa 31/01/2026

Descripció

Les plataformes d'enrutament universal MX10000 brinden un rendiment de gran escalabilitat i un factor de forma optimitzat per al núvol i les economies de cost per port o bit més exigents. Es poden utilitzar tant en xarxes de tipus operador com node de vora PE en una xarxa MPLS, com en entorns de mobilitat convergent, IoT, empresarial i també en arquitectures de Core convergent i de vora multiservei. També suporta l'ús com a enrutador de commutació d'etiquetes (LSR), provider Edge, equip d'intercanvi d'Internet i xarxa troncal per a implementacions en xarxes de caràcter metropolitanes, regionals o nacionals. La Serie MX admet un ampli conjunt de funcionalitats IPoDWDM, L2, L3, IP/MPLS, SR, SRv6 per permetre xarxes de transport a gran escala amb operacions i aprovisionament de serveis simplificats, mantenint simplicitat a la xarxa. Gràcies al tipus de xipsets implementats, tenen una capacitat de programació de pla de dades gairebé infinita, cosa que li brinda la llibertat d'implementar noves innovacions de xarxa.

Amb tecnologia de silici TRIO, la família MX10000 és altament escalable des dels 2.4Tbps en 3U, passant per 38,4 Tbps en 7 slots i fins a un rendiment de 76,8 Tbps en 13 slots.

Observacions

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

Cisco Catalyst 9500 Series Switches (C9500-12Q|24Q|40X|16X|32C|32QC|24Y4C|48Y4C) amb els següents mòduls de xarxa (C9500-NM-8X i C9500-NM-2Q)

Versió IOS-XE 17.9 (amb 17.9.4a)

Fabricant Cisco Systems

Família Enrutadors

Tipus Producte

Data Inclusió 13/11/2023

Revisió de Validesa 30/04/2026

Descripció

Els Cisco Catalyst 9400 9500 i 9600 són equips de xarxa d'alt rendiment. Ofereixen alta densitat de ports Ethernet per mòdul, amb opcions de 10 Gbps, 25 Gbps i 40 Gbps. Estan equipats amb un processador que proporciona una alta capacitat de processament i seguretat avançada.

Observacions

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

Cisco Catalyst 9200 Series Switches (C9200-24T, C9200-48T, C9200-24P, C9200-48P, C9200-24PB, C9200-48PB, C9200-48PL, C9200-24PXG, C9200-48PXG) amb els mòduls de xarxa (C9200-NM 4G|4X|2Y|2Q)	
Versió	IOS-XE 17.9 (con fix 17.9.a)
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	14/11/2023
Revisió de Validesa	30/04/2024
Descripció	

Els equips Cisco Catalyst 9200 i 9200L són switches d'alt rendiment i seguretat reforçada, ideals per a empreses que requereixen solucions de xarxa segures i escalables. Amb models que varien des de 24 fins a 48 ports, proporciona una gran flexibilitat per adaptar-se a qualsevol mida de xarxa. Ofereixen gestió avançada i detecció d'amenaces millorada.

Observacions

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

Cisco Catalyst 9400 Series Switches (C9404R, C9407R, C9410R, C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y, C9400-LC-24S|48S|24XS|48P|48T|48U|48UX|48H)	
Versió	IOS-XE 17.9 (amb 17.9.4a)
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	13/11/2023
Revisió de Validesa	30/04/2024
Descripció	

Els Cisco Catalyst 9400, 9500 i 9600 són equips de xarxa d'alt rendiment. Ofereixen alta densitat de ports Ethernet per mòdul, amb opcions de 10 Gbps, 25 Gbps i 40 Gbps. Estan equipats amb un processador que proporciona una alta capacitat de processament i seguretat avançada.

Observacions

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

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

Versió	V300R006C10SPC300
Fabricant	Huawei Technologies Espanña
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/10/2022
Revisió de Validesa	31/03/2025

Descripció

La Serie ATN 980C, 950D, 910C-G i 910D-A de Huawei són routers d'accés multiservei que s'han introduït en la transició a LTE i a la cobertura FMC dels operadors.

L'objectiu de la Serie ATN de Huawei és oferir solucions de xarxa de portadores d'IP de gamma alta. Ofereix característiques riques de segona i tercera capa i compta amb comoditats com el manteniment i l'administració remots, l'absència de posada en marxa in situ i la funcionalitat plug-and-play.

La Serie ATN és compatible amb l'accés virtual SDN i està pensada per satisfer les necessitats de la capa d'accés, els dispositius de desplegament a gran escala i l'accés a serveis integrats. En ser un router d'accés multiservei compacte de 2U d'alçada i 10GE, pot compartir un armari amb l'estació base, amb una capacitat de commutació de fins a 56G i suportar un accés màxim de 8 10GE.

Observacions

CCN-STIC-1439 Procediment d'ocupació assegurança Enrutadors ATN de Huawei

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

Versió	V200R022C00SPC500
Fabricant	Huawei Technologies Espanya
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2024

Descripció

Els switches de la Serie-S de Huawei estan dissenyats per cobrir les necessitats d'evolució de la xarxa de campus. Entre les seves capacitats destaquen la gestió simplificada i l'alt rendiment. Poden ser utilitzats en qualsevol tipus de sector: empresarial, governamental, educatiu, financer o industrial.

Observacions

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

Huawei S Series Ethernet Switches S5735S (H24S4XC-A, L12P4S-A, L12T4S-A, L24FT4S-A, L24P4S-A, L24P4S-A1, L24P4S-MA, L24P4X-A, L24P4X-A1, L24T4S-A, L24T4S-A1, L24T4S-MA, L24T4X-A, L24T4X-A1, L32ST4X-A, L32ST4X-A1, L48FT4S-A, L48P4S-A, L48P4S-A1, L48P4X-A, L48P4X-A1, L48T4S-A, L48T4S-A1, L48T4S-MA, L48T4X-A, L48T4X-A1, L8P4S-A1, L8T4S-A1, S24P4X-A, S24T4S-A, S24T4X-A, S32ST4X-A, S48P4X-A, S48T4S-A, S48T4X-A)	
Versió	V200R022C00SPC500
Fabricant	Huawei Technologies Espanya
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2026
Descripció	

Els switches de la Serie-S de Huawei estan dissenyats per cobrir les necessitats d'evolució de la xarxa de campus. Entre les seves capacitats destaquen la gestió simplificada i l'alt rendiment. Poden ser utilitzats en qualsevol tipus de sector: empresarial, governamental, educatiu, financer o industrial.

Observacions

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

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

Versió	Junos OS 22.2R1
Fabricant	Juniper Networks
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2024

Descripció

La família de switches EX4400, en les seves diferents variants, són dispositius de xarxa segurs amb alta densitat de ports 10/100/1000Base-T, 100/1000/2500/5000/10000Base-T, així com uplinks 1/10/25GbE o 40/100GbE o variants amb tots els seus ports en fibra. Totes les plataformes EX4400 funcionen amb el programari Junos US, que és un sistema operatiu especialment dissenyat per a aquesta mena de dispositius. Junos US Proporciona funcions de gestió, control i monitoratge, així com tota la provisió de canvis en els dispositius.

Els switches EX4400 són dispositius de xarxa que suporten la definició, i compliment, de polítiques de flux d'informació entre els nodes de la xarxa. Al costat de funcions de seguretat del trànsit d'informació, el producte registra totes les activitats rellevants, i compta amb eines de seguretat per a la gestió segura.

Com switch de nivell 2 en la capa OSI, realitza l'anàlisi de paquets entrants, reexpedint aquests paquets en funció de la informació que contenen, fent-los arribar així al seu destinatari. Com switch de nivell 3 en la capa OSI, admet l'encaminament del trànsit, basat en taules, identificant les rutes disponibles, les condicions, la distància i els costos per a així determinar el camí més adequat per a cada paquet

Observacions

Procediments d'Ocupació Segura pendent de publicació.

Huawei AR6000&AR600 Series Routers (NetEngine AR6120, NetEngine AR6121,NetEngine AR6140-9G-2AC, NetEngine AR6140-16G-4XG. NetEngine AR6280, NetEngine AR6300, NetEngine AR651, NetEngine AR651C, NetEngine AR651W, NetEngine AR657W, NetEngine AR611W i NetEngine AR617VW-LTE4EA)			
Versió	V300R019C11SPC200	+	Patch
	V300R019C11HP0095T		
Fabricant	Huawei Technologies		
Espanya			
Família	Enrutadors		
Tipus	Producte		
Data Inclusió	01/01/2022		
Revisió de Validesa	30/06/2024		
Descripció			

Les plataformes d'enrutament Huawei AR són els primers dissenyats per a l'era de la cloud, presenta enllaços ascendents de banda ultra ampla 4G/5G i compta amb un rendiment de reenviament que és tres vegades la mitjana de la indústria. Oferint a més diverses característiques. Compatible amb la xarxa definida per Software (SD-WAN), la gestió del núvol, la xarxa privada virtual (VPN), la commutació d'etiquetes (MPLS), la seguretat i la veu.

Observacions

CCN-STIC-1437 Procediment d'ocupació segur Enrutadors Huawei AR6000&AR600

Huawei S Series Ethernet Switches S5731 (H24P4XC, H24T4XC, H48P4XC, H48T4XC, S24P4X, S24T4X, S48P4X, S48T4X, H24HB4XZ, H24P4XC-K, H24T4XC-K, H48HB4XZ, H48P4XC-K, H48T4XC-B, S24N4X2Q-A, S24T4X-A, S24T4X-D, S24UN4X2Q, S32ST4X, S32ST4X-A, S32ST4X-D, S48S4X, S48S4X-A, S48T4X-A) i S5731S (S8UM16UN2Q, H24HB4XZ-A, H24T4S-A, H24T4X-A, H24T4XC-A, H48HB4XZ-A, H48T4S-A, H48T4X-A, H48T4XC-A)	
Versió	V200R022C00SPC500
Fabricant	Huawei Technologies Espanya
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/12/2026
Descripció	

Els switches de la Serie-S de Huawei estan dissenyats per cobrir les necessitats 'evolució de la xarxa de campus. Entre les seves capacitats destaquen la gestió simplificada i l'alt rendiment. Poden ser utilitzats en qualsevol tipus de sector: empresarial, governamental, educatiu, financer o industrial.

Observacions

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

ISR4000 (ISR4321, ISR4331, ISR4351, ISR4431, ISR4451-X, ISR4461, NIMs: NIM-1GE-CU-SFP, NIM-2GE-CU-SFP)	
Versió	IOS-XE 17.3 (amb 17.3.8a)
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/06/2022
Revisió de Validesa	30/11/2024
Descripció	

Els routers de Cisco permeten el seu desplegament en xarxes WAN, LAN i el núvol. Proporcionen una solució completa i provada a través d'anàlisis avançades, optimització d'aplicacions, aprovisionament automatitzat i seguretat integrada.

Observacions

CCN-STIC-1461 PES Cisco ISR 4000 Series - ASR 1000 Series - Catalyst 8300-8500 running IOS-XE 17

Cisco Aggregation Services Router Cat8500 (C8500-12X4QC, C8500-12X)

Versió IOS-XE 17.3 (con fix 17.3.8a)

Fabricant Cisco Systems

Família Enrutadors

Tipus Producte

Data Inclusió 01/06/2022

Revisió de Validesa 31/10/2024

Descripció

Els routers de Cisco permeten el seu desplegament en xarxes WAN, LAN i el núvol. Proporcionen una solució completa i provada a través d'anàlisis avançades, optimització d'aplicacions, aprovisionament automatitzat i seguretat integrada.

Observacions

CCN-STIC-1461 PES Cisco ISR 4000 Series - ASR 1000 Series - Catalyst 8300-8500 running IOS-XE 17

Cisco Aggregation Services Router Cat8300 (C8300-1N1S-6T, C8300-1N1S-4T2X, C8300-2N2S-6T, C8300-2N2S-4T2X, NIMs: C-NIM-1X)

Versió IOS-XE 17.3 (con fix 17.3.8a)

Fabricant Cisco Systems

Família Enrutadors

Tipus Producte

Data Inclusió 01/06/2022

Revisió de Validesa 30/11/2024

Descripció

Els routers de Cisco permeten el seu desplegament en xarxes WAN, LAN i el núvol. Proporcionen una solució completa i provada a través d'anàlisis avançades, optimització d'aplicacions, aprovisionament automatitzat i seguretat integrada.

Observacions

CCN-STIC-1461 PES Cisco ISR 4000 Series - ASR 1000 Series - Catalyst 8300-8500 running IOS-XE 17

Huawei CloudEngine 16800 (CE16804, CE16808 i CE16816), Huawei CloudEngine 12800 (CE12804, CE12808 i CE12816), Huawei CloudEngine 8800 (CE8861-4C-EI i CE8850-64CQ-EI), Huawei CloudEngine 6800 (CE6863-48S6CQ, CE6881-48S6CQ, CE6820-48S6CQ, CE6863E-48S6CQ, CE6870-48S6CQ-EICE6870-48S6CQ-EI-A), CE5882-48T4S, CE9860-4C-EI I CE9860-4C-EI-A

Versió	V200R022C00SPC500
Fabricant	Huawei Technologies Espanya
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2026

Descripció

Els switches CloudEngine són switches que proporcionen serveis estables, fiables i d'alt rendiment en capa 2 i capa 3. Aquests switches estan dissenyats per a centres de dades i xarxes de campus d'alta gamma. Proporcionen alt rendiment, interfícies d'alta densitat i baixa latència. Els switches CloudEngine Series tenen un disseny maquinari avançat que subministra ports d'alta densitat mentre fa servir la mateixa plataforma Software Huawei VRP.

Observacions

Procediment d'ocupació assegurança pendent de publicació

Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches IE-9310-26S2C-E|A, IE-9320-26S2C-E|A, IE9320-22S2C4X-E|A, IE-9320-24P4S-E|A, IE-9320-24T|P4X-E|A, IE-9320-16P8U4X-E|A

Versió	IOS-XE 17.9
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/01/2024
Revisió de Validesa	31/07/2024

Descripció

Els Catalyst Industrial Ethernet 9300 Rugged Sèries Switches són equips dissenyat per a entorns industrials exigents. Aquest switch és resistent i durador, capaç de suportar condicions extremes. Ofereix una connectivitat de confiança i segura per a dispositius industrials, com a càmeres de vigilància, sensors i controladors. Té múltiples ports Ethernet que permeten la connexió de diversos dispositius i garanteixen una comunicació fluida en la xarxa.

A més, són equips fàcils de configurar i administrar, la qual cosa ho fa adequat per a entorns industrials on es requereix una infraestructura de xarxa robusta i de confiança.

Observacions

Procediment d'ocupació assegurança pendent de publicació

Cisco Nexus 3600 Series Switches (36180YC-R, 3636C-R)	
Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

Cisco Nexus 3400 Series Switches (34180-YC, 3464C, 3432D-S, 3408-S)	
Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

F**Descripció**

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

Cisco Catalyst 9400X/9600X (C9404R, C9407R, C9410R, C9400X-SUP-2, C9400X-SUP-2XL, C9400-LC-48HX, C9400-LC-48XS, C9606R, C9600X-SUP2, C9600-LC-40YL4CD, C9600X-LC-32CD)	
Versió	IOS-XE 17.9
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

FDescripció

Els Cisco Catalyst 9400X/9600X són switches de xarxa que ofereixen una alta densitat ports Ethernet per mòdul, incloent-hi opcions de PoE+. Estan dissenyats amb un potent processador i ofereixen serveis de xarxa avançats per a empreses que necessiten una xarxa segura i escalable. Són equips de xarxa d'alt rendiment. Ofereixen alta densitat de ports Ethernet per mòdul, amb opcions de 10 Gbps, 25 Gbps i 40 Gbps. Estan equipats amb un processador que proporciona una alta capacitat de processament i seguretat avançada.

Observacions

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

Cisco Catalyst 9300 Series Switches (C9300-24T|P|U|AUX|S|H, C9300-48T|P|U|UXM|UN|S|H, C9300D-24UB|UXB, C9300D-48UB) amb els següents mòduls de xarxa (C9300-NM-4G|8X|2Q|4M|2Y)	
Versió	IOS-XE 17.9 (amb 17.9.4a)
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	10/11/2023
Revisió de Validesa	30/04/2026

Descripció

Els Cisco Catalyst 9300y 9300L són switches de xarxa que ofereixen una alta densitat ports Ethernet per mòdul, incloent opcions de PoE+. Estan dissenyats amb un potent processador i ofereixen serveis de xarxa avançats per a empreses que necessiten una xarxa segura i escalable. Els Cisco Catalyst 9300L, la variant compacta de la Serie 9300, ideals per a petites i mitjanes empreses.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	04/10/2025

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	04/10/2025

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	ArubaOS 16.11
Fabricant	HPE Aruba Networking
Família	Enrutadors
Tipus	Producte
Data Inclusió	27/12/2023
Revisió de Validesa	30/06/2024

Descripció

Equips dissenyats per a utilitzar-se en labors d'accés i agregació, o nucli de xarxa d'accés. Són equips que proporcionen connexions de totes les velocitats i tipus de mitjans. Equips amb capacitat de commutació sense bloqueig (senar-blocking). Segons la família, ofereixen solucions escalables mitjançant constitució de stacks via port de xarxa, port dedicat així com existeixen models de xassissos. Totes les funcions del sistema operatiu s'ofereixen amb l'equip. Ofereixen diversos tipus d'interfícies i velocitats. Ofereixen PoE en alguns models, a diferents potències.

Poden són gestionables, tant localment (gestió on-premise) com poden arribar a administrar-se en modalitat Programari-as-a-Service.

Observacions

Procediment d'Ocupació Segura pendent de publicació

Dell EMC Networking SmartFabric (Models: S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, MX5108n, S4248FB-ON, S4248FBL-ON, S6010-ON, Z9100-ON, MX9116n, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9264F ON i Z9332F-ON)

Versió	OS 10 Build: 10.5.1.3.
Fabricant	Dell Computer
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/12/2020
Revisió de Validesa	31/08/2024

Descripció

Dell EMC Smart Fabric OS10 és el sistema operatiu de xarxa (NOS) que s'utilitza en les famílies d'enrutadors i commutadors de les Serie N (alguns models), Serie S, Serie Z i Serie MX de Dell EMC Networking (les plataformes HW que actualment suporten OS10 són N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n i MX9116n). Dell EMC SmartFabric OS10 és un sistema operatiu de xarxa (NOS) que admet múltiples arquitectures i entorns. La solució SmartFabric OS10 permet la desagregació en diverses capes de la funcionalitat de xarxa. SmartFabric OS10 comprèn l'administració, monitoratge i funcionalitat completa i estàndard de la indústria de xarxes de nivell 2 i nivell 3 a través d'interfícies CLI, SNMP i REST. Els usuaris poden triar les seves pròpies aplicacions d'organització, gestió, supervisió i xarxes de tercers. Per desenvolupar xarxes escalables L2 i L3, SmartFabric OS10 ofereix una solució modular i desagregada en una única imatge binària.

Observacions

CCN-STIC-1429 PES DELL EMC Networking

Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800) i Cisco Catalyst 8300 Rugged Series Routers (IR8300)	
Versió	IOS-XE 17.9 (amb 17.9.4a)
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/09/2023
Revisió de Validesa	29/02/2024

Descripció

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

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

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

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

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

Observacions

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

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

Versió	V200R022C00SPC500
Fabricant	Huawei Technologies Espanya
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2024

Descripció

Els switches de la Serie-S de Huawei estan dissenyats per cobrir les necessitats d'evolució de la xarxa de campus. Entre les seves capacitats destaquen la gestió simplificada i l'alt rendiment. Poden ser utilitzats en qualsevol tipus de sector: empresarial, governamental, educatiu, financer o industrial.

Observacions

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

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

Versió	V200R022C00SPC500
Fabricant	Huawei Technologies Espanya
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2024

Descripció

Els switches de la Serie-S de Huawei estan dissenyats per cobrir les necessitats d'evolució de la xarxa de campus. Entre les seves capacitats destaquen la gestió simplificada i l'alt rendiment. Poden ser utilitzats en qualsevol tipus de sector: empresarial, governamental, educatiu, financer o industrial.

Observacions

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

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

Versió	V600R021C10SPC100
Fabricant	Huawei Technologies Espanya
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/02/2024
Revisió de Validesa	31/07/2026

Descripció

Les plataformes d'encaminament Huawei AR són els primers dissenyats per a l'era de la cloud, presenta enllaços ascendent de banda ultra ampla 4G/5G i compta amb un rendiment de reexpedició que és tres vegades la mitjana de la indústria. Oferint a més diverses característiques. Compatible amb la xarxa definida per programari (SD-WAN), la gestió del núvol, la xarxa privada virtual (VPN), la commutació d'etiquetes (MPLS), la seguretat i la veu.

Observacions

CCN-STIC 1462 Huawei NetEngine AR6700&AR8000

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

Versió	V200R022C00SPC500
Fabricant	Huawei Technologies Espanya
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2024

Descripció

Els switches de la Serie-S de Huawei estan dissenyats per cobrir les necessitats d'evolució de la xarxa de campus. Entre les seves capacitats destaquen la gestió simplificada i l'alt rendiment. Poden ser utilitzats en qualsevol tipus de sector: empresarial, governamental, educatiu, financer o industrial.

Observacions

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

Huawei S Series Ethernet Switches S5736 (S24UM4XC, S48S4X-A, S24S4XC, S24T4XC, S24U4XC, S48S4XC, S48S4X-D, S48T4XC, S48U4XC)	
Versió	V200R022C00SPC500
Fabricant	Huawei Technologies Espanya
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2024

Descripció

Els switches de la Serie-S de Huawei estan dissenyats per cobrir les necessitats d'evolució de la xarxa de campus. Entre les seves capacitats destaquen la gestió simplificada i l'alt rendiment. Poden ser utilitzats en qualsevol tipus de sector: empresarial, governamental, educatiu, financer o industrial.

Observacions

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

7.5.2. SWITCHES

Dell EMC Networking SmartFabric OS10.5.4en Switches de les series N, S i Z (N3248TE, S41xx, S52xx, S54xx, Z91xx, Z92xx, Z93xx, Z94xx, Z96xx)	
Versió	OS10.5.4
Fabricant	DELL COMPUTER, S.A.
Família	Switches
Tipus	Producte
Data Inclusió	01/10/2023
Revisió de Validesa	31/03/2024

Descripció

Dell EMC Smart Fabric OS10 és el sistema operatiu de xarxa (NOS) que s'utilitza en les famílies d'enrutadors i commutadors de les Serie N (alguns models), Serie S, Serie Z i Serie MX de Dell EMC Networking (les plataformes HW que actualment suporten OS10 són N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n i MX9116n). Dell EMC SmartFabric OS10 és un sistema operatiu de xarxa (NOS) que admet múltiples arquitectures i entorns. La solució SmartFabric OS10 permet la desagregació en diverses capes de la funcionalitat de xarxa. SmartFabric OS10 comprèn l'administració, monitoratge i funcionalitat completa i estàndard de la indústria de xarxes de nivell 2 i nivell 3 a través d'interfícies CLI, SNMP i REST. Els usuaris poden triar les seves pròpies aplicacions d'organització, gestió, supervisió i xarxes de tercers. Per desenvolupar xarxes escalables L2 i L3, SmartFabric OS10 ofereix una solució modular i desagregada en una única imatge binària.

Observacions

CCN-STIC-1429 PES DELL EMC Networking

Cisco Catalyst 9600 Series Switches (C9606R, C9600-SUP-1 i C9600-LC-24C|48YL|48TX|24S)	
Versió	IOS-XE 17.9 (amb 17.9.4a)
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	13/11/2023
Revisió de Validesa	30/04/2026

Descripció

Els Cisco Catalyst 9400 9500 i 9600 són equips de xarxa d'alt rendiment. Ofereixen alta densitat de ports Ethernet per mòdul, amb opcions de 10 Gbps, 25 Gbps i 40 Gbps. Estan equipats amb un processador que proporciona una alta capacitat de processament i seguretat avançada.

Observacions

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

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

Versió	22.4R2
Fabricant	Juniper Networks
Família	Switches
Tipus	Producte
Data Inclusió	01/06/2022
Revisió de Validesa	31/12/2024

Descripció

La família de switches EX4100, en les seves diferents variants, són dispositius de xarxa segurs amb alta densitat de ports 10/100/1000Base-T o multigigabit 100/1000/2500/5000/10000Base-T així com ports de uplinks 1/10/25GbE. Totes les plataformes EX4100 funcionen amb el programari Junos US, que és un sistema operatiu especialment dissenyat per a aquesta mena de dispositius de xarxa. Junos US Proporciona funcions de gestió, control i monitoratge, així com tota la provisió de canvis en els dispositius. Els switches EX4100 són dispositius de xarxa que suporten la definició, i compliment, de polítiques de flux d'informació entre els nodes de la xarxa. Al costat de funcions de seguretat en el trànsit d'informació, el producte registra totes les activitats rellevants, i compta amb eines de seguretat per a la gestió segura. Com switch de nivell 2 en la capa OSI, realitza l'anàlisi de paquets entrants, reexpedeix aquests paquets en funció de la informació que contenen en la seva capçalera Ethernet, fent-los arribar així al seu destinatari. Com switch de nivell 3 en la capa OSI, permet l'encaminament del trànsit, basat en taules, identificant les rutes disponibles, les condicions, la distància i els costos per a així determinar el camí més adequat per a cada paquet. La família EX4100 suporta també l'ús de tecnologies de overlay com és el cas de EVPN-VXLAN que permeten la microsegmentació usant group-based policies (GBP), a més de suportar MACsec AES-256 i Power over Ethernet.

Observacions

Procediment d'Ocupació Segura Pendent de Publicació

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

Versió	IOS-XE 17.9 (amb 17.9.a)
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	14/11/2023
Revisió de Validesa	30/04/2026

Descripció

Els equips Cisco Catalyst 9200 i 9200L són switches d'alt rendiment i seguretat reforçada, ideals per a empreses que requereixen solucions de xarxa segures i escalables. Amb models que varien des de 24 fins a 48 ports, proporciona una gran flexibilitat per adaptar-se a qualsevol mida de xarxa. Ofereixen gestió avançada i detecció d'amenaces millorada.

Els Cisco Catalyst 9200L són la variant de la Serie 9200, mantenint les mateixes característiques de seguretat i rendiment. Són ideals per a petites i mitjanes empreses que busquen una xarxa segura i escalable.

Observacions

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

RUCKUS FastIron series ICX8200, ICX7550 e ICX7850 Switch/Router

Versió	10.0.10c
Fabricant	CommScope Technologies
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	31/12/2026

Descripció

La família RUCKUS ICX de commutadors de nivell 2 i 3 disposa d'una gamma de models tant per a campus i xarxes empresarials de 2 i 3 nivells com per a Data Center, cobrint tot el rang de velocitats de port des de 1G fins a 100G.

Inclou tecnologies com Stacking a tala i llarga distància, fonts d'alimentació redundants, nivell 3 avançat, protocols d'alta disponibilitat, microsegmentació i automatització, entre altres.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

Junos OS 22.4R1 MX304

Versió	22.2R1
Fabricant	Juniper Networks
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2024

Descripció

Les plataformes d'encaminament universal MX304 brinden un rendiment de gran escalabilitat en un factor de forma optimitzat per al núvol i les economies de cost per port o bit més exigents. Es poden utilitzar tant en xarxes de tipus operador, com a node de vora en xarxes MPLS, en entorns de mobilitat convergent, IoT, empresarial i també en arquitectures de Core convergent i de bord multiservei. També suporta l'ús com a encaminador de commutació d'etiquetes (LSR), provider Edge, equip d'intercanvi d'Internet i xarxa troncal per a implementacions en xarxes de caràcter metropolitanes, regionals o nacionals, o terminador de túnels IPSEC o Firewall de capa 4. La sèrie MX admet un ampli conjunt de funcionalitats IPoDWDM, L2, L3, IP/MPLS, SR, SRv6, o terminador de túnels IPSEC per a permetre xarxes de transport a gran escala amb operacions i aprovisionament de serveis simplificats, mantenint simplicitat en la xarxa. Gràcies al tipus de chipsets implementats, tenen una capacitat de programació en el pla de dades gairebé infinita, la qual cosa li brinda la llibertat d'implementar noves innovacions de xarxa. Amb tecnologia de silici TRIO, la família MX304 és altament escalable des dels 1.6Tbps, passant per 3.2 Tbps fins als 4.8 Tbps en 2U depenent del número de slots utilitzats.

Observacions

Procediment d'ocupació assegurança pendent de publicació

Cisco Catalyst 9500 Series Switches (C9500-12Q|24Q|40X|16X|32C|32QC|24Y4C|48Y4C) amb els següents mòduls de xarxa (C9500-NM-8X i C9500-NM-2Q)

Versió	IOS-XE 17.9 (amb 17.9.4a)
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	13/11/2023
Revisió de Validesa	30/04/2026

Descripció

Els Cisco Catalyst 9400 9500 i 9600 són equips de xarxa d'alt rendiment. Ofereixen alta densitat de ports Ethernet per mòdul, amb opcions de 10 Gbps, 25 Gbps i 40 Gbps. Estan equipats amb un processador que proporciona una alta capacitat de processament i seguretat avançada.

Observacions

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

ACX5448-M

Versió	Junos OS 22.3R1
Fabricant	Juniper Networks
Família	Enrutadors
Tipus	Producte
Data Inclusió	07/05/2024
Revisió de Validesa	31/10/2024

Descripció

La línia Juniper Networks® ACX5000 sorgeix com a resposta a un canvi en les arquitectures de xarxes metropolitanes on les capes d'accés i agregació estan estenent la intel·ligència operativa des de l'extrem del proveïdor de serveis fins a la xarxa d'accés. La línia ACX5000 simplifica les arquitectures d'accés i agregació en eliminar capes innecessàries i superposicions de xarxa, la qual cosa redueix dràsticament CapEx i OpEx. Està basada en la simplificació de l'arquitectura i en la reducció de costos, la línia ACX5000 brinda als proveïdors de serveis i empreses la capacitat d'adoptar un veritable paradigma de metre universal.

Així mateix, proporciona alta capacitat, escalabilitat i una capa de transport òptic de paquets, al mateix temps que ofereix un rendiment líder en la indústria amb una àmplia gamma de densitats de ports i tipus d'interfície.

La sèrie ACX presenta el lideratge IP/MPLS de Juniper des del core i el perímetre de la xarxa fins a les capes d'accés. La sèrie ACX admet un ampli conjunt de funcionalitats L2, L3 i IP/MPLS per a permetre xarxes MPLS transparents a gran escala amb operacions i aprovisionament de serveis simplificats mantenint simplicitat en la xarxa.

ACX5448-M: L'ACX5448-M té 44 ports 1GbE/10GbE i 6 ports 40GbE/100GbE, així com capacitats de seguretat avançades com such as Mitjana Access Control Security (MACsec) on all 1GbE/10GbE ports.

Observacions

CCN-STIC-1445 PES Router_Juniper_ACX5448-M_JunOS 20.3R1

Cisco Embedded Services 9300 & 3300 Series Switches (ESS-3300-NCP|CON, ESS-3300-24T-NCP|CON, ESS9300-10X-E)

Versió	IOS-XE 17.9
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	07/03/2024
Revisió de Validesa	31/08/2024

Descripció

Els Cisco Embedded Services 9300 i 3300 Sèries Switches són plataformes de commutació integrades i altament versàtils, dissenyades per a aplicacions empresarials i d'Internet de les Coses (IoT) que requereixen una integració i resistència excepcionals en entorns desafiadors.

La sèrie 9300 és un conjunt de switches d'alt rendiment amb capacitats de Layer 2 i Layer 3, oferint funcionalitats avançades d'encaminament i seguretat. Aquests switches estan equipats amb la tecnologia de Cisco IOS XE, la qual cosa els permet manejar aplicacions intensives en dades i proporcionar una connectivitat de confiança i segura per a dispositius de vora.

La sèrie 3300 està dissenyada per a entorns industrials i de transport, amb un factor de forma compacte i resistent, complint amb els estàndards de durabilitat industrial. Aquests switches suporten una àmplia gamma de voltatges d'entrada i tenen classificacions esteses de temperatura, la qual cosa els fa ideals per al seu ús en condicions adverses on altres equips podrien fallar.

Totes dues sèries ofereixen característiques com Power over Ethernet (PoE) i PoE+, optimitzant la instal·lació de dispositius de IoT en permetre la transmissió de dades i energia elèctrica a través del mateix cable de xarxa. Amb la gestió intel·ligent d'energia i una arquitectura de maquinari de confiança, els Cisco Embedded Services 9300 i 3300 Sèries Switches són solucions robustes per a xarxes que demanden resistència i rendiment en qualsevol entor.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

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

Versió	09.0.10
Fabricant	CommScope Technologies
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	30/09/2025

Descripció

La família RUCKUS ICX de commutadors de nivell 2 i 3 disposa d'una gamma de models tant per a campus i xarxes empresarials de 2 i 3 nivells com per a Data Center, cobrint tot el rang de velocitats de port des de 1G fins a 100G.

Inclou tecnologies com Stacking a tala i llarga distància, fonts d'alimentació redundants, nivell 3 avançat, protocols d'alta disponibilitat, microsegmentació i automatització, entre altres.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

QFX5120-48YM

Versió	Junos OS 22.3R1
Fabricant	Juniper Networks
Família	Switches
Tipus	Producte
Data Inclusió	10/05/2024
Revisió de Validesa	31/12/2024

Descripció

Les famílies QFX5k i EX4650, en les seves diferents variants, són dispositius de xarxa segurs amb alta densitat de ports 1GbE, 10GbE, 25GbE i 100GbE. Aquestes plataformes de commutació per al centre de dades funcionen amb el Software Junos OS, que és un sistema operatiu especialment dissenyat per a aquest tipus de dispositius. Junos OS proporciona funcions de gestió, control i monitoratge, així com tota la provisió de canvis en els dispositius.

Aquests switches per a centres de dades són dispositius de xarxa que suporten la definició, i compliment, de polítiques de flux d'informació entre els nodes de la xarxa. Juntament amb funcions de seguretat del trànsit d'informació, el producte registra totes les activitats rellevants, i compta amb eines de seguretat per a la gestió segura.

Com a switch de nivell 2 a la capa OSI, realitza l'anàlisi de paquets entrants, reenviant aquests paquets en funció de la informació que contenen, fent-los arribar així al seu destinatari.

Com a switch de nivell 3 a la capa OSI, admet l'encaminament del trànsit, basat en taules, identificant les rutes disponibles, les condicions, la distància i els costos per així determinar el camí més adequat per a cada paquet.

Observacions

Procediment d'Ocupació Segura pendent de publicació

Cisco Catalyst 9200CX Series Switches

Versió	IOS-XE 17.9
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	20/03/2024
Revisió de Validesa	31/08/2024

Descripció

Els Cisco Catalyst 9200CX són switches compactes de la sèrie Catalyst, dissenyat per a espais petits, ofereix capacitats de commutació de nivell empresarial, seguretat, PoE i suport per a IoT, ideal per a micro sucursals i entorns amb limitacions d'espai.

Catalyst 9200CX inclouen:

- C9200CX-12T-2X2G
- C9200CX-12P-2X2G
- C9200CX-8P-2X2G

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

Cisco Catalyst 9300LM Series Switches

Versió	IOS-XE 17.9
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	20/03/2024
Revisió de Validesa	31/08/2024

Descripció

Els Cisco Catalyst 9300LM són part de la sèrie Catalyst, són switches d'accés empresarial dissenyats per a xarxes de campus i sucursals. La variant "LM" s'enfoca a oferir capacitats de multigigabit Ethernet (mGig) que permeten velocitats de xarxa superiors a 1 Gbps en cablejat de coure existent. Aquests switches són apilables i suporten funcionalitats avançades com a seguretat integrada, automatització i una plataforma preparada per a suportar aplicacions de IoT. Són ideals per a escenaris que demanden alta densitat de connectivitat i velocitats de xarxa elevades per a manejar el creixent trànsit de dades i dispositius connectats.

Catalyst 9300LM inclouen:

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

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

Cisco Catalyst 9300X Series Switches

Versió	IOS-XE 17.9
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	20/03/2024
Revisió de Validesa	31/08/2024

Descripció

Els Cisco Catalyst 9300X són una línia de switches de xarxa de la sèrie Catalyst, que representen la següent generació de dispositius de commutació d'accés empresarial. Aquests switches ofereixen un alt rendiment, són apilables i estan dissenyats per a suportar una àmplia gamma de funcionalitats com a seguretat avançada, automatització i connectivitat d'alta densitat amb suport per a tecnologies com a Wi-Fi 6, mGig i UPOE+ (Universal Power Over Ethernet Plus). Són adequats per a organitzacions que requereixen una infraestructura de xarxa àgil i preparada per al futur en entorns de campus i sucursals.

Catalyst 9300X inclouen:

- C9300X-48HX con los siguientes módulos de red: C9300X-NM-4C, C9300X-NM-8M, C9300X-NM-2C,
- C9300X-NM-8Y
- C9300X-48TX con los siguientes módulos de red: C9300X-NM-4C, C9300X-NM-8M,C9300X-NM-2C,
- C9300X-NM-8Y
- C9300X-12Y con los siguientes módulos de red: C9300X-NM-8M, C9300X-NM-2C, C9300X-NM-8Y
- C9300X-24Y con los siguientes módulos de red: C9300X-NM-4C, C9300X-NM-8M, C9300X-NM-2C, C9300XNM-8Y
- C9300X-48HXN con los siguientes módulos de red: C9300X-NM-8M, C9300X-NM-2C, C9300X-NM-8Y
- C9300X-24HX con los siguientes módulos de red: C9300X-NM-8M, C9300X-NM-2C, C9300X-NM-8Y

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

Cisco Catalyst 9500X Series Switches

Versió	IOS-XE 17.9
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	20/03/2024
Revisió de Validesa	31/08/2024

Descripció

Els Cisco Catalyst 9500X formen part del Porfolio de switches de nucli i distribució d'alt rendiment. Aquests dispositius estan dissenyats per a satisfer les necessitats de xarxes de campus, oferint una gran capacitat de commutació, altes velocitats de port, i suport per a tecnologies de xarxa de pròxima generació. Amb característiques avançades de seguretat, automatització i analítica, els Catalyst 9500X són ideals per a entorns que requereixen una infraestructura de xarxa robusta, segura i d'alta eficiència.

Catalyst 9500X inclouen:

- C9500X-28C8D

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

RouterTeldat-M1 Series

Versió	11.01.09
Fabricant	TELDAT, S.A.
Família	Switches
Tipus	Producte
Data Inclusió	01/05/2023
Revisió de Validesa	31/10/2025

Descripció

Es tracta d'una família de routers compactes orientats a oficines petites i mitjanes, però que requereixen connexió d'alta velocitat. El seu disseny compacte i sense ventiladors, per no generar soroll, permeten instal·lar-lo en àrees de treball, una cosa molt útil en petites oficines, botigues o despatxos professionals. A més, en aquests entorns aquesta família de routers afavoreix l'ús de connexions 3G/4G per la disponibilitat més gran de cobertura que en instal·lacions realitzades en sales o armaris tècnics. Tot i ser routers compactes, alguns models poden assolir velocitats de fins a 600 Mbps simètrics, i són molt escalables gràcies a un slot i una àmplia varietat de targetes. Integren connectivitat Ethernet WAN i commutador Ethernet de 4 ports LAN, a més d'un punt d'accés Wi-Fi i connectivitat 3G/4G. A més d'un sofisticat maquinari, inclouen un avançat Software adaptat a xarxes professionals que inclou totes les funcionalitats demandades a un router professional com routing (RIP, OSPF, BGP, VRF, PolicyRouting,...), seguretat (ACLs, Firewall, IPSec, 802.1X, ...), qualitat de servei (CBWFQ, PQ, perfilat, ...), o gestió (CLI, SNMPv3, RADIUS, TACACS+, Syslog, Netflow, Mirroring,...).

Observacions

CCN-STIC-1455 Procediment d'ocupació assegurança Teldat M1 Series

EX4300-48MP

Versió	Junos OS 19.4R1
Fabricant	Juniper Networks
Família	Switches
Tipus	Producte
Data Inclusió	01/06/2022
Revisió de Validesa	31/12/2024

Descripció

La família de switches EX4300, en les seves diferents variants, són dispositius de xarxa segurs amb alta densitat de ports 10/100/1000Base-T o 100/1000/2500/5000/10000Base-T així com uplinks 1/10/25GbE o 40/100GbE. Totes les plataformes EX4300 funcionen amb el Software Junos OS, que és un sistema operatiu especialment dissenyat per a aquest tipus de dispositius. Junos OS proporciona funcions de gestió, control i monitoratge, així com tota la provisió de canvis en els dispositius.

Els switches EX4300 són dispositius de xarxa que suporten la definició, i compliment, de polítiques de flux d'informació entre els nodes de la xarxa. Juntament amb funcions de seguretat del trànsit d'informació, el producte registra totes les activitats rellevants, i compta amb eines de seguretat per a la gestió segura.

Com a switch de nivell 2 a la capa OSI, realitza l'anàlisi de paquets entrants, reenviant aquests paquets en funció de la informació que contenen, fent-los arribar així al seu destinatari.

Com a switch de nivell 3 a la capa OSI, admet l'encaminament del trànsit, basat en taules, identificant les rutes disponibles, les condicions, la distància i els costos per així determinar el camí més adequat per a cada paquet.

Observacions

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

Nokia 1830 Photonic Service Switch (PSS)

Versió	9.1
Fabricant	NOKIA
Família	Switches
Tipus	Producte
Data Inclusió	01/03/2022
Revisió de Validesa	31/08/2024

Descripció

El commutador de servei fotònic Nokia 1830PSS és una plataforma que ofereix connectivitat multiservei de multiplexació òptica per divisió de longitud d'ona densa de gran capacitat. Inclou xifrat, baixa latència i detecció d'intrusions òptiques, la qual cosa garanteix la confidencialitat i integritat de les dades, així com el suport de comunicacions.

La família 1830PSS consta de diferents plataformes que s'han optimitzat per a la seva aplicabilitat en diversos entorns de desplegament de xarxes òptiques, des de la interconnexió de CPD fins a l'escalat de grans xarxes òptiques multiservei, multicapa, regionals i de llarga distància. Aquests equips aprofiten el Software , el maquinari, la gestió i el control comuns, per oferir operacions fluides en tota la cartera de possibilitats que ofereix la família 1830PSS.

Són compatibles amb múltiples aplicacions de xarxa de transport, que inclouen: transport i agregació metro multiservei, implementacions de llarga distància/nucli òptic, configuracions de commutació fotònica amb encaminament colorless, directionless i contentionless amb Flexgrid, agregació/commutació en capa L1, mesures reflextomètriques OTDR de les fibres òptiques, i altres mecanismes de protecció.

Observacions

CCN-STIC-1463 Procediment d'ocupació assegurança Nokia 1830 Photon Service Switch (PSS) v.9.1

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

Versió	10.11
Fabricant	HPE Aruba Networking
Família	Switches
Tipus	Producte
Data Inclusió	20/03/2024
Revisió de Validesa	31/08/2024

Descripció

La família Aruba CX implementen solucions de switching i routing per a xarxes de sucursals, campus i datacenter. Els equips 10000, 8320, 8325, 8360, i 8400 són idonis per a Datacenter i equips nucli (core) de la xarxa de campus. Els equips 6400 es posicionen com a equips nucli (core) de la xarxa de campus, mentre els 6300 i 6200 estan orientats per a xarxes d'accés. Implementen funcionalitats multicapa, implementen múltiples mecanismes de seguretat en l'accés i administració. Orientat a la segmentació dinàmica i a implementar entorns Zero Trust. Permet el desplegament automàtic desatès (ZTP) Aruba CX disposa d'una arquitectura interna de Sistema Operatiu que proporciona una manera de treballar amb el completament programable. El seu motor d'analítiques (NAE) permet la inserció de scripts de per a l'execució de tasques avançades de monitoratge i respostes a esdeveniments.Els equips 4100i són equips amb protecció mediambientals i de format industrial.

Observacions

Procediment d'Ocupació Segura pendent de publicació

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	10/04/2025

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	IOS-XE 17.9 (con fix 17.9.4a)
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	14/11/2023
Revisió de Validesa	30/04/2026

Descripció

Els Cisco Catalyst 9300y 9300L són switches de xarxa que ofereixen una alta densitat ports Ethernet per mòdul, incloent opcions de PoE+. Estan dissenyats amb un potent processador i ofereixen serveis de xarxa avançats per a empreses que necessiten una xarxa segura i escalable. Els Cisco Catalyst 9300L, la variant compacta de la Serie 9300, ideals per a petites i mitjanes empreses.

Observacions

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

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

Versió	22.2R1
Fabricant	Juniper Networks
Família	Switches
Tipus	Producte
Data Inclusió	01/02/2024
Revisió de Validesa	31/07/2024

Descripció

Les plataformes d'encaminament universal MX240/MX480/MX960 brinden un rendiment de gran escalabilitat en un factor de forma optimitzat per al núvol i les economies de cost per port o bit més exigents. Es poden utilitzar tant en xarxes de tipus operador, com a node de vora en xarxes MPLS, en entorns de mobilitat convergent, IoT, empresarial i també en arquitectures de Core convergent i de bord multiservei. També suporta l'ús com a encaminador de commutació d'etiquetes (LSR), provider Edge, equip d'intercanvi d'Internet i xarxa troncal per a implementacions en xarxes de caràcter metropolitanes, regionals o nacionals, o terminador de túnels IPSEC o Firewall de capa 4. La sèrie MX admet un ampli conjunt de funcionalitats IPoDWDM, L2, L3, IP/MPLS, SR, SRv6, erminador de túnels IPSEC o CGNAT per a permetre xarxes de transport a gran escala amb operacions i aprovisionament de serveis simplificats, mantenint simplicitat en la xarxa. Gràcies al tipus de chipsets implementats, tenen una capacitat de programació en el pla de dades gairebé infinita, la qual cosa li brinda la llibertat d'implementar noves innovacions de xarxa. Amb tecnologia de silici TRIO, la família MX és altament escalable des dels 3Tbps en 3U, passant per 38,4 Tbps en 5 slots i fins a un rendiment de 12 Tbps en 16 slots.

Observacions

Procediment d'ocupació segura pendent de publicació

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

Versió	ArubaOS 16.08
Fabricant	Aruba
Família	Switches
Tipus	Producte
Data Inclusió	01/12/2021
Revisió de Validesa	31/05/2024

Descripció

Equips dissenyats per utilitzar-se en tasques d'accés i agregació, o nucli de xarxa d'accés. Són equips que proporcionen connexions de totes les velocitats i tipus de mitjans. Equips amb capacitat de commutació sense bloqueig (non-blocking). Segons la família, ofereixen solucions escalables mitjançant constitució de stacks via port de xarxa, port dedicat així com existeixen models de xassís. Totes les funcions del sistema operatiu s'ofereixen amb l'equip. Ofereixen diversos tipus d'interfícies i velocitats. Ofereixen PoE en alguns models, a diferents potències.

Poden ser gestionables, tan localment (gestió on-premise) com poden arribar a administrar-se en modalitat Software-as-a-Service

Observacions

CCN-STIC-647C Seguretat en commutadors HPE Aruba

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

Versió	8.3
Fabricant	Extreme Networks
Família	Switches
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	30/09/2025

Descripció

Família de switches i routers WAN que suporten tecnologia Fabric. Mitjançant aquesta tecnologia, basada en els estàndards IEEE 802.1aq i IETF RFC 6329, es permet la creació de xarxes virtualitzades que automatitzen el provisionament extrem a extrem de serveis de xarxa, eliminant el risc de bucles i utilitzant un únic protocol. Se suporten virtualitzacions de Nivell 2, Nivell 3 i routing d'IP Multicast.

Els equips ofereixen una varietat d'interfícies, des d'1 Gbps fins a 100 Gbps.

Observacions

CCN-STIC-1451 Procediment d'ocupació segur Extreme Networks Virtual Services Platform (VSP) Series Switches

Cisco Catalyst 9500 Series Switches (C9500-12Q|24Q|40X|16X|32C|32QC|24Y4C|48Y4C) amb els següents mòduls de xarxa (C9500-NM-8X i C9500-NM-2Q)	
Versió	IOS-XE 17.9 (amb 17.9.4a)
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	13/11/2023
Revisió de Validesa	30/04/2026
Descripció	

Els Cisco Catalyst 9400 9500 i 9600 són equips de xarxa d'alt rendiment. Ofereixen alta densitat de ports Ethernet per mòdul, amb opcions de 10 Gbps, 25 Gbps i 40 Gbps. Estan equipats amb un processador que proporciona una alta capacitat de processament i seguretat avançada.

Observacions

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

Cisco Catalyst 9200 Series Switches (C9200-24T, C9200-48T, C9200-24P, C9200-48P, C9200-24PB, C9200-48PB, C9200-48PL, C9200-24PXG, C9200-48PXG) amb els mòduls de xarxa (C9200-NM 4G|4X|2Y|2Q)	
Versió	IOS-XE 17.9 (con fix 17.9.a)
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	14/11/2023
Revisió de Validesa	30/04/2024
Descripció	

Els equips Cisco Catalyst 9200 i 9200L són switches d'alt rendiment i seguretat reforçada, ideals per a empreses que requereixen solucions de xarxa segures i escalables. Amb models que varien des de 24 fins a 48 ports, proporciona una gran flexibilitat per adaptar-se a qualsevol mida de xarxa. Ofereixen gestió avançada i detecció d'amenaces millorada.

Observacions

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

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

Versió	IOS-XE 17.9 (amb 17.9.4a)
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	13/11/2023
Revisió de Validesa	30/04/2024

Descripció

Els Cisco Catalyst 9400, 9500 i 9600 són equips de xarxa d'alt rendiment. Ofereixen alta densitat de ports Ethernet per mòdul, amb opcions de 10 Gbps, 25 Gbps i 40 Gbps. Estan equipats amb un processador que proporciona una alta capacitat de processament i seguretat avançada.

Observacions

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

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

Versió	EXOS 31.3.100
Fabricant	Extreme Networks
Família	Switches
Tipus	Producte
Data Inclusió	01/12/2022
Revisió de Validesa	31/05/2025

Descripció

Família de commutadors apilables d'alt rendiment, que proporcionen connectivitat gigabit, multigigabit, 10G, 25G, 40G i 100G. Els equips poden posicionar-se tant en l'accés com en l'agregació en el nucli, suportant protocols de routing avançat (BGP, MPLS, VXLAN, etc). També proporciona solucions d'implementació de Fabric

Observacions

CCN-STIC-1446 PES Switches EXoS

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

Versió	Junos OS 22.2R1
Fabricant	Juniper Networks
Família	Switches
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2024

Descripció

La família de switches EX4400, en les seves diferents variants, són dispositius de xarxa segurs amb alta densitat de ports 10/100/1000Base-T, 100/1000/2500/5000/10000Base-T, així com uplinks 1/10/25GbE o 40/100GbE o variants amb tots els seus ports en fibra. Totes les plataformes EX4400 funcionen amb el programari Junos US, que és un sistema operatiu especialment dissenyat per a aquesta mena de dispositius. Junos US Proporciona funcions de gestió, control i monitoratge, així com tota la provisió de canvis en els dispositius.

Els switches EX4400 són dispositius de xarxa que suporten la definició, i compliment, de polítiques de flux d'informació entre els nodes de la xarxa. Al costat de funcions de seguretat del trànsit d'informació, el producte registra totes les activitats rellevants, i compta amb eines de seguretat per a la gestió segura.

Com switch de nivell 2 en la capa OSI, realitza l'anàlisi de paquets entrants, reexpedint aquests paquets en funció de la informació que contenen, fent-los arribar així al seu destinatari. Com switch de nivell 3 en la capa OSI, admet l'encaminament del trànsit, basat en taules, identificant les rutes disponibles, les condicions, la distància i els costos per a així determinar el camí més adequat per a cada paquet

Observacions

Procediments d'Ocupació Segura pendent de publicació.

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

Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/05/2022
Revisió de Validesa	28/02/2026

Descripció

OS6360: Família de commutadors L2+ apilables amb ports 1G i enllaços 1G/10G. Dissenyats com a equips d'accés en xarxes convergents d'alta capacitat.

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches	
Versió	IOS-XE 17.3 (amb 17.3.8a)
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/11/2022
Revisió de Validesa	31/03/2025
Descripció	

La família de switches industrials Catalyst de Cisco estan basats en una plataforma de switching i routing construïda a propòsit amb capacitats de filtre per a capa 2 i 3 dels nivells OSI.

Observacions

CCN-STIC-1450 Procediment d'ocupació Assegurança de Catalyst 9000 i Catalyst IE3000

Cisco Catalyst 9200 Series Switches (C9200-24T, C9200-48T, C9200-24P, C9200-48P, C9200-24PB, C9200-48PB, C9200-48PL, C9200-24PXG, C9200-48PXG) amb els mòduls de xarxa (C9200-NM-4G,C9200-NM-4X,C9200-NM)	
Versió	IOS-XE 17.6.6a
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	30/06/2025
Descripció	

Cisco Catalyst 9200 Series Switches

Observacions

CCN-STIC-1450 Procediment d'ocupació Assegurança de Catalyst 9000 i Catalyst IE3000. La versió inicial qualificada va ser la 17.6 però després de la publicació de la vulnerabilitat pública [CVE-2023-20198], CISCO ha publicat una nova versió amb el fix (17.6.6a).

Huawei S Series Switches (S3710, S5732, S5735I, S5735, S6730, S16700-4, S16700-8, S8700-10, S8700-4 S8700-6)	
Versió	V600R022C10SPC500
Fabricant	Huawei Technologies Co., Ltd.
Família	Switches
Tipus	Producte
Data Inclusió	01/10/2023
Revisió de Validesa	31/03/2026

Descripció

Els models qualificats són: S3710-H24P4S-A, S3710-H24T4S-A, S3710-H48LP4S-A,S3710-H48T4S-A, S5732-H24S4X6QZ-TV2, S5732-H24S4X6QZ-V2, S5732-H24UM4Y2CZ-TV2, S5732-H24UM4Y2CZ-V2, S5732-H44S4X6QZ-TV2, S5732-H44S4X6QZ-V2, S5732-H48UM4Y2CZ-TV2, S5732-H48UM4Y2CZ-V2, S5735I-L10T4X-A-V2, S5735I-L10T4X-A-V2, S5735I-L8P4X-A-V2, S5735I-S24T4XE-V2, S5735I-S24U4XE-V2, S5735I-S8T4SN-V2, S5735I-S8T4XN-V2, S5735I-S8U4XN-V2, S5735-L10T4X-A-V2, S5735-L16T4S-A-V2, S5735-L16T4X-QA-V2, S5735-L24P4S-A-V2, S5735-L24P4XE-A-V2, S5735-L24T4S-A-V2, S5735-L24T4XE-A- V2, S5735-L24T4XE-D-V2, S5735-L24T4X-QA-V2, S5735-L48LP4S L48T4XE-A-V2, S5735-L48LP4XE-A-V2, S5735- L48P4XE-A-V2, S5735-L48T4S-A-V2, S5735-L48T4XE-A-V2, S5735-L48T4XE-D-V2, S5735-L8P2T4X-A-V2, S5735-L8P4S-A-V2, S5735-L8P4X-QA-V2, S5735-L8T4S-A-V2, S5735-L8T4X-QA-V2, S5735-S24P4XE-V2, S5735-S24T4XE-V2, S5735-S24U4XE-V2, S5735-S48P4XE-V2, S5735-S48T4XE-V2, S5735-S48U4XE-V2, S6730-H24X6C-TV2, S6730-H24X6C-V2, S6730-H28X6CZ-TV2, S6730-H28X6CZ-V2, S6730-H48X6C-TV2, S6730-H48X6C-V2, S6730-H48X6CZ-TV2, S6730-H48X6CZ-V2, S6730-H48Y6C-TV2, S6730-H48Y6C-V2, S16700-4, S16700-8, S8700-10, S8700-4 i S8700-6.

Observacions

CCN-STIC-1418 Procediment d'ocupació segur Switches Huawei Serie S Ethernet

Cisco Catalyst 9200L Series Switches (C9200L-24P-4G|4X, C9200L-24T-4G|4X, C9200L-48P-4G|4X, C9200L-48T-4G|4X, C9200L-48PL-4G|4X, C9200L-24|48PXG-2Y i C9200L-24|48PXG-4X)	
Versió	OS-XE 17.6.6a
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	30/06/2025
Descripció	
Series Cisco Catalyst 9200L.	
Observacions	
CCN-STIC-1450 Procedimiento de empleo Seguro de Catalyst 9000 y Catalyst IE3000. La versió inicial qualificada va ser la 17.6 però després de la publicació de la vulnerabilitat pública [CVE-2023-20198], CISCO ha publicat una nova versió amb el fix (17.6.6a).	

Cisco Catalyst 9300 Series Switches (C9300-24T|P|U|AUX|S|H, C9300-48T|P|U|UXM|UN|S|H, C9300D-24UB|UXB, C9300D-48UB) amb els següents mòduls de xarxa (C9300-NM-4G|8X|2Q|4M|2Y)	
Versió	IOS-XE 17.6.6a
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	31/07/2025
Descripció	
Series Cisco Catalyst 9200L.	
Observacions	
CCN-STIC-1458 Procedimiento de Empleo Seguro CISCO Routers y Switches IOS-XE 17.X. La versió inicial qualificada va ser la 17.6 però després de la publicació de la vulnerabilitat pública [CVE-2023-20198], CISCO ha publicat una nova versió amb el fix (17.6.6a).	

Cisco Catalyst 9300L Series Switches (C9300L-24T|P-4G,C9300L-48T|P-4G, C9300L-24T|P-4X, C9300L48T|P-4X,C9300L-48PF-4G|4X, C9300L-24UXG-4X|2Q, C9300L-48UXG-4X|2Q)	
Versió	IOS-XE 17.6.6a
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	31/07/2025
Descripció	
Series Cisco Catalyst 9200L.	
Observacions	
CCN-STIC-1458 Procedimiento de Empleo Seguro CISCO Routers y Switches IOS-XE 17.X. La versió inicial qualificada va ser la 17.6 però després de la publicació de la vulnerabilitat pública [CVE-2023-20198], CISCO ha publicat una nova versió amb el fix (17.6.6a).	

Cisco Catalyst 9300L Series Switches (C9300L-24T|P-4G,C9300L-48T|P-4G, C9300L-24T|P-4X, C9300L48T|P-4X,C9300L-48PF-4G|4X, C9300L-24UXG-4X|2Q, C9300L-48UXG-4X|2Q)	
Versió	IOS-XE 17.6.6a
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	31/07/2025
Descripció	
Cisco Catalyst 9300L Series Switches	
Observacions	
CCN-STIC-1458 Procedimiento de Empleo Seguro CISCO Routers y Switches IOS-XE 17.X. La versió inicial qualificada va ser la 17.6 però després de la publicació de la vulnerabilitat pública [CVE-2023-20198], CISCO ha publicat una nova versió amb el fix (17.6.6a).	

Cisco Catalyst 9300L Series Switches (C9300L-24T|P-4G,C9300L-48T|P-4G, C9300L-24T|P-4X, C9300L48T|P-4X,C9300L-48PF-4G|4X, C9300L-24UXG-4X|2Q, C9300L-48UXG-4X|2Q)	
Versió	IOS-XE 17.6.6a
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	31/07/2025
Descripció	
Cisco Catalyst 9300L Series Switches	
Observacions	
CCN-STIC-1458 Procedimiento de Empleo Seguro CISCO Routers y Switches IOS-XE 17.X. La versió inicial qualificada va ser la 17.6 però després de la publicació de la vulnerabilitat pública [CVE-2023-20198], CISCO ha publicat una nova versió amb el fix (17.6.6a).	

Cisco Catalyst 9600 Series Switches (C9606R, C9600-SUP-1 y C9600-LC-24C|48YL|48TX|24S)	
Versió	IOS-XE 17.6.6a
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	31/07/2025
Descripció	
Cisco Catalyst 9600 Series Switches	
Observacions	
CCN-STIC-1450 Procedimiento de empleo Seguro de Catalyst 9000 y Catalyst IE3000. La versió inicial qualificada va ser la 17.6 però després de la publicació de la vulnerabilitat pública [CVE-2023-20198], CISCO ha publicat una nova versió amb el fix (17.6.6a).	

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

Versió	H3C Comware Software 7.1.070
Fabricant	New H3C Technologies Co., Ltd
Família	Switches
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	30/04/2026

Descripció

Els switches series de H3C són dispositius de xarxa dissenyats per a entorns empresarials, governamentals, educatius, financers o industrials que ofereixen una varietat de funcions per garantir connectivitat eficient i confiable. Els switches series de H3C proporcionen protocols de seguretat estandarditzats per a la gestió de la configuració.

Entre altres capacitats, els dispositius de switch de H3C inclouen una diversitat de ports, gestió d'energia eficient, qualitat de servei (QoS) per prioritzar el trànsit crític, VLAN per a segmentació de xarxa, mesures de seguretat avançades com control d'accés i autenticació, opcions d'apilament per augmentar la capacitat, eines de gestió remota i supervisió, compatibilitat amb IPv6 i característiques com el port mirall per facilitar el monitoratge i l'anàlisi de xarxa.

Observacions

CCN-STIC-1459 Procedimiento de empleo seguro Switches H3C

Huawei Cloud Engine 6800 (6881-48T6CQ)

Versió	V200R020C00SPC600 Patch V200R020SPH100T
Fabricant	Huawei Technologies Espanya
Família	Switches
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

Descripció

És un switch que proporciona serveis estables, fiables i d'alt rendiment en capa 2 i capa 3. Aquests switches estan dissenyats per a centres de dades i xarxes de campus d'alta gamma. Proporcionen alt rendiment, interfícies d'alta densitat i baixa latència. Tenen un disseny maquinari avançat que subministra ports d'alta densitat mentre fa servir la mateixa plataforma Software Huawei VRP.

Observacions

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

Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches IE-9310-26S2C-E|A, IE-9320-26S2C-E|A, IE9320-22S2C4X-E|A, IE-9320-24P4S-E|A, IE-9320-24T|P4X-E|A, IE-9320-16P8U4X-E|A

Versió	IOS-XE 17.9
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/01/2024
Revisió de Validesa	31/07/2024

Descripció

Els Catalyst Industrial Ethernet 9300 Rugged Sèries Switches són equips dissenyat per a entorns industrials exigents. Aquest switch és resistent i durador, capaç de suportar condicions extremes. Ofereix una connectivitat de confiança i segura per a dispositius industrials, com a càmeres de vigilància, sensors i controladors. Té múltiples ports Ethernet que permeten la connexió de diversos dispositius i garanteixen una comunicació fluida en la xarxa.

A més, són equips fàcils de configurar i administrar, la qual cosa ho fa adequat per a entorns industrials on es requereix una infraestructura de xarxa robusta i de confiança.

Observacions

Procediment d'ocupació assegurança pendent de publicació

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Product
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	IOS-XE 17.9
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

Descripció

Els Cisco Catalyst 9400X/9600X són switches de xarxa que ofereixen una alta densitat ports Ethernet per mòdul, incloent-hi opcions de PoE+. Estan dissenyats amb un potent processador i ofereixen serveis de xarxa avançats per a empreses que necessiten una xarxa segura i escalable. Són equips de xarxa d'alt rendiment. Ofereixen alta densitat de ports Ethernet per mòdul, amb opcions de 10 Gbps, 25 Gbps i 40 Gbps. Estan equipats amb un processador que proporciona una alta capacitat de processament i seguretat avançada.

Observacions

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

Cisco Catalyst 9300 Series Switches (C9300-24T|P|U|AUX|S|H, C9300-48T|P|U|UXM|UN|S|H, C9300D-24UB|UXB, C9300D-48UB) amb els següents mòduls de xarxa (C9300-NM-4G|8X|2Q|4M|2Y)	
Versió	IOS-XE 17.9 (amb 17.9.4a)
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	10/11/2023
Revisió de Validesa	30/04/2026

Descripció

Els Cisco Catalyst 9300y 9300L són switches de xarxa que ofereixen una alta densitat ports Ethernet per mòdul, incloent opcions de PoE+. Estan dissenyats amb un potent processador i ofereixen serveis de xarxa avançats per a empreses que necessiten una xarxa segura i escalable. Els Cisco Catalyst 9300L, la variant compacta de la Serie 9300, ideals per a petites i mitjanes empreses.

Observacions

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

Huawei CE Series Switches (CE6820H-48S6CQ , CE6860-HAM, CE6860-SAN, CE6863H-48S6CQ, CE6866-48S8CQ-P, CE6881H-48S6CQ, CE6881H-48T6CQ, CE8850-HAM, CE8850-SAN, CE8851-32CQ8DQ-P i CE16804)	
Versió	V300R022C00SPC200
Fabricant	Huawei Technologies Co., Ltd.
Família	Switches
Tipus	Producte
Data Inclusió	01/10/2023
Revisió de Validesa	31/03/2026

Descripció

És un switch que proporciona serveis estables, fiables i d'alt rendiment en capa 2 i capa 3. Aquests switches estan dissenyats per a centres de dades i xarxes de campus d'alta gamma. Proporcionen alt rendiment, interfícies d'alta densitat i baixa latència. Tenen un disseny maquinari avançat que subministra ports d'alta densitat mentre fa servir la mateixa plataforma Software Huawei VRP.

Observacions

CCN-STIC 1424 Procediment d'Ocupació Segur Huawei CE Series Switches

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	04/10/2025

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	04/10/2025

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	ArubaOS 16.11
Fabricant	HPE Aruba Networking
Família	Switches
Tipus	Producte
Data Inclusió	27/12/2023
Revisió de Validesa	30/06/2024

Descripció

Equips dissenyats per a utilitzar-se en labors d'accés i agregació, o nucli de xarxa d'accés. Són equips que proporcionen connexions de totes les velocitats i tipus de mitjans. Equips amb capacitat de commutació sense bloqueig (senar-blocking). Segons la família, ofereixen solucions escalables mitjançant constitució de stacks via port de xarxa, port dedicat així com existeixen models de xassissos. Totes les funcions del sistema operatiu s'ofereixen amb l'equip. Ofereixen diversos tipus d'interfícies i velocitats. Ofereixen PoE en alguns models, a diferents potències.

Poden són gestionables, tant localment (gestió on-premise) com poden arribar a administrar-se en modalitat Programari-as-a-Service.

Observacions

Procediment d'Ocupació Segura pendent de publicació

Dell EMC Networking SmartFabric (Models: S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, MX5108n, S4248FB-ON, S4248FBL-ON, S6010-ON, Z9100-ON, MX9116n, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9264F-ON i Z9332F-ON)

Versió	OS 10 Build: 10.5.1.3.
Fabricant	Dell Computer
Família	Switches
Tipus	Producte
Data Inclusió	01/12/2020
Revisió de Validesa	31/08/2024

Descripció

Dell EMC Smart Fabric OS10 és el sistema operatiu de xarxa (NOS) que s'utilitza en les famílies d'enrutadors i commutadors de les Serie N (alguns models), Serie S, Serie Z i Serie MX de Dell EMC Networking (les plataformes HW que actualment suporten OS10 són N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n i MX9116n). Dell EMC SmartFabric OS10 és un sistema operatiu de xarxa (NOS) que admet múltiples arquitectures i entorns. La solució SmartFabric OS10 permet la desagregació en diverses capes de la funcionalitat de xarxa. SmartFabric OS10 comprèn l'administració, monitoratge i funcionalitat completa i estàndard de la indústria de xarxes de nivell 2 i nivell 3 a través d'interfícies CLI, SNMP i REST. Els usuaris poden triar les seves pròpies aplicacions d'organització, gestió, supervisió i xarxes de tercers. Per desenvolupar xarxes escalables L2 i L3, SmartFabric OS10 ofereix una solució modular i desagregada en una única imatge binària.

Observacions

CCN-STIC-1429 PES DELL EMC Networking

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

Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	28/02/2026

Descripció

Família de commutadors L3 compactes apilables amb alta densitat de ports 1GE, Multigigabit ethernet 1/2.5 GigE i enllaços 10GE, dissenyats com a equips d'accés en xarxes convergents d'alta capacitat. https://www.al-enterprise.com/es-es/productos/conmutadores

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

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

Versió	V200R020C00SPC300 y V200R021C00SPC100
Fabricant	Huawei Technologies Espanya
Família	Switches
Tipus	Producte
Data Inclusió	01/03/2021
Revisió de Validesa	31/08/2024

Descripció

Els switches de la Serie-S de Huawei estan dissenyats per cobrir les necessitats 'evolució de la xarxa de campus. Entre les seves capacitats destaquen la gestió simplificada i l'alt rendiment. Poden ser utilitzats en qualsevol tipus de sector: empresarial, governamental, educatiu, financer o industrial.

Observacions

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

Alcatel-Lucent Enterprise OmniSwitch Serie 6900 (OS6900-X20, OS6900-X40, OS6900-T20, OS6900-T40, OS6900-X72, OS6900-Q32, OS6900-V72, OS6900-C32,OS6900-C32E, OS6900-X48C6, OS6900-T48C6, S6900-X48C4E, OS6900-V48C8, OS6900-X24C2, OS6900-T24C2)

Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	28/02/2026

Descripció

OS6900: Família de commutadors L3+ compactes apilables d'alta densitat 10GE, 25GE, 40GE i 100GE. Dissenyades perquè siguin flexibles. Poden instal·lar-se com a commutadors convergents situats en la part superior del bastidor (TOR) o tipus spine per a entorns de Data Centers i també com a dispositius d'agregació i de nucli en una xarxa de campus. https://www.al-enterprise.com/es és/productes/commutadors.

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6865 (OS6865-P16X, OS6865-U12X y OS6865-U28X)	
Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	28/02/2026
Descripció	

OS6865: Família de commutadors L3+ amb ports 1G i 10G, preparats per a entorn industrial o xarxes de missió crítica com a transports i utilities, amb ampli rang de temperatures de funcionament (-40 °C a +75 °C). https://www.al-enterprise.com/es-es/productos/conmutadores

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6860 (OS6860E-24, OS6860E-P24, OS6860E-48, OS6860E-P48, OS6860E-U28, OS6860E-P24Z8, TA6860E-P48, OS6860N-U28, OS6860N-P48Z, OS6860N-P48M, O6860NP24M, OS6860N-P24Z)	
Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	28/02/2026
Descripció	

OS6860: Família de commutadors L3+ compactes apilables amb alta densitat de ports 1GE, multigigabitethernet 1/2.5/5/10 GigE i enllaços 10GE, 25GE i 100GE, dissenyades per a xarxes convergents. Amb funcions d'Accés unificat avançades que permeten la creació de xarxes orientades a les aplicacions. Pot supervisar i controlar les aplicacions de la xarxa mitjançant capacitats de Deep Packet Inspection (DPI). https://www.al-enterprise.com/es-es/productos/conmutadores

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

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

Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	28/02/2026

Descripció

OS9900: Commutador LAN L3+ amb xassís modular d'alta capacitat d'interfícies 1GE, 10GE i 100GE per a commutació segura i amb alta disponibilitat en el nucli de les xarxes empresarials, campus i xarxes Metre Ethernet. https://www.al-enterprise.com/es-es/productos/conmutadores

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

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

Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	28/02/2026

Descripció

OS6465: Família de commutadors L2+ amb ports 1G i 10G, preparats per a entorn industrial, amb ampli rang de temperatures de funcionament (-40 °C a +75 °C). Dissenyats com a equips d'accés en xarxes de tipus industrial, transports o utilities. https://www.al-enterprise.com/es és/productes/commutadors

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

7.5.3. TALLAFOCS

Cisco ASA 5500 Series (5508-X and 5516-x)	
Versió	7.0
Fabricant	Cisco Systems
Família	Tallafocs
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
- FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observacions

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

CloudGuard Network (VMware ESXi/NSX)

Versió	R.81
Fabricant	Check Point Software Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	31/07/2025

Descripció

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

Cisco Firepower Threat Defense (FTD) a Firepower 1000 i 2100 Series (FP1010, FP1120, FP1140, FP2110, FP2120, FP2130, FP2140)

Versió	FTD 6.4 i FMC/FCMv 6.4
Fabricant	Cisco Systems
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).
Compatible amb:

- -Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
- -FMCv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220- M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S- M3 and UCS-E180D-M3

Observacions

CCN-STIC-651B Seguretat en tallafocs CISCO Firepower

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

Versió	6.5.4.4-44n-federal-12n
Fabricant	SonicWall
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/08/2021
Revisió de Validesa	28/02/2025

Descripció

La Serie TZ de SonicWall ofereix seguretat i rendiment d'entorn Enterprise orientat a petites companyies. Enfocat a entorns departamentals o PIMES d'entre 5 i 100 usuaris (aprox), incorpora funcions de prevenció d'intrusions, antimalware, filtratge de continguts/URL i control d'aplicacions a través de xarxes i entorns sense fil. Proporciona inspecció profunda de paquets (DPI), SD-WAN i desplegament zero-touch. Opcions de ports PoE i wifi 802.11ac. Més info a: https://www.sonicwall.com/es-mx/products/firewalls/entry-level

Observacions

CCN-STIC-1420 Procediment d'Ocupació Segur Sonicwall SonicOS

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

Versió	6.5.4.4-44n-federal-12n
Fabricant	SONICWALL
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/08/2021
Revisió de Validesa	28/02/2025

Descripció

La Serie TZ de SonicWall ofereix seguretat i rendiment d'entorn Enterprise orientat a petites companyies. Enfocat a entorns departamentals o PIMES d'entre 5 i 100 usuaris (aprox), incorpora funcions de prevenció d'intrusions, antimalware, filtratge de continguts/URL i control d'aplicacions a través de xarxes i entorns sense fil. Proporciona inspecció profunda de paquets (DPI), SD-WAN i desplegament zero-touch.

La Serie SOHO són una solució adequada per a oficines petites i domèstiques, així com per a entorns distribuïts en ubicacions remotes. Despleguen funcionalitats per construir Secure SD-WAN i connectivitat WIFI (opcional). El SOHO 250 proporciona un 50% més de rendiment sobre el seu antecessor SOHO, així com accés als sandboxes avançats Capture ATP, amb la qual cosa es millora la seguretat en prevenció i detecció de malware desconegut en un entorn remot.

La Serie NSa estan indicats per a companyies mitjanes / grans, empreses deslocalitzades geogràficament i datacenters, consolidant tecnologies automatitzades de prevenció i detecció d'amenaces com la inspecció de memòria profunda en temps real (RTDMI). Desenvolupats sobre una arquitectura de maquinari de múltiples nuclis amb interfícies 10-GbE i 2.5-GbE, la Serie NSa compta amb capacitats basades en el núvol i en l'equip, com desxifrat i inspecció TLS/SSL, application intelligence i control, SD-WAN segura, visualització en temps real i administració de WLAN.

La Serie SM està dedicada per a grans empreses, centres de dades, carriers i proveïdors de serveis amb necessitats multi-gigabit. Dirigit a companyies d'entre 1000 i més de 50.000 usuaris (aprox.), realitza detecció i prevenció d'amenaces mitjançant la combinació de la protecció basada en appliances amb la intel·ligència del núvol en una plataforma d'alt acompliment i consolida tecnologies de seguretat que brinden protecció contra amenaces a milions de connexions sense alentir l'acompliment.

Observacions

CCN-STIC-1420 Procediment d'Ocupació Segur Sonicwall SonicOS

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

Versió	R.81
Fabricant	Check Point Software Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	31/07/2025

Descripció

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

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

Versió	PA-OS v10.2
Fabricant	Palo Alto
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	29/02/2024

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

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

Versió	R.81
Fabricant	Check Point Software Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	31/07/2025

Descripció

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

Forcepoint NGFW 2200 series (N2201, N2205, N2210)

Versió	6.10
Fabricant	Forcepoint
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/04/2022
Revisió de Validesa	30/09/2024

Descripció

Firewalls de Nova Generació orientats a companyies o organismes de mida mitjana, de tipus appliance físic de 1RU, amb capacitats IPS, SD-WAN, URL Filtering i Detecció Avançada de Malware. Depenent del model concret de dispositiu es pot disposar d'un rendiment de 13,5 Gbps de Throughput NGFW/NGIPS, 35 milions de connexions concurrents i 100 contextos virtuals. Més informació a: https://www.forcepoint.com/environments/forcepoint-ngfw-appliances

Observacions

CCN-STIC-1409 Procediment d'ocupació segura tallafocs Forcepoint NGFW

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

Versió R.81

Fabricant Check Point Software Technologies

Família Tallafocs

Tipus Producte

Data Inclusió 01/02/2023

Revisió de Validesa 31/07/2025

Descripció

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

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

Versió V600R007C20SPC300 + V600R007C20SPH315T

Fabricant Huawei Technologies España

Família Tallafocs

Tipus Producte

Data Inclusió 01/12/2021

Revisió de Validesa 31/05/2024

Descripció

Els firewalls de nova generació de la Serie Huawei HiSecEngine estan dissenyats per a tota mena de empreses, institucions i centres de dades de propera generació. Els firewalls disposen de capacitats NGFW i s'integren amb altres dispositius de seguretat per defensar-se de manera proactiva contra amenaces de xarxa, millorar les capacitats de detecció i resoldre problemes de deteriorament del rendiment. Proporcionen capacitats d'acceleració de processament de serveis de xifrat/desxifrat millorant el rendiment dels firewalls, la detecció de seguretat i els serveis

IPSec.

Observacions

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

Checkpoint Security Gateway y Maestro Hyperscale Appliances (140, 154**, 156**, 175, 3600, 3800, 6200, 6400, 6600, 6700, 7000, 16000, 16200, 16600HS, 26000, 28000, 6600, 6700, 6900, 7000, 16600, 28600, 28600HS, Smart-1 525, Smart-1 660-S, Smart-1 660-M, Smart-1 6000-L, Smart-1 6000-XL, ESXi (HPE D360 G10))	
Versió	R.81
Fabricant	Check Point Software Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/06/2022
Revisió de Validesa	30/11/2024
Descripció	

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

FortiGate NGFW Appliances (FG40F, FG-60F, FWF-60F, FG-80F, FG-80F-PoE, FG-90G, FG-91G, FG-200F, FG-1100E, FG-1800F, FG-1800F-0DC, FG-2200E, FG-2600F, FG-2600F-0DC, FG-3300E, FG-3400E, FG-3400E0DC, FG-4200F, FG-4200F-0DC, FG-4400F, FG-4400F-0DC)	
Versió	FortiOS 6.4
Fabricant	Fortinet
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	30/09/2024
Descripció	

Firewalls de Nova Generació amb capacitats d'inspecció en capa 7, IPS i concentrador VPN IPSEC. Les funcionalitats de seguretat més destacables són: reconeixement d'aplicacions i usuaris de la xarxa, protecció enfront de malware conegut, amenaces avançades i atacs zero-day, protecció enfront de botnets, filtre de navegació web, protecció DoS, proxy explícit, Inspecció SSL, capacitats SDWAN, VPN (IPSEC i SSL), control d'Access Points, LTE/5G i Switches, etc. Més informació a: https://docs.fortinet.com/product/fortigate/6.4

Observacions

CCN-STIC 1406 Procediment d'ocupació assegurança Tallafocs FortiGate

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

Versió	PAN-OS v10.2
Fabricant	Palo Alto
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2025

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa que s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

WatchGuard Fireware on Firebox NGFWs (T25, T45, T85, M290, M390, M590, M590, M690, M4800, M5800

Versió	FirewareOS 12.6
Fabricante	TecHnologies WatchGuard
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	30/05/2025

Descripció

Els equips UTM de WatchGuard estan enfocats a oferir la millor seguretat per a qualsevol empresa i entorn corporatiu distribuït. Els nostres dispositius de seguretat de xarxa estan dissenyats, des de l'inici, per enfocar-se a facilitar el desplegament, l'ús i l'administració contínua. Proporcionen protecció contra atacs de malware avançat i phishing, així com les proteccions de seguretat tradicionals: prevenció d'intrusions (IPS), filtratge d'URL, control d'aplicacions, antispam i antivirus, oferint en tot moment visibilitat de l'entorn (productivitat i seguretat) Compten amb capacitats SD-WAN, i VPN. Estan disponibles tant en equips físics com virtuals. https://www.watchguard.com/es/wgrd-products/network-security

Observacions

CCN-STIC-1421 Procedimiento de empleo seguro WatchGuard Fireware

SRX1500, SRX4100, SRX4200, SRX4600

Versió	Juns OS 19.2R1
Fabricant	Juniper Networks
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/10/2022
Revisió de Validesa	30/09/2024

Descripció

El firewall SRX4600 de Juniper Networks® protegeix les xarxes de centres de dades i campus de missió crítica per a empreses, proveïdors de serveis mòbils i proveïdors de serveis al núvol. Està dissenyat per a arquitectures de serveis de seguretat d'alt rendiment i protegeix els actius de TI corporatius crítics com un firewall de pròxima generació (NGFW). A més, actua com un punt de compliment per a les solucions de seguretat basades en el núvol i proporciona visibilitat i control d'aplicacions per millorar l'usuari i l'aplicació. experiència. En integrar xarxes i seguretat en una sola plataforma, el SRX4600 compta amb múltiples interfícies d'alta velocitat, prevenció d'atacs, protecció avançada contra amenaces i autenticació, juntament amb capacitats d'IPsec d'alt rendiment. També ofereix alta escalabilitat, alta disponibilitat, protecció robusta, visibilitat d'aplicacions, identificació d'usuaris i inspecció profunda de contingut per proporcionar un control sense igual sobre la infraestructura de seguretat.

El SRX4600 també actua com un punt de compliment central, aprofitant l'automatització per protegir els usuaris en un entorn de xarxa de múltiples proveïdors. Així mateix, ofereix SD-WAN totalment automatitzat tant per a empreses com per a proveïdors de serveis. A causa del seu alt rendiment i escala, el SRX4600 actua com un concentrador de VPN i finalitza les connexions superposades segures/VPN en diverses topologies SD-WAN.

Observacions

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

ISA 3000 (ISA 3000-4C and ISA 3000-2C2F)	
Versió	FTD 7.0 y FMC/FMCv 7.0
Fabricant	Cisco Systems
Família	Tallafocs
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	30/04/2026
Descripció	

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Observacions

CCN-STIC 651B Seguretat a Cortafocs Cisco Firepower

SRX1600, SR2300, SRX4300

Versió	Juns OS 19.2R1
Fabricant	Juniper Networks
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/10/2022
Revisió de Validesa	30/09/2024

Descripció

El firewall SRX4600 de Juniper Networks® protegeix les xarxes de centres de dades i campus de missió crítica per a empreses, proveïdors de serveis mòbils i proveïdors de serveis al núvol. Està dissenyat per a arquitectures de serveis de seguretat d'alt rendiment i protegeix els actius de TI corporatius crítics com un firewall de pròxima generació (NGFW). A més, actua com un punt de compliment per a les solucions de seguretat basades en el núvol i proporciona visibilitat i control d'aplicacions per millorar l'usuari i l'aplicació. experiència. En integrar xarxes i seguretat en una sola plataforma, el SRX4600 compta amb múltiples interfícies d'alta velocitat, prevenció d'atacs, protecció avançada contra amenaces i autenticació, juntament amb capacitats d'IPsec d'alt rendiment. També ofereix alta escalabilitat, alta disponibilitat, protecció robusta, visibilitat d'aplicacions, identificació d'usuaris i inspecció profunda de contingut per proporcionar un control sense igual sobre la infraestructura de seguretat.

El SRX4600 també actua com un punt de compliment central, aprofitant l'automatització per protegir els usuaris en un entorn de xarxa de múltiples proveïdors. Així mateix, ofereix SD-WAN totalment automatitzat tant per a empreses com per a proveïdors de serveis. A causa del seu alt rendiment i escala, el SRX4600 actua com un concentrador de VPN i finalitza les connexions superposades segures/VPN en diverses topologies SD-WAN.

Observacions

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

FortiGate NGFW VM64	
Versió	FortiOS 6.4
Fabricant	Fortinet
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	30/09/2025

Descripció

Firewalls de Nova Generació amb capacitats d'inspecció en capa 7, IPS i concentrador VPN IPSEC.

Les funcionalitats de seguretat més destacables són: reconeixement d'aplicacions i usuaris de la xarxa, protecció enfront de malware conegut, amenaces avançades i atacs zero-day, protecció enfront de botnets, filtre de navegació web, protecció DoS, proxy explícit, Inspecció SSL, capacitats SDWAN,

VPN (IPSEC i SSL), control d'Access Points, LTE/5G i Switches, etc. Més informació a: https://docs.fortinet.com/product/fortigate/6.4

Observacions

CCN-STIC 1406 Procediment d'ocupació assegurança Tallafocs FortiGate

Next-Generation Firewall with PAN-OS PA-200 Series (PA-220, PA220R), PA-400, PA-800 Series (PA-820, PA850), PA-3200 Series (PA-3220, PA3250, PA3260), PA-5200 Series (PA-5220, PA5250, PA5260, PA5280), PA-5450, PA-7000 Series (PA-7050, PA7080), VM-Series (VM-50, VM-100, VM-300, VM-500, VM-700, VM-1000HV)	
Versió	FortiOS 6.4
Fabricant	Fortinet
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	30/09/2025

Descripció

Firewalls de Nova Generació amb capacitats d'inspecció en capa 7, IPS i concentrador VPN IPSEC.

Les funcionalitats de seguretat més destacables són: reconeixement d'aplicacions i usuaris de la xarxa, protecció enfront de malware conegut, amenaces avançades i atacs zero-day, protecció enfront de botnets, filtre de navegació web, protecció DoS, proxy explícit, Inspecció SSL, capacitats SDWAN,

VPN (IPSEC i SSL), control d'Access Points, LTE/5G i Switches, etc. Més informació a: https://docs.fortinet.com/product/fortigate/6.4

Observacions

CCN-STIC 1406 Procediment d'ocupació assegurança Tallafocs FortiGate

Cortafuegos SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC y SRX380

Versió	Juns OS 20.4R1
Fabricant	Juniper Networks
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2025

Descripció

La línia SRX300 de firewalls proporciona capacitats de seguretat, xarxes i SD-WAN de pròxima generació per a satisfer les necessitats canviants de la seva xarxa empresarial basada en la IA i habilitada per al núvol. La gestió del SRX300 a través de l'arquitectura en el núvol Juniper Mist simplifica les operacions de les seves sucursals. Tant si està afegint noves aplicacions en diverses ubicacions, connectant-se al núvol o esforçant-se per millorar l'eficiència operativa, el SRX300 pot ajudar-lo amb una connectivitat escalable, segura i fàcil de gestionar.

El SRX300 admet funcions de firewall de nova generació com a prevenció d'intrusions, visibilitat i control d'aplicacions i funcions de seguretat de continguts que inclouen antivirus, antispam i filtrat Web millorat.Advanced Threat Prevention proporciona una defensa integral enfront d'amenaces amb detecció dinàmica de malware, fonts d'amenaces de SecIntel, Juniper Encrypted Traffic Insights i Juniper Adaptive Threat Profiling.

Observacions

CCN-STIC-1442 PES Cortafuegos Juniper SRX

Aruba Mobility Controller (9004, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280) i punts d'accés.

Versió	ArubaOS 8.6
Fabricant	Aruba
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/07/2021
Revisió de Validesa	30/06/2024

Descripció

Les famílies Aruba Mobility Controllers 7000´s, 7200´s, 9000s i les Virtual Mobility Controller (appliance virtual) juntament amb els punts d'accés de les famílies 500s, 300s i 200s permeten desplegar xarxes sense fil de màxima seguretat i rendiment. Amb aquesta versió se suporta també WPA3 i Wifi6/802.11ax (amb les famílies 500s) així com WiFi-5/802.1ac i Wifi-4/802.11n. S'implementen avançades característiques de seguretat, en el control d'accés a la xarxa, així com en l'assignació de polítiques de seguretat. També se suporten mecanismes de monitoratge d'espectre. Els Punts d'Accés en mode poden treballar en mode Campus (CAP) i mode Remot (RAP), la qual cosa permet connectar de forma segura punts d'accés que creuen xarxes alienes com internet). S'implementen millores en actualitzacions de Software sense pèrdua de servei. Aruba Multizona permet a un Punt d'Accés donar servei a diverses Mobility Controllers de diferents dominis o entorns de seguretat. Els Mobility Controllers pot actuar com a servidors de túnels IPSEC/SSL per al client Aruba VIA.

Observacions

CCN-STIC 1431 Procediment d'Ocupació Assegurança ArubaOS 8.6. Controladores i Punts d'Accés

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

Versió	ArubaOS 8.10
Fabricant	Aruba
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/07/2021
Revisió de Validesa	30/06/2024

Descripció

Les famílies Aruba Mobility Controllers 7000´s, 7200´s, 9000s i les Virtual Mobility Controller (appliance virtual) juntament amb els punts d'accés de les famílies 500s, 300s i 200s permeten desplegar xarxes sense fil de màxima seguretat i rendiment. Amb aquesta versió se suporta també WPA3 i Wifi6/802.11ax (amb les famílies 500s) així com WiFi-5/802.1ac i Wifi-4/802.11n. S'implementen avançades característiques de seguretat, en el control d'accés a la xarxa, així com en l'assignació de polítiques de seguretat. També se suporten mecanismes de monitoratge d'espectre. Els Punts d'Accés en mode poden treballar en mode Campus (CAP) i mode Remot (RAP), la qual cosa permet connectar de forma segura punts d'accés que creuen xarxes alienes com internet). S'implementen millores en actualitzacions de Software sense pèrdua de servei. Aruba Multizona permet a un Punt d'Accés donar servei a diverses Mobility Controllers de diferents dominis o entorns de seguretat. Els Mobility Controllers pot actuar com a servidors de túnels IPSEC/SSL per al client Aruba VIA.

Observacions

CCN-STIC 1431 Procediment d'Ocupació Assegurança ArubaOS 8.6. Controladores i Punts d'Accés

Check Point Security Gateway Serie 7000 (CPAP-SG7000)

Versió	R.81
Fabricant	Check Point Software Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	31/07/2025

Descripció

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

Servidors de Gestió Smart-1 (CPAP-NGSM-405, CPAP-NGSM-410, CPAP-NGSM-625, CPAP-NGSM-5050, CPAP-NGSM-5150)

Versió	R.81
Fabricant	Check Point Software Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	31/07/2025

Descripció

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

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

Versió	R.81
Fabricant	Check Point Software Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	31/07/2025

Descripció

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

Check Point Security Gateway Serie 23000 (CPAP-SG23500, CPAP-SG23800, CPAP-SG23900)

Versió	R.81
Fabricant	Check Point Software Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	31/07/2025

Descripció

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

Check Point Security Gateway Serie 16000 (CPAP-SG16000, CPAP-SG16200, CPAP-SG16600HS)

Versió	R.81
Fabricant	Check Point Software Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	31/07/2025

Descripció

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

Check Point Security Threat Emulation/Extraction (CPAP-SBTE250XN i CPAP-SBTE2000XN)

Versió	R.81
Fabricant	Check Point Software Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	31/07/2025

Descripció

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

Check Point Security Gateway Serie 26000 i 28000 (CPAP-SG26000, CPAP-SG28000, CPAP-SG28600)

Versió	R.81
Fabricant	Check Point Software Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	31/07/2025

Descripció

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

PA-400 Series (PA-410, PA-440, PA-450, PA-460)

Versió	PA-OS v10.2
Fabricant	Palo Alto
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2025

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

FTD Virtual (FTDv) sobre ESXi 6.7 or 7.0 en Cisco Unified Computing System (UCS) - UCSC-C220-M5, UCSCC240-M5, UCSC-C480-M5, UCS-E160S-M3 y UCS-E180D-M3 instalado en ISR

Versió	FTD 7.0 y FMC/FMCv 7.0
Fabricant	Cisco Systems
Família	Tallafocs
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	30/04/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtrat de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
- FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observacions

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

PA-800 Series (PA-820, A-850)

Versió	PA-OS v10.2
Fabricant	Palo Alto
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2025

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

Check Point Maestro Hyperscale Appliances (CPAP-MHO-140, CPAP-MHO-175-xC)

Versió	R.81
Fabricant	Check Point Software Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	31/07/2025

Descripció

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

PA-3400 Series (PA-3410, PA-3420, PA-3430, PA-3440)

Versió	PA-OS v10.2
Fabricant	Palo Alto
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	29/02/2024

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

Forcepoint NGFW 3400 series (N3401, N3405, N3410)

Versió	6.10
Fabricant	Forcepoint
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/04/2022
Revisió de Validesa	30/09/2024

Descripció

Firewalls de Nova Generació orientats a grans xarxes Campus i Datacenters, de tipus appliance físic de 2RU, IPS, SD-WAN, URL Filtering i Detecció Avançada de Malware. Depenent del model concret de dispositiu es pot disposar de fins a un rendiment de 35 Gbps de Throughput NGFW/NGIPS, 200 milions de connexions concurrents i 250 contextos virtuales. Més informació en: https://www.forcepoint.com/environments/forcepoint-ngfw-appliances

Observacions

CCN-STIC-1409 Procediment d'ocupació segura tallafocs Forcepoint NGFW

Forcepoint Virtual Appliance (ESXi)

Versió	6.10
Fabricant	Forcepoint
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/04/2022
Revisió de Validesa	30/09/2024

Descripció

Firewalls de Nova Generació orientats a donar serveis de protecció perimetral en entorns virtuals, IPS, SD-WAN, URL Filtering i Detecció Avançada de Malware. Depenent del nombre de vCPU assignats es va poderdisposar d'un rendiment de més de 10GB Gbps de Throughput NGFW/NGIPS. Més informació a: https://www.forcepoint.com/environments/forcepoint-ngfw-appliances

Observacions

CCN-STIC-1409 Procediment d'ocupació segura tallafocs Forcepoint NGFW

Forcepoint NGFW N120 series (N120, N120W, N120WL) i N60

Versió	6.10
Fabricant	Forcepoint
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/04/2022
Revisió de Validesa	30/09/2024

Descripció

Firewalls de Nova Generació orientats a protegir oficines remotes o entorns SD-WAN de tipus appliance físic amb format sobretaula, amb capacitats IPS, SD-WAN, URL Filtering i Detecció Avançada de Malware. Depenent del model concret de dispositiu es pot disposar un rendiment fins a 450mbps de Throughput NGFW/NGIPS i 3,2 milions de connexions concurrents. Més informació a: https://www.forcepoint.com/environments/forcepoint-ngfw-appliances

Observacions

CCN-STIC-1409 Procediment d'ocupació segura tallafocs Forcepoint NGFW

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

Versió	FTD 7.0 y FMC 7.0
Fabricant	Cisco Systems
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/11/2022
Revisió de Validesa	30/04/2025

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Compatible amb:

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 i FMC4600-K9)
- FMCv executant-se en ESXi 6.0 o 6.5 en el Sistema Unificat de Computació (UCS) UCSB-B200-M4, UCSC-C220- M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S- M3 i UCS-E180D-M3

Observacions

CCN-STIC-651B Seguretat a Cortafocs Cisco Firepower

Servidors de Gestió Smart-1 600 and 6000 series (CPAP-NGSM600S-X, CPAP-NGSM600M-X, CPAP-NGSM6000L-X, CPAP-NGSM6000XL-X	
Versió	R.81
Fabricant	Check Point Software Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	31/07/2025

Descripció

Són dispositius dedicats que poden realitzar inspecció a nivell de xarxa, d'aplicació i d'amenaça avançada, ja sigui virus, botnet, ramsonware o zero-day. Ofereix fins a 128Gbps d'inspecció Firewall, 26Gbps d'IPS i 20 Gbps per a protecció davant amenaces avançades. Un màxim de 51,2 milions de connexions concurrents i 400.000 de noves per segon.

Per a més informació: https://www.checkpoint.com/downloads/products/check-point-appliance- comparison-chart.pdf

Observacions

CCN-STIC 653 Seguretat a Check Point

WatchGuard Fireware on Firebox NGFWs (T35, T40, T80, T55, M270, M370, M470, M570, M670, M4600 y M5600)	
Versió	FirewareOS 12.6
Fabricant	WatchGuard Technologies
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	30/05/2025

Descripció

Els equips UTM de WatchGuard estan enfocats a oferir la millor seguretat per a qualsevol empresa i entorn corporatiu distribuït. Els nostres dispositius de seguretat de xarxa estan dissenyats, des del inici, per enfocar-se a facilitar el desplegament, l'ús i l'administració contínua. Proporcionen protecció contra atacs de malware avançat i phishing, així com les proteccions de seguretat tradicionals: prevenció d'intrusions (IPS), filtratge d'URL, control d'aplicacions, antispam i antivirus, ... oferint en tot moment visibilitat de l'entorn (productivitat i seguretat) Compten amb capacitats SD-WAN, i VPN. Estan disponibles tant en equips físics com virtuals.

https://www.watchguard.com/es/wgrd-products/network-security

Observacions

CCN-STIC-1421 Procediment d'ocupació assegurança WatchGuard Fireware OS v12.6.2

PA-3200 Series (PA-3220, PA-3250, PA-3260	
Versió	PAN-OS v10.2
Fabricant	Palo Alto
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2025

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

PA-220 Series (PA-220, PA-220R)	
Versió	PAN-OS v10.2
Fabricant	Palo Alto
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2025

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa que s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

PA-7000 Series (PA-7050, PA-7080)

Versió PAN-OS v10.2

Fabricant Palo Alto

Família Tallafocs

Tipus Producte

Data Inclusió 01/06/2023

Revisió de Validesa 30/11/2025

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa que s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

VM-Series (VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000-HV

Versió PAN-OS v10.2

Fabricant Palo Alto

Família Tallafocs

Tipus Producte

Data Inclusió 01/06/2023

Revisió de Validesa 30/11/2025

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa que s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

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

Versió	7.0
Fabricant	Cisco Systems
Família	IDS, IPS i AntiDDoS
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Compatible amb:

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 i FMC4600-K9)
- FMCv executant-se en ESXi 6.0 o 6.5 en el Sistema Unificat de Computació (UCS) UCSB-B200-M4, UCSC-C220- M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S- M3 i UCS-E180D-M3

Observacions

CCN-STIC 651B Seguretat a Cortafocs Cisco Firepower

FTD Virtual (FTDv) sobri NFVIS 4.4 en ENCS 5406, 5408, i 5412

Versió	FTDv 7.0 y FMC/FMCv 7.0
Fabricant	Cisco Systems
Família	Tallafocs
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	30/04/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Compatible amb:

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 i FMC4600-K9)
- FMCv executant-se en ESXi 6.0 o 6.5 en el Sistema Unificat de Computació (UCS) UCSB-B200-M4, UCSC-C220- M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S- M3 i UCS-E180D-M3

Observacions

Pendent de Publicació de Procediment d'ocupació assegurança

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

Versió	7.0
Fabricant	Cisco Systems
Família	Tallafocs
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Observacions

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

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

Versió	7.0
Fabricant	Cisco Systems
Família	Tallafocs
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Observacions

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

OpnSense

Versió	21.7
Fabricant	Deciso B.V
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/03/2022
Revisió de Validesa	31/08/2024

Descripció

OPNsense és una plataforma d'encaminament i tallafocs basada en un sistema operatiu BSD de codi obert fortificat, fàcil d'usar i implantar.

Es tracta d'un tallafocs amb estat, és a dir, un tallafocs que fa un seguiment de l'estat de les connexions de xarxa (com a fluxos TCP, comunicació UDP) que viatgen a través d'ell. El producte ofereix una agrupació de regles de tallafocs per categoria, una característica excel·lent per a les configuracions de xarxa més exigents.

OPNsense inclou la majoria de les funcions disponibles en els tallafocs comercials i més en molts casos amb els beneficis del programari de codi obert i verificable.

Observacions

CCN-STIC-1453 Procediment d'Ocupació Segur Tallafocs OPNSense

FortiGate NGFW Appliances (FG-61E, FG-61F, FWF-61E, FWF-61F, FG-81E, FG-81E-PoE, FG-81F, FG-81F-2R, FG-81F-2R-3G4G-PoE, FG-81F-2R-PoE, FG-81F-PoE, FG-90E, FG-91E)	
Versió	FortiOS 6.4
Fabricant	Fortinet
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	30/09/2024

Descripció

Firewalls de Nova Generació amb capacitats d'inspecció en capa 7, IPS i concentrador VPN IPSEC.

Les funcionalitats de seguretat més destacables són: reconeixement d'aplicacions i usuaris de la xarxa, protecció enfront de malware conegut, amenaces avançades i atacs zero-day, protecció enfront de botnets, filtre de navegació web, protecció DoS, proxy explícit, Inspecció SSL, capacitats SDWAN,

VPN (IPSEC i SSL), control d'Access Points, LTE/5G i Switches, etc. Més informació a: https://docs.fortinet.com/product/fortigate/6.4

Observacions

CCN-STIC 1406 Procediment d'ocupació assegurança Tallafocs FortiGate

FortiGate NGFW Appliances (FG-100F, FG-101E, FG-101F, FG-201E, FG-201F, FG-301E, FG400F, FG-401E, FG401F, FG-501E, FG-600F, FG-601E, FG-601F)	
Versió	FortiOS 6.4
Fabricant	Fortinet
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	30/09/2025

Descripció

Firewalls de Nova Generació amb capacitats d'inspecció en capa 7, IPS i concentrador VPN IPSEC.

Les funcionalitats de seguretat més destacables són: reconeixement d'aplicacions i usuaris de la xarxa, protecció enfront de malware conegut, amenaces avançades i atacs zero-day, protecció enfront de botnets, filtre de navegació web, protecció DoS, proxy explícit, Inspecció SSL, capacitats SDWAN,

VPN (IPSEC i SSL), control d'Access Points, LTE/5G i Switches, etc. Més informació a: https://docs.fortinet.com/product/fortigate/6.4

Observacions

CCN-STIC 1406 Procediment d'ocupació assegurança Tallafocs FortiGate

FortiGate NGFW Appliances (FG-1101E, FG-1801F, FG-1801F-DC, FG-2000E, FG-2201E, FG-2500E, FG-2601F, FG-2601F-DC, FG-3301E, FG-3401E, FG-3401E-DC, FG-3601E, FG-4201F, FG-4201F-DC, FG-4401F, FG-4401F-DC, FG-5001E1, FG-6300F, FG-6301F, FG-6500F, FG-6501F)	
Versió	FortiOS 6.4
Fabricant	Fortinet
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	30/09/2025

Descripció

Firewalls de Nova Generació amb capacitats d'inspecció en capa 7, IPS i concentrador VPN IPSEC.

Les funcionalitats de seguretat més destacables són: reconeixement d'aplicacions i usuaris de la xarxa, protecció enfront de malware conegut, amenaces avançades i atacs zero-day, protecció enfront de botnets, filtre de navegació web, protecció DoS, proxy explícit, Inspecció SSL, capacitats SDWAN,

VPN (IPSEC i SSL), control d'Access Points, LTE/5G i Switches, etc. Més informació a: https://docs.fortinet.com/product/fortigate/6.4

Observacions

CCN-STIC 1406 Procediment d'ocupació assegurança Tallafocs FortiGate

OpnSense Business Edition

Versió	23.4
Fabricant	Deciso B.V
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/08/2022
Revisió de Validesa	31/08/2024

Descripció

OPNsense és una plataforma d'enrutament i tallafocs basada en un sistema operatiu BSD de codi obert fortificat, fàcil d'usar i implantar.

Es tracta d'un tallafocs amb estat, és a dir, un tallafocs que fa un seguiment de l'estat de les connexions de xarxa (com fluxos TCP, comunicació UDP) que viatgen a través d'ell. El producte ofereix una agrupació de regles de tallafocs per categoria, una característica excel·lent per a les configuracions de xarxa més exigents.

OPNsense inclou la majoria de les funcions disponibles en els tallafocs comercials i més en molts casos amb els beneficis del Software de codi obert i verificable.

Subministra les següents funcionalitats de seguretat:

- Protecció davant el trànsit de xarxa extern a través de la limitació dels paquets entrants seguint política aplicada.
- Limitació de l'accés a la xarxa externa des de la xarxa interna, de manera que només es permeti a aquells dispositius o usuaris especificats en la política de seguretat aplicada.

Pel que fa a la versió estàndard, aquesta versió dona accés a un repositori millorat d'actualitzacions Business Edition i plugins extra.

Observacions

CCN-STIC-1453 Procediment d'Ocupació Segur Tallafocs OPNSense

SonicWall SOHO Serie (250, 250W)

Versió	6.5.4.4-44n-federal-12n
Fabricant	SonicWall
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/08/2021
Revisió de Validesa	28/02/2025

Descripció

Els tallafocs de la Serie TZ SOHO de Sonicwall són una solució adequada per a oficines petites i domèstiques, així com per a entorns distribuïts en ubicacions remotes. Despleguen funcionalitats per a construir Secure SD-WAN i connectivitat WIFI (opcional). El SOHO 250 proporciona un 50% més de rendiment sobre el seu antecessor SOHO, així com accés als sandboxes avançats Capture ATP, amb el que es millora la seguretat en prevenció i detecció de malware desconegut en un entorn remot.

Observacions

CCN-STIC-1420 Procediment d'Ocupació Segur Sonicwall SonicOS

Stormshield Network Security UTM/NG-Firewall (Appliances desde SN200 a SN6100 en 4 compilaciones distintas: S, M, L y XL).

Versió	3.11.LTSB
Fabricant	Stormshield SAS
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/12/2022
Revisió de Validesa	30/06/2024

Descripció

Firewalls de nova generació de capa 7, IPS i concentrador de túnels VPN. Amb capacitats de bloqueig d'amenaces avançades, atacs de dia zero, filtratge de navegació web o gestió de vulnerabilitats.

El mateix equipament realitza inspecció profunda de protocols OT, a més d'IT.

Observacions

CCN-STIC-1415 Procediment d'Ocupació Segur Tallafocs UTMNG Stormshield

7.5.4. PROXIES

Symantec WPS

Versió

Fabricant Symantec a division of Broadcom

Família Proxies

Tipus Producte

Data Inclusió 01/02/2024

Revisió de Validesa 31/07/2024

Descripció

Web Protecció Suite de Symantec és una solució integral de seguretat en el núvol dissenyat per a salvaguardar a les empreses contra les amenaces en línia. Aquesta suite ofereix un proxy web segur que opera en el núvol i es connecta als dispositius dels usuaris a través d'un túnel xifrat, garantint la protecció dels dispositius i dades corporatives durant la navegació per Internet. Web Protecció Suite de Symantec ofereix una àmplia gamma de característiques de seguretat, entre les quals s'inclouen el filtrat de contingut, la detecció d'amenaces, la prevenció d'intrusions i el compliment normatiu. El filtrat de contingut ajuda a bloquejar l'accés a llocs web maliciosos o inapropiats, mentre que la detecció d'amenaces utilitza avançades tècniques d'anàlisis per a identificar i neutralitzar les amenaces en temps real. La prevenció d'intrusions protegeix contra atacs de xarxa i la violació de dades, mentre que el compliment normatiu ajuda a les empreses a complir amb les regulacions i estàndards de seguretat. A més, Web Protecció Suite ofereix funcionalitats addicionals, com el control d'accés a aplicacions i serveis en el núvol, Web Isolation i Sandboxing Així mateix, proporciona una visibilitat detallada i un control granular de les activitats en línia dels usuaris, la qual cosa permet a les empreses detectar i abordar ràpidament qualsevol activitat sospitosa. A més, Web Protecció Suite s'integra fàcilment amb altres solucions de seguretat, com firewalls, sistemes de detecció d'intrusos i sistemes de gestió d'amenaces, per a proporcionar una protecció completa i una resposta ràpida davant qualsevol amenaça.

Observacions

Procediment d'ocupació segura pendent de publicació.

Zscaler Work from Anywhere

Versió	ZIA Agent 4.2.0.178
Fabricant	Zscaler Spain, S.L
Família	Proxies
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	30/06/2025

Descripció

Zscaler és una plataforma de seguretat al núvol que proporciona un proxy web segur per protegir les empreses de les amenaces en línia. El proxy de Zscaler s'executa al núvol i es connecta a través d'un túnel xifrat als dispositius dels usuaris, cosa que permet a les empreses protegir els seus dispositius i dades mentre els usuaris accedeixen a Internet.

El proxy de Zscaler ofereix diverses característiques de seguretat, incloent filtrat de contingut, detecció d'amenaces, prevenció d'intrusions i compliment normatiu. El filtratge de contingut ajuda a evitar l'accés a llocs web maliciosos o inapropiats, mentre que la detecció d'amenaces utilitza tècniques avançades d'aprenentatge automàtic per identificar i bloquejar les amenaces en temps real. La prevenció d'intrusions ajuda a protegir contra atacs de xarxa i la violació de dades, mentre que el compliment normatiu ajuda les empreses a complir amb les regulacions i estàndards de seguretat.

A més, el proxy de Zscaler també ofereix característiques addicionals, com la capacitat de controlar l'accés a aplicacions i serveis al núvol, la protecció contra el robatori d'identitat i el filtratge de correu electrònic. També proporciona una visibilitat detallada i un control granular de les activitats en línia dels usuaris, la qual cosa permet a les empreses detectar i abordar ràpidament qualsevol activitat sospitosa.

A més, Zscaler ofereix una integració amb altres solucions de seguretat, com firewalls, sistemes de detecció d'intrusos i sistemes de gestió d'amenaces, la qual cosa permet una protecció més completa i una resposta més ràpida a les amenaces.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

Fortinet FortiProxy	
Versió	2.0
Fabricant	Fortinet
Família	Proxies
Tipus	Producte
Data Inclusió	01/07/2020
Revisió de Validesa	15/05/2025

Descripció

A mesura que les ciberassetjaments es van fent més sofisticades, les companyies necessiten cada vegada més una aproximació integral per protegir els usuaris del tràfic web maliciós, els websites perillosos i aquell contingut que pugui suposar una amenaça per a ells i les seves organitzacions. El Secure Web Gateway (SWG) de Fortinet (FortiProxy) aborda aquesta situació amb un únic producte que inclou filtrat d'URL, protecció contra amenaces avançades i malware, filtrat de DNS, DLP, IPS.... La protecció dels usuaris contra amenaces procedents d'Internet facilita el compliment de les polítiques corporatives tant normatives com de seguretat.

Observacions

CCN-STIC-1425 PES FortiProxy

Fortinet FortiProxy	
Versió	8.5
Fabricant	Forcepoint
Família	Proxies
Tipus	Producte
Data Inclusió	01/05/2021
Revisió de Validesa	31/10/2024

Descripció

Els dispositius Forcepoint Web Security realitzen la funció de proxy de navegació segura integrant múltiples motors de classificació de continguts i anàlisis de seguretat en temps real amb capacitat d'inspecció de trànsit segur i també anàlisi de dades sortints amb capacitat per a aplicar polítiques enfront de fugides d'informació. Les plataformes funcionen com proxies directes http, https, ftp i SOCKS per a la protecció i control d'usuaris i llocs de connexió. El propòsit d'aquests dispositius és proporcionar una capa de seguretat entre la xarxa Interna i una o més xarxes externes (típicament una xarxa corporativa i Internet), aïllant el trànsit dels usuaris a nivell d'aplicació i proporcionant a més diferents mecanismes d'optimització WAN per al trànsit que processen.

Observacions

CCN-STIC-1507 Procedimiento de Empleo Seguro Forcepoint On-premise Security 8.5

7.5.5. DISPOSITIUS DE XARXA SENSE FILS

Cisco Aironet 3800 Series Access Points (AIR-AP3802I-x-K9, AIR-AP3802I-x-K9C, AIR-AP3802e-x-K9, AIR- AP3802E-x-K9C, AIR-AP3802p-x-K9 i AIR-AP3802p-x-K9C)

Versió	IOS-XE versió 17.6
Fabricant	Cisco Systems
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Categoria ENS	ALTA
Data Inclusió	01/08/2023
Revisió de Validesa	31/07/2024

Descripció

Els dispositius Cisco Wireless LAN combinen plataformes específiques de Controlador i Punt d'Accés per crear un Sistema d'Accés WLAN. Aquests dispositius proporcionen als usuaris sense fil accés segur a la xarxa de l'organització.

Observacions

Procediment d'ocupació assegurança pendent de publicació

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

Versió	IOS-XE 17.6
Fabricant	Cisco Systems
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/07/2024

Descripció

Els dispositius Cisco Wireless LAN combinen plataformes específiques de Controlador i Punt d'Accés per crear un Sistema d'Accés WLAN. Aquests dispositius proporcionen als usuaris sense fil accés segur a la xarxa de l'organització.

Observacions

Procediment d'ocupació assegurança pendent de publicació

Aruba Mobility Controller (9004, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280) i punts d'accés.

Versió	ArubaOS 8.6
Fabricant	Aruba
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/07/2021
Revisió de Validesa	30/06/2024

Descripció

Les famílies Aruba Mobility Controllers 7000´s, 7200´s, 9000s i les Virtual Mobility Controller (appliance virtual) juntament amb els punts d'accés de les famílies 500s, 300s i 200s permeten desplegar xarxes sense fil de màxima seguretat i rendiment. Amb aquesta versió se suporta també WPA3 i Wifi- 6/802.11ax (amb les famílies 500s) així com WiFi-5/802.1ac i Wifi-4/802.11n. S'implementen avançades característiques de seguretat, en el control d'accés a la xarxa, així com en l'assignació de polítiques de seguretat. També se suporten mecanismes de monitoratge d'espectre. Els Punts d'Accés en mode poden treballar en mode Campus (CAP) i mode Remot (RAP), la qual cosa permet connectar de forma segura punts d'accés que creuen xarxes alienes com internet). S'implementen millores en actualitzacions de Software sense pèrdua de servei. Aruba Multizona permet a un Punt d'Accés donar servei a diverses Mobility Controllers de diferents dominis o entorns de seguretat. Els Mobility Controllers pot actuar com a servidors de túnels IPSEC/SSL per al client Aruba VIA.

Observacions

CCN-STIC 1431 Procediment d'Ocupació Assegurança ArubaOS 8.6. Controladores i Punts d'Accés

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

Versió	ArubaOS 8.10
Fabricant	HPE Aruba Networking
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/10/2023
Revisió de Validesa	30/06/2024

Descripció

Els Aruba Mobility Controllers permeten desplegar xarxes sense fil de màxima seguretat i rendiment. S'implementen avançades característiques de seguretat, en el control d'accés a la xarxa, així com en l'assignació de polítiques de seguretat. També se suporten mecanismes de monitoratge d'espectre.

Observacions

CCN-STIC 1431 Procediment d'Ocupació Assegurança ArubaOS Controladores i Punts d'Accés

Cisco Aironet 2800 Series Access Points (AIR-AP2802I-x-K9, AIR-AP2802I-x-K9C, AIR-AP2802E-x-K9 i AIR- AP2802E-x-K9C)	
	IOS-XE versió 17.6
Fabricant	Cisco Systems
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	30/07/2024
Descripció	

Els dispositius Cisco Wireless LAN combinen plataformes específiques de Controlador i Punt d'Accés per crear un Sistema d'Accés WLAN. Aquests dispositius proporcionen als usuaris sense fil accés segur a la xarxa de l'organització.

Observacions

Procediment d'ocupació assegurança pendent de publicació

Cisco 9115 Series Wi-Fi 6 Access Points (C9115AXI-x i C9115AXE-x)	
Versió	IOS-XE versió 17.6
Fabricant	Cisco Systems
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	30/07/2024
Descripció	

Els dispositius Cisco Wireless LAN combinen plataformes específiques de Controlador i Punt d'Accés per crear un Sistema d'Accés WLAN. Aquests dispositius proporcionen als usuaris sense fil accés segur a la xarxa de l'organització.

Observacions

Procediment d'ocupació assegurança pendent de publicació

Cisco 9130 Series Wi-Fi 6 Access Points (C9130AXI-x, C9130AXE-x, C9130AXE-STA-x)

Versió	IOS-XE versió 17.6
Fabricant	Cisco Systems
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	30/07/2024

Descripció

Els dispositius Cisco Wireless LAN combinen plataformes específiques de Controlador i Punt d'Accés per crear un Sistema d'Accés WLAN. Aquests dispositius proporcionen als usuaris sense fil accés segur a la xarxa de l'organització.

Observacions

Procediment d'ocupació assegurança pendent de publicació

Cisco Aironet 4800 Access Point (AIR-AP4800-x-K9 i AIR-AP4800-x-K9)C

Versió	IOS-XE 17.6
Fabricant	Cisco Systems
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2024

Descripció

Els dispositius Cisco Wireless LAN combinen plataformes específiques de Controlador i Punt d'Accés per crear un Sistema d'Accés WLAN. Aquests dispositius proporcionen als usuaris sense fil accés segur a la xarxa de l'organització.

Observacions

Procediment d'ocupació assegurança pendent de publicació

Cisco 9800-80-K9 Wireless Controller, 9800-40-K9 Wireless Controller, 9800-L Wireless Controller (C9800- L-F-K9 i C9800-L-C-K9), C9800-CL-K9 Wireless Controller for Private Cloud.	
Versió	IOS-XE versió 17.6
Fabricant	Cisco Systems
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2026
Descripció	

Els dispositius Cisco Wireless LAN combinen plataformes específiques de Controlador i Punt d'Accés per crear un Sistema d'Accés WLAN. Aquests dispositius proporcionen als usuaris sense fil accés segur a la xarxa de l'organització.

Observacions

Procediment d'Ocupació Assegurança Pendent de Publicació

Cisco 9120 Series Wi-Fi 6 Access Points (C9120AXI-x, C9120AXE-x, C9120AXP-x)	
Versió	IOS-XE versió 17.6
Fabricant	Cisco Systems
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/07/2024
Descripció	

Els dispositius Cisco Wireless LAN combinen plataformes específiques de Controlador i Punt d'Accés per crear un Sistema d'Accés WLAN. Aquests dispositius proporcionen als usuaris sense fil accés segur a la xarxa de l'organització.

Observacions

Procediment d'ocupació assegurança pendent de publicació

Cisco Aironet 1560 Series Access Points (AIR-AP1562I-x-K9, AIR-AP1562E-x-K9 i AIR-AP1562D-x-K9)	
Versió	IOS-XE versió 17.6
Fabricant	Cisco Systems
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/07/2024
Descripció	

Els dispositius Cisco Wireless LAN combinen plataformes específiques de Controlador i Punt d'Accés per crear un Sistema d'Accés WLAN. Aquests dispositius proporcionen als usuaris sense fil accés segur a la xarxa de l'organització.

Observacions

Procediment d'ocupació assegurança pendent de publicació

Cisco EW6300 Series Access Points (ESW-6300-CON-X-K9)	
Versió	IOS-XE 17.6
Fabricant	Cisco Systems
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/07/2024
Descripció	

Els dispositius Cisco Wireless LAN combinen plataformes específiques de Controlador i Punt d'Accés per crear un Sistema d'Accés WLAN. Aquests dispositius proporcionen als usuaris sense fil accés segur a la xarxa de l'organització.

Observacions

Procediment d'ocupació assegurança pendent de publicació

Cisco IW6300 Series Access Points (IW-6300H-AC-X-K9, IW-6300H-DC-X–K9 i W-6300H-DCW-X–K9)	
Versió	IOS-XE 17.6
Fabricant	Cisco Systems
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/07/2024

Descripció

Els dispositius Cisco Wireless LAN combinen plataformes específiques de Controlador i Punt d'Accés per crear un Sistema d'Accés WLAN. Aquests dispositius proporcionen als usuaris sense fil accés segur a la xarxa de l'organització.

Observacions

Procediment d'ocupació assegurança pendent de publicació

Access Controllers (AC6508, AC6605, AC6805, ACU2, AC6800V, AC6507S, AirEngine 9700-M, AirEngine 9700-M1 i AirEngine 9700S-S) con Access Points (AP6050DN, AP6150DN, AP4050DE-M, AP7060DN i AirEngine 5760, 5761, 6760, 6761, 6761 Series)	
Versió	AC V200R021C00SPC100 + V200R021C00SPH301
Fabricant	Huawei Technologies Espanya
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/01/2022
Revisió de Validesa	30/06/2024
Descripció	

Els equips Huawei Wireless Lan combinen plataformes específiques de Controlador (Access Controller) i Punt d'Accés (Access Points) per crear un sistema d'accés sense fil que s'adapta a xarxes de campus, xarxes d'oficines i xarxes d'àrea metropolitana (MAN) de qualsevol mida, i a la cobertura de zones Wi-Fi, proporcionant accés segur a la xarxa als usuaris sense fil.

Punts d'accessos V200R021C00SPC200 + V200R021C00SPH301T qualificats:

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

Observacions

CCN-STIC-1426 Procediment d'ocupació assegurança Huawei AirEngine Series

Cisco 9800-80, 9800-40, 9800-L Wireless Controller con Cisco Aironet 1560, 2800, 4800, 3800 Series Access Points	
Versió	IOS-XE 16.12
Fabricant	Cisco Systems
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

Descripció

Els dispositius Cisco Wireless LAN combinen plataformes específiques de Controlador i Punt d'Accés per crear un Sistema d'Accés WLAN. Aquests dispositius proporcionen als usuaris sense fil accés segur a la xarxa de l'organització.

Punts d'accés qualificats:

- Punts d'accés Serie Cisco Aironet 1560: Cisco Aironet 1562i, Cisco Aironet 1562e, Cisco Aironet 1562d,
- Punts d'accés Cisco Aironet 2800 Series: Cisco Aironet 2802i, Cisco Aironet 2802e,
- Punts d'accés Cisco Aironet 3800 Series: Cisco Aironet 3802i, Cisco Aironet 3802e, Cisco Aironet 3802p,
- Punt d'accés Cisco Aironet 4800

Observacions

Procediment d'Ocupació Assegurança Controladores Sense fil CISCO WLC 9800 i Punts d'Acces Cisco Catalyst

Huawei AirEngine (5760-22W, 5760-51,5761-10W, 5761-11,5761-11W, 5761-12W, 5761-21,5761R-11, 5761R-11E, 5761S-10W, 5761S-11, 5761S-11W, 5761S-12, 5761S-13, 5761S-21, 6760-51EI, 6760R-51,6760-X1,6760-X1E, 6761-21,6761-21E, 6761S-21, 8760R-X1, 8760-X1-PRO, 5761-10WD, 5761-11EI,5761-12, 5761RS-11, 5762-12, 5762-12SW, 5762-13W, 5762-15HW, 5762-16W, 5762S-11, 5762S-11SW,5762S-12, 5762S-12SW, 5762S-13W, 6760R-51E, 6761-21T, 6761-22T, 6761S-21T, 8760R-X1E) i WLAN AC (AC6508, AC6805, AirEngine 9700-M1)

Versió	V200R022C00SPC100 + V200R022C00SPH301T
Fabricant	Huawei Technologies Espanya Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/08/2023
Revisió de Validesa	31/01/2024

Descripció

Els equips Huawei Wireless Lan combinen plataformes específiques de Controlador (Access Controller) i Punt d'Accés (Access Points) per crear un sistema d'accés sense fil que s'adapta a xarxes de campus, xarxes d'oficines i xarxes d'àrea metropolitana (MAN) de qualsevol mida, i a la cobertura de zones Wi-Fi, proporcionant accés segur a la xarxa als usuaris sense fil.

Observacions

CCN-STIC-1426 Procediment d'ocupació segura Huawei AirEngine Sèries

Access Controllers (AC6508, AC6605, AC6805, ACU2, AC6800V, AC6507S, AirEngine 9700-M, AirEngine 9700-M1 i AirEngine 9700S-S) con Access Points (AP6050DN, AP6150DN, AP4050DE-M, AP7060DN i AirEngine 5760, 5761, 6760, 6761, 6761 Series)	
Versió	V200R020C00SPC300 + V200R020C00SPH301T
Fabricant	Huawei Technologies Espanya
Família	Dispositius de Xarxa Sense fil
Tipus	Producte
Data Inclusió	01/07/2021
Revisió de Validesa	31/01/2024

Descripció

Els equips Huawei Wireless Lan combinen plataformes específiques de Controlador (Access Controller) i Punt d'Accés (Access Points) per crear un sistema d'accés sense fil que s'adapta a xarxes de campus, xarxes d'oficines i xarxes d'àrea metropolitana (MAN) de qualsevol mida, i a la cobertura de zones Wi-Fi, proporcionant accés segur a la xarxa als usuaris sense fil.

Punts d'accessos qualificats:

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

Observacions

CCN-STIC-1426 Procediment d'ocupació assegurança Huawei AirEngine Series

7.5.6. PASSAREL·LES SEGURES D'INTERCANVI DE DADES

PSTfile

Versió	v4.4.2
Fabricant	Autek Ingeniería
Família	Passarel·les segures d'intercanvi de dades
Tipus	Producte
Data Inclusió	01/12/2017
Revisió de Validesa	31/05/2025

Descripció

PSTfile és un dispositiu de protecció de perímetre de la família PSTgateways. Permet l'intercanvi controlat de fitxers entre dominis de seguretat. S'estableix una correspondència entre carpetes, en servidors de fitxers d'ambdues xarxes i PSTfile, automàticament, mou o copia els fitxers de l'origen a la destinació. Suporta els protocols FTP, FTPS, SFTP i SMB. La transferència de fitxers des del domini d'alta seguretat al de baixa requereix autorització mitjançant signatura digital.

Observacions

Procediment d'ocupació segura: CCN-STIC-1401 Configuració segura de passarel·les d'AUTEK

PSTmail

Versió	v3.0.5
Fabricant	Autek Ingeniería
Família	Passarel·les segures d'intercanvi de dades
Tipus	Producte
Data Inclusió	01/12/2017
Revisió de Validesa	31/05/2025

Descripció

PSTmail és un dispositiu de protecció de perímetre de la família PSTgateways. Permet l'intercanvi controlat de correu electrònic entre dominis de seguretat. Possibilita l'ús d'adreces de correu de xarxes externes, des d'una xarxa interna, més segura. Suporta les versions segures dels protocols de correu. Els missatges de sortida requereixen autorització mitjançant signatura digital (S/MIME).

Observacions

Procediment d'ocupació segura: CCN-STIC-1401 Configuració segura de passarel·les d'AUTEK

7.5.7. DÍODES DE DADES

PSTdiode

Versión	v1.3.1-A
Fabricant	Autek Ingeniería
Família	Díodes de dades
Tipus	Producte
Data Inclusió	01/09/2019
Revisió de Validesa	31/08/2024

Descripció

El díode de dades maquinari PSTdiode és un dispositiu de protecció de perímetre que permet la transferència d'informació en un únic sentit entre dos dominis de seguretat amb garantia física de transmissió unidireccional. La seva aplicació principal és la introducció d'informació en una xarxa aïllada en entorns classificats. També es pot aplicar per extreure informació d'una xarxa de control industrial en entorns d'infraestructures crítiques. En ambdós casos es garanteix que no hi ha trànsit en el sentit invers. Existeixen models de transferència de fitxers i trànsit UDP.

Observacions

Procediment d'ocupació segura: CCN-STIC 1408 Procediment d'ocupació assegurança Díode Autek Ingeniería

7.5.8. XARXES PRIVADES VIRTUALS: IPSEC

Cisco ASA 5500 Series (5508-X and 5516-X)	
Versió	7.0
Fabricant	Cisco Systems
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	30/04/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Observacions

CCN-STIC 651B Seguretat a Cortafocs Cisco Firepower

Cisco Firepower Threat Defense (FTD) en Firepower 1000 i 2100 Series (FP1010, FP1120, FP1140, FP2110, FP2120, FP2130, FP2140)

Versió	FTD 6.4 i FMC/FCMv 6.4
Fabricant	Cisco Systems
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/02/2022
Revisió de Validesa	31/07/2024

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Compatible amb:

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 i FMC4600-K9)
- FMCv executant-se en ESXi 6.0 o 6.5 en el Sistema Unificat de Computació (UCS) UCSB-B200-M4, UCSC-C220- M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S- M3 i UCS-E180D-M3

Observacions

CCN-STIC-651B Seguretat en tallafocs CISCO Firepower

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

Versió	6.5.4.4-44n-federal-12n
Fabricant	SonicWall
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/08/2021
Revisió de Validesa	28/02/2025

Descripció

La Serie TZ de SonicWall ofereix seguretat i rendiment d'entorn Enterprise orientat a petites companyies. Enfocat a entorns departamentals o PIMES d'entre 5 i 100 usuaris (aprox), incorpora funcions de prevenció d'intrusions, antimalware, filtratge de continguts/URL i control d'aplicacions a través de xarxes i entorns sense fil. Proporciona inspecció profunda de paquets (DPI), SD-WAN i desplegament zero-touch. Opcions de ports PoE i wifi 802.11ac. Més info a: https://www.sonicwall.com/es-mx/products/firewalls/entry-level

Observacions

CCN-STIC-1420 Procediment d'Ocupació Segur Sonicwall SonicOS

PA-5400 Series (PA-5410, PA-5420, PA-5430, PA-5450)	
Versió	PAN-OS v10.2
Fabricant	Palo Alto
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	29/02/2024

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

FortiGate NGFW Appliances (FG40F, FG-60F, FWF-60F, FG-80F, FG-80F-PoE, FG-90G, FG-91G, FG-200F, FG-1100E, FG-1800F, FG-1800F-0DC, FG-2200E, FG-2600F, FG-2600F-0DC, FG-3300E, FG-3400E, FG-3400E0DC, FG-4200F, FG-4200F-0DC, FG-4400F, FG-4400F-0DC)	
Versió	FortiOS 6.4
Fabricant	Fortinet
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	30/09/2024

Descripció

Firewalls de Nova Generació amb capacitats d'inspecció en capa 7, IPS i concentrador VPN IPSEC. Les funcionalitats de seguretat més destacables són: reconeixement d'aplicacions i usuaris de la xarxa, protecció enfront de malware conegut, amenaces avançades i atacs zero-day, protecció enfront de botnets, filtre de navegació web, protecció DoS, proxy explícit, Inspecció SSL, capacitats SDWAN, VPN (IPSEC i SSL), control d'Access Points, LTE/5G i Switches, etc. Més informació a: https://docs.fortinet.com/product/fortigate/6.4

Observacions

CCN-STIC 1406 Procediment d'ocupació assegurança Tallafocs FortiGate

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

Versió	PA-OS v10.2
Fabricant	Palo Alto
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2025

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

WatchGuard Fireware on Firebox NGFWs (T25, T45, T85, M290, M390, M590, M590, M690, M4800, M5800

Versió	FirewareOS 12.6
Fabricante	TecHnologies WatchGuard
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	30/05/2025

Descripció

Els equips UTM de WatchGuard estan enfocats a oferir la millor seguretat per a qualsevol empresa i entorn corporatiu distribuït. Els nostres dispositius de seguretat de xarxa estan dissenyats, des de l'inici, per enfocar-se a facilitar el desplegament, l'ús i l'administració contínua. Proporcionen protecció contra atacs de malware avançat i phishing, així com les proteccions de seguretat tradicionals: prevenció d'intrusions (IPS), filtratge d'URL, control d'aplicacions, antispam i antivirus, oferint en tot moment visibilitat de l'entorn (productivitat i seguretat) Compten amb capacitats SD-WAN, i VPN. Estan disponibles tant en equips físics com virtuals. https://www.watchguard.com/es/wgrd-products/network-security

Observacions

CCN-STIC-1421 Procedimiento de empleo seguro WatchGuard Fireware

Cisco Secure Client - AnyConnect 5.0 for Ios16

Versió	5.0
Fabricant	Cisco Systems
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	18/03/2024
Revisió de Validesa	31/08/2024

Descripció

Cisco Secure Client (abans conegut com a Cisco Anyconnect) és un client VPN, que permet als usuaris d'una organització, amb dispositius Android, treballar de manera remota de forma completament segura com si estiguessin connectats directament a la seva xarxa privada. Proporciona als usuaris remots un túnel VPN segur que autentica i xifra el trànsit de xarxa que viatja a través d'una xarxa pública desprotegida.

Cisco Secure Client és un client Software . Per a la certificació a Common Criteria es va avaluar en un equip iPhone 11 amb versió iOS 16.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

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

Versió	7.0
Fabricant	Cisco Systems
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	30/04/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Observacions

CCN-STIC 651B Seguretat a Cortafocs Cisco Firepower

Cisco Secure Client - AnyConnect 5.0 for Android 12

Versió	5.0
Fabricant	Cisco Systems
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/12/2023
Revisió de Validesa	31/08/2024

Descripció

Cisco Secure Client (abans conegut com a Cisco Anyconnect) és un client VPN, que permet als usuaris d'una organització, amb dispositius Android, treballar de manera remota de forma completament segura com si estiguessin connectats directament a la seva xarxa privada. Proporciona als usuaris remots un túnel VPN segur que autentica i xifra el trànsit de xarxa que viatja a través d'una xarxa pública desprotegida.

Cisco Secure Client és un client Software . Per a la certificació a Common Criteria es va avaluar en un equip Galaxy A71 5G amb versió Android 12.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

FortiGate NGFW VM64

Versió	FortiOS 6.4
Fabricant	Fortinet
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	30/09/2024

Descripció

Firewalls de Nova Generació amb capacitats d'inspecció en capa 7, IPS i concentrador VPN IPSEC. Les funcionalitats de seguretat més destacables són: reconeixement d'aplicacions i usuaris de la xarxa, protecció enfront de malware conegut, amenaces avançades i atacs zero-day, protecció enfront de botnets, filtre de navegació web, protecció DoS, proxy explícit, Inspecció SSL, capacitats SDWAN, VPN (IPSEC i SSL), control d'Access Points, LTE/5G i Switches, etc. Més informació a: https://docs.fortinet.com/product/fortigate/6.4

Observacions

CCN-STIC 1406 Procediment d'ocupació assegurança Tallafocs FortiGate

Next-Generation Firewall with PAN-OS PA-200 Series (PA-220, PA220R), PA-400, PA-800 Series (PA-820, PA850), PA-3200 Series (PA-3220, PA3250, PA3260), PA-5200 Series (PA-5220, PA5250, PA5260, PA5280), PA-5450, PA-7000 Series (PA-7050, PA7080), VM-Series (VM-50, VM-100, VM-300, VM-500, VM-700, VM- 1000HV)	
Versió	10.1
Fabricant	Palo Alto
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/10/2022
Revisió de Validesa	31/03/2025

Descripció

Firewalls de Nova Generació orientat a grans empreses i datacenters, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat.

Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut. Suporten hipervisors: vmware ESXi, Citrix SDX, Microsoft Hyper-V, KVM, vmware vCloud Air, Microsoft Azure i Amazon AWS.

Observacions

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

Aruba Mobility Controller (9004, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280) i punts d'accés.

Versió	ArubaOS 8.6
Fabricant	Aruba
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/07/2021
Revisió de Validesa	30/06/2024

Descripció

Les famílies Aruba Mobility Controllers 7000´s, 7200´s, 9000s i les Virtual Mobility Controller (appliance virtual) juntament amb els punts d'accés de les famílies 500s, 300s i 200s permeten desplegar xarxes sense fil de màxima seguretat i rendiment. Amb aquesta versió se suporta també WPA3 i Wifi- 6/802.11ax (amb les famílies 500s) així com WiFi-5/802.1ac i Wifi-4/802.11n. S'implementen avançades característiques de seguretat, en el control d'accés a la xarxa, així com en l'assignació de polítiques de seguretat. També se suporten mecanismes de monitoratge d'espectre. Els Punts d'Accés en mode poden treballar en mode Campus (CAP) i mode Remot (RAP), la qual cosa permet connectar de forma segura punts d'accés que creuen xarxes alienes com internet). S'implementen millores en actualitzacions de Software sense pèrdua de servei. Aruba Multizona permet a un Punt d'Accés donar servei a diverses Mobility Controllers de diferents dominis o entorns de seguretat. Els Mobility Controllers pot actuar com a servidors de túnels IPSEC/SSL per al client Aruba VIA.

Observacions

CCN-STIC 1431 Procediment d'Ocupació Assegurança ArubaOS 8.6. Controladores i Punts d'Accés

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

Versió	ArubaOS 8.10
Fabricant	HPE Aruba Networking
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/10/2023
Revisió de Validesa	30/06/2024

Descripció

Els Aruba Mobility Controllers permeten desplegar xarxes sense fil de màxima seguretat i rendiment. S'implementen avançades característiques de seguretat, en el control d'accés a la xarxa, així com en l'assignació de polítiques de seguretat. També se suporten mecanismes de monitoratge d'espectre.

Observacions

CCN-STIC 1431 Procediment d'Ocupació Assegurança ArubaOS Controladores i Punts d'Accés

Cisco Secure Client - AnyConnect para Windows 10

Versió	22.2R1
Fabricant	Juniper Networks
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/02/2024
Revisió de Validesa	31/07/2024

Descripció

Les plataformes d'encaminament universal MX240/MX480/MX960 brinden un rendiment de gran escalabilitat en un factor de forma optimitzat per al núvol i les economies de cost per port o bit més exigents. Es poden utilitzar tant en xarxes de tipus operador, com a node de vora en xarxes MPLS, en entorns de mobilitat convergent, IoT, empresarial i també en arquitectures de Core convergent i de bord multiservei. També suporta l'ús com a encaminador de commutació d'etiquetes (LSR), provider Edge, equip d'intercanvi d'Internet i xarxa troncal per a implementacions en xarxes de caràcter metropolitanes, regionals o nacionals, o terminador de túnels IPSEC o Firewall de capa 4. La sèrie MX admet un ampli conjunt de funcionalitats IPoDWDM, L2, L3, IP/MPLS, SR, SRv6, terminador de túnels IPSEC o CGNAT per a permetre xarxes de transport a gran escala amb operacions i aprovisionament de serveis simplificats, mantenint simplicitat en la xarxa. Gràcies al tipus de chipsets implementats, tenen una capacitat de programació en el pla de dades gairebé infinita, la qual cosa li brinda la llibertat d'implementar noves innovacions de xarxa. Amb tecnologia de silici TRIO, la família MX és altament escalable des dels 3Tbps en 3U, passant per 38,4 Tbps en 5 slots i fins a un rendiment de 12 Tbps en 16 slots.

Observacions

Procediment d'Ocupació Segura pendent de publicació

PA-400 Series (PA-410, PA-440, PA-450, PA-460)

Versió	PA-OS v10.2
Fabricant	Palo Alto
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2025

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

FTD Virtual (FTDv) sobri ESXi 6.7 or 7.0 en Cisco Unified Computing System (UCS) - UCSC-C220-M5, UCSC-C240- M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3 installed on ISR	
Versió	7.0
Fabricant	Cisco Systems
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2024

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
- FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5,

UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observacions

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

PA-800 Series (PA-820, A-850)	
Versió	PA-OS v10.2
Fabricant	Palo Alto
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/01/2025
Descripció	

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

PA-3400 Series (PA-3410, PA-3420, PA-3430, PA-3440)	
Versió	PA-OS v10.2
Fabricant	Palo Alto
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2025
Descripció	

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

Firepower 2100 Series (2110, 2120, 2130, 2140)	
Versió	FTD 7.0 y FMC 7.0
Fabricant	Cisco Systems
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtrat de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
- FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observacions

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

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

Versió	FirewareOS 12.10
Fabricant	WatchGuard Technologies
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/03/2023
Revisió de Validesa	30/05/2025

Descripció

Els equips UTM de WatchGuard estan enfocats a oferir la millor seguretat per a qualsevol empresa i entorn corporatiu distribuït. Els nostres dispositius de seguretat de xarxa estan dissenyats, des de l'inici, per a enfocar-se a facilitar el desplegament, l'ús i l'administració contínua. Proporcionen protecció contra atacs de malware avançat i phishing, així com les proteccions de seguretat tradicionals: prevenció d'intrusions (IPS), filtrat d'URL, control d'aplicacions, antispam i antivirus, … oferint en tot moment visibilitat de l'entorn (productivitat i seguretat) Compten amb capacitats SD-WAN, i VPN. Estan disponibles tant en equips físics com virtuals.

https://www.watchguard.com/es/wgrd-products/network-security

Observacions

CCN-STIC-1421 Procedimiento de empleo seguro WatchGuard Fireware

PA-3200 Series (PA-3220, PA-3250, PA-3260

Versió	PAN-OS v10.2
Fabricant	Palo Alto
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2024

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

PA-220 Series (PA-220, PA-220R)

Versió	PAN-OS v10.2
Fabricant	Palo Alto
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2025

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

PA-7000 Series (PA-7050, PA-7080)

Versió	PAN-OS v10.2
Fabricant	Palo Alto
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2025

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

VM-Series (VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000-HV	
Versió	PAN-OS v10.2m
Fabricant	Palo Alto
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2025

Descripció

Firewalls de Nova Generació per a entorns virtuals, amb capacitat d'identificar l'aplicació, amb capacitat d'identificar l'aplicació per a la presa de decisions de seguretat, independentment del port, la tècnica evasiva, o el tipus de xifrat. Són capaços d'aplicar polítiques en base a l'usuari, per a la qual cosa s'integren amb diferents sistemes d'identificació i directoris LDAP.

Bloquegen els atacs coneguts, a més de realitzar filtratge URL dinàmic i identificar i generar protecció contra el malware desconegut.

Observacions

CCN-STIC-1413 PES Cortafocs NGFW Palo Alto Networks

Firepower 4100 Series (4110, 4112, 4115, 4120, 4125, 4140, 4145 and 4150)	
Versió	7.0
Fabricant	Cisco Systems
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Observacions

CCN-STIC 651B Seguretat a Cortafocs Cisco Firepower

FTD Virtual (FTDv) sobri NFVIS 4.4 on the ENCS 5406, 5408, and 5412	
Versió	FTDv 7.0 y FMC/FMCv 7.0
Fabricant	Cisco Systems
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
ata Inclusió	19/10/2023
Revisió de Validesa	30/04/2026

Descripció

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
- FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observacions

CCN-STIC 651B Seguridad en Cortafuegos Cisco Firepower

Firepower 9300 (includig chassis, supervisor blade, and security module)	
Versió	FTD 7.0, FXOS 2.10 y FMC/FMCv 7.0
Fabricant	Cisco Systems
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2026
Descripció	

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

- Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
- FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3

Observacions

CCN-STIC 651B Seguretat a Cortafocs Cisco Firepower

Firepower 1000 Series (1010, 1120, 1140, 1150)	
Versió	FTD 7.0, FXOS 2.10 y FMC/FMCv 7.0
Fabricant	Cisco Systems
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	19/10/2023
Revisió de Validesa	31/03/2026
Descripció	

Cisco Firepower Threat Defense (FTD) té capacitats de firewall, VPN i IPS. Aquesta plataforma ofereix la capacitat de filtratge de paquets amb estat (stateful packet filtering), i d'inspecció de paquets basada en informació de les aplicacions (application-aware). També proporcionen capacitats IPsec per a l'establiment de túnels VPN amb altres servidors VPN (VPN peer-to-peer) o amb dispositius VPN client (VPN d'accés remot).

Observacions

CCN-STIC 651B Seguretat a Cortafocs Cisco Firepower

FortiGate NGFW Appliances (FG-61E, FG-61F, FWF-61E, FWF-61F, FG-81E, FG-81E-PoE, FG-81F, FG-81F- 2R, FG-81F-2R-3G4G-PoE, FG-81F-2R-PoE, FG-81F-PoE, FG-90E, FG-91E)

Versió	FortiOS 6.4
Fabricant	Fortinet
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	30/09/2025

Descripció

Firewalls de Nova Generació amb capacitats d'inspecció en capa 7, IPS i concentrador VPN IPSEC. Les funcionalitats de seguretat més destacables són: reconeixement d'aplicacions i usuaris de la xarxa, protecció enfront de malware conegut, amenaces avançades i atacs zero-day, protecció enfront de botnets, filtre de navegació web, protecció DoS, proxy explícit, Inspecció SSL, capacitats SDWAN, VPN (IPSEC i SSL), control d'Access Points, LTE/5G i Switches, etc. Més informació a: https://docs.fortinet.com/product/fortigate/6.4

Observacions

CCN-STIC 1406 Procediment d'ocupació assegurança Tallafocs FortiGate

FortiGate NGFW Appliances (FG-100F, FG-101E, FG-101F, FG-201E, FG-201F, FG-301E, FG400F, FG-401E, FG401F, FG-501E, FG-600F, FG-601E, FG-601F)

Versió	FortiOS 6.4
Fabricant	Fortinet
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	30/09/2024

Descripció

Firewalls de Nova Generació amb capacitats d'inspecció en capa 7, IPS i concentrador VPN IPSEC. Les funcionalitats de seguretat més destacables són: reconeixement d'aplicacions i usuaris de la xarxa, protecció enfront de malware conegut, amenaces avançades i atacs zero-day, protecció enfront de botnets, filtre de navegació web, protecció DoS, proxy explícit, Inspecció SSL, capacitats SDWAN, VPN (IPSEC i SSL), control d'Access Points, LTE/5G i Switches, etc. Més informació a: https://docs.fortinet.com/product/fortigate/6.4

Observacions

CCN-STIC 1406 Procediment d'ocupació assegurança Tallafocs FortiGate

FortiGate NGFW Appliances (FG-1101E, FG-1801F, FG-1801F-DC, FG-2000E, FG-2201E, FG-2500E, FG-2601F, FG-2601F-DC, FG-3301E, FG-3401E, FG-3401E-DC, FG-3601E, FG-4201F, FG-4201F-DC, FG-4401F, FG-4401F-DC, FG-5001E1, FG-6300F, FG-6301F, FG-6500F, FG-6501F)

Versió	FortiOS 6.4
Fabricant	Fortinet
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/04/2023
Revisió de Validesa	30/09/2025

Descripció

Firewalls de Nova Generació amb capacitats d'inspecció en capa 7, IPS i concentrador VPN IPSEC. Les funcionalitats de seguretat més destacables són: reconeixement d'aplicacions i usuaris de la xarxa, protecció enfront de malware conegut, amenaces avançades i atacs zero-day, protecció enfront de botnets, filtre de navegació web, protecció DoS, proxy explícit, Inspecció SSL, capacitats SDWAN, VPN (IPSEC i SSL), control d'Access Points, LTE/5G i Switches, etc. Més informació a: https://docs.fortinet.com/product/fortigate/6.4

Observacions

CCN-STIC 1406 Procediment d'ocupació assegurança Tallafocs FortiGate

Aruba Virtual Intranet Access (VIA) Client

Versió	4.3
Fabricant	Aruba
Família	Xarxes privades virtuals: IPSec
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	30/06/2025

Descripció

Aruba Virtual Intranet Access (VIA) és un servei VPN segur per a usuaris que necessiten connectivitat corporativa remota des de la llar, ubicacions temporals o mentre estan en moviment. Es troba disponible com una descàrrega de Software per a Google Android, Apple iOS, MacOS, Linux i Windows, podent-se integrar amb plataformes de múltiple factor d'autenticació (MFA, 2FA).

La funció qualificada del VIA és la de client VPN IPSEC que avalua i selecciona automàticament la millor connexió segura per efectuar la connexió VPN amb l'organització. A diferència de les VPN tradicionals que requereixen maquinari dedicat (terminadors de túnels), Aruba integra serveis VPN directament en la infraestructura segura existent d'Aruba (Mobility Controllers) per simplificar l'arquitectura i l'administració.

Observacions

CCN-STIC 1431 Procediment d'Ocupació Assegurança ArubaOS 8.6. Controladores i Punts d'Accés

IS101

Versió 1.01

Fabricant ISTRIA SOLUCIONES DE CRIPTOGRAFIA

Família Xarxes privades virtuals: IPSec

Tipus Producte

Data Inclusió 01/07/2018

Revisió de Validesa 31/12/2025

Descripció

L'equip IS101 és un xifrador d'altes prestacions que, sobre una plataforma maquinari segura amb un FW/SW específic, implementa protocol IPSec en mode túnel. (amb encapsulat ESP i protocol IKEv2), cosa que permet establir, de forma senzilla i eficient, xarxes privades virtuals (VPN) sobre una xarxa IP no confiable (ja sigui pública o privada). Dissenyat per a sistemes en entorns crítics que manegen informació sensible. Velocitat de transferència de 2Gbps agregats.

Observacions

CCN-STIC-1405 Procediment d'ocupació assegurança IS101

SonicWall SOHO Serie (250, 250W)

Versió 6.5.4.4-44n-federal-12n

Fabricant SonicWall

Família Xarxes privades virtuals: IPSec

Tipus Producte

Data Inclusió 01/08/2021

Revisió de Validesa 28/02/2025

Descripció

Els tallafocs de la Serie TZ SOHO de Sonicwall són una solució adequada per a oficines petites i domèstiques, així com per a entorns distribuïts en ubicacions remotes. Despleguen funcionalitats per construir Secure SD-WAN i connectivitat WIFI (opcional). El SOHO 250 proporciona un 50% més de rendiment sobre el seu antecessor SOHO, així com accés als sandboxes avançats Capture ATP, amb la qual cosa es millora la seguretat en prevenció i detecció de malware desconegut en un entorn remot.

Observacions

CCN-STIC-1420 Procediment d'Ocupació Segur Sonicwall SonicOS

7.5.9. XARXES PRIVADES VIRTUALS: SSL

Cisco AnyConnect Secure Mobility Client for iOS 13

Versió 4.10

Fabricant Cisco Systems

Família Xarxes privades virtuals: SSL

Tipus Producte

Data Inclusió 01/11/2022

Revisió de Validesa 30/06/2026

Descripció

El Cisco AnyConnect Secure Mobility Client v4.10 for Android 11 és un client VPN, que permet als usuaris d'una organització, amb dispositius Android, treballar de manera remota de forma completament segura com si estiguessin connectats directament a la seva xarxa privada.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

Cisco AnyConnect Secure Mobility Client for Android 11

Versió 4.10

Fabricant Cisco Systems

Família Xarxes privades virtuals: SSL

Tipus Producte

Data Inclusió 01/11/2022

Revisió de Validesa 30/06/2026

Descripció

El Cisco AnyConnect Secure Mobility Client v4.10 for Android 11 és un client VPN, que permet als usuaris d'una organització, amb dispositius Android, treballar de manera remota de forma completament segura com si estiguessin connectats directament a la seva xarxa privada.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

Cisco AnyConnect Secure Mobility Client for Windows 10

Versió	4.10
Fabricant	Cisco Systems
Família	Xarxes privades virtuals: SSL
Tipus	Producte
Data Inclusió	01/11/2022
Revisió de Validesa	30/06/2026

Descripció

El Cisco AnyConnect Secure Mobility Client v4.10 for Windows 10 és un client VPN, que permet als usuaris d'una organització, amb dispositius Windows, treballar de manera remota de forma completament segura com si estiguessin connectats directament a la seva xarxa privada.

Observacions

Procediment d'Ocupació Assegurança Pendent de publicació

7.5.10. XARXES PRIVADES VIRTUALS: ALTRES

EMMA VPN	
Versió	CMI/CMIX 1.6.0-23.7153 | Core 1.2.2-0.11643
Fabricant	OpenCloud Factory
Família	Xarxes privades virtuals: SSL
Tipus	Producte
Data Inclusió	01/09/2021
Revisió de Validesa	30/06/2024

Descripció

El mòdul de concentració de VPNs d'EMMA actua com a frontend per a la finalització de túnels VPN, mitjançant un agent. EMMA realitza l'autenticació, autorització i auditoria contra el gestor d'identitat corporatives de l'Organisme i permet afegir un segon factor d'autenticació, per minimitzar el risc de suplantació d'identitat. Permet definir i aplicar polítiques d'accés en funció d'una postura de seguretat basada en el nivell de bastionat desitjat, a més d'altres factors, com l'horari de la connexió, característiques de l'equip, role d'usuari, etc...

Observacions

CCN-STIC-1105 Procediment d'ocupació assegurança EMMA

7.5.11. EINES PER A COMUNICACIONS MÒBILS SEGURES

COMSec	
Versió	v4.2
Fabricant	Indra
Família	Eines per a comunicacions mòbils segures
Tipus	Producte
Data Inclusió	01/10/2018
Revisió de Validesa	29/02/2024

Descripció

COMSec és una solució global de comunicacions segures que proporciona serveis xifrats de veu, missatgeria instantània i videoconferència sobre telèfons mòbils emprant qualsevol xarxa cel·lular, sense fil o satelital. Amb el seu alt nivell de seguretat, gran qualitat d'àudio i facilitat d'ús protegeix de forma eficaç qualsevol informació sensible de l'organització. Les trucades i les dades intercanviades per COMSec són segures, independentment de l'operador mòbil utilitzat i el país on es trobi. Més informació: comsec.indracompany.com

Observacions

CCN-STIC-1407 Procediment d'Ocupació Assegurança de COMSec

7.5.12. EINES DE VIDEOCONFERÈNCIA

PEXIP Infinity

Versió v.25.4 (Build 59565.0.0); Client software v1.6.2

Fabricant PEXIP

Família Eines de videoconferència

Tipus Producte

Data Inclusió 01/03/2022

Revisió de Validesa 31/08/2024

Descripció

Plataforma d'infraestructura de videoconferència virtualitzada i distribuïda, per gestionar equips de videoconferència de sala H.323/SIP i clients d'escriptori PC, Mac, Linux, amb client WebRTC.

Actua de Call Control, consta de firewall traversal, unitat multiconferència (MCU), sistema de gestió de terminals i allotja usuaris d'escriptori i mòbils. Proporciona bridge per interoperar amb usuaris de Microsoft Teams CVI, Google Meet, Skype for Business, Webex i WebRTC, i fa streaming i recording. Integra Outlook i Google Calendar per a la planificació de sessions, SSO, certificats i LDAP. Consta d'una àmplia llibreria d'APIs.

L'arquitectura es basa en 3 tipus de nodes:

- Management Node per gestionar i configurar la plataforma, les polítiques de trucades i el monitoratge.
- Transcoding Nodes, on es processen i allotgen les conferències i multiconferències. Proporciona redundància i és resistent a pèrdua de paquets i baixos ràtios de transferència.
- Edge Nodes on es negocia la senyalització amb xarxes externes i on es fa el trànsit i oculta la topologia de xarxa interna.
- Aquesta arquitectura és escalable i permet la securització de les comunicacions mitjançant xifrat. Permet la privacitat de dades, equips i usuaris.

Observacions

CCN-STIC-1616 PES Pexip Infinity

7.5.13. XIFRADORS IP

EP430TX

Versió 1.04

Fabricant: Epicom

Família Xifradors IP

Tipus Producte

Data Inclusió 01/12/ 2017

Revisió de Validesa 31/12/2024

Descripció

Xifrador de comunicacions IP fins a 200 Mbps, interoperable amb la resta de xifradors de la família EP430.

Observacions

Utilització segons PE-2016-28 Procediment d'ocupació EP430TX.

EP430GX

Versió v.1.08

Fabricant: Epicom

Família Xifradors IP

Tipus Producte

Data Inclusió 27/12/2021

Revisió de Validesa 31/12/2024

Descripció

Xifrador de xarxes IP a 2 Gbps (agregats), interoperable amb la resta de xifradors de la família EP430.

Observacions

Utilització segons PE-2012-49 Procediment d'Ocupació EP430GX.

EP430GN

Versió v2.04

Fabricant Epicom

Família Xifradors IP

Tipus Producte

Data Inclusió 01/12/2022

Revisió de Validesa 31/12/2024

Descripció

Xifrador de xarxa IP a 2 Gbps (agregat).

Observacions

Aquest model no és compatible amb la resta de la família de xifradors EP430 d'EPICOM. Utilització segons P029-PE-2011-33 Operational doctrine EP430GN v2.

IS101

Versió 1.01

Fabricant ISTRIA SOLUCIONSE DE CRIPTOGRAFIA

Família Xifradors IP

Tipus Producte

Data Inclusió 01/07/2018

Revisió de Validesa 31/12/2025

Descripció

L'equip IS101 és un xifrador d'altes prestacions que, sobre una plataforma maquinari segura amb un FW/SW específic, implementa protocol IPSec en mode túnel. (amb encapsulat ESP i protocol IKEv2), cosa que permet establir, de forma senzilla i eficient, xarxes privades virtuals (VPN) sobre una xarxa IP no confiable (ja sigui pública o privada). Dissenyat per a sistemes en entorns crítics que manegen informació sensible. Velocitat de transferència de 2Gbps agregats.

Observacions

CCN-STIC-1405 Procediment d'ocupació assegurança IS101

EP960

Versió 1.09.17
Fabricant: Epicom
Família Xifradors IP
Tipus Producte
Data Inclusió 01/09/2020
Revisió de Validesa 31/12/2025
Descripció

Xifrador personal de mida reduïda (120x80x25mm) per a la protecció de les comunicacions. Compta amb diversos interfícies negres (interfícies no segurs on la informació ja està xifrada): Ethernet, WiFi i 3G/4G. Ofereix un nivell mitjà de seguretat i proporciona una solució de WiFi segur.

Observacions

Procediment d'ocupació assegurança pendent de publicació.

EP430GN

Versió 1.08.29
Fabricant: Epicom
Família Xifradors IP
Tipus Producte
Data Inclusió 01/12/2017
Revisió de Validesa 31/12/2024
Descripció

Xifrador de xarxa IP a 2 Gbps (agregat).

Observacions

Aquest model no és compatible amb la resta de la família de xifradors EP430 d'EPICOM. Utilització segons P029-PE 2011-33 Operational doctrine EP430GN v2.

7.6. PROTECCIÓ DE LA INFORMACIÓ I ELS SUPORTS DE LA INFORMACIÓ

7.6.1. EMMAGATZEMATGE XIFRAT DE DADES

CRYHOD	
Versió	Q.2021.2
Fabricant	PRIMX
Família	Emmagatzematge xifrat de dades
Tipus	Producte
Data Inclusió	01/05/2023
Revisió de Validesa	30/11/2025

Descripció

Cryhod és un programa de xifratge modern que assegura el xifratge complet dels discos durs de les estacions de treball portàtils de l'organització. Cryhod implementa mecanisme d'autenticació forta (doble factor) mitjançant la targeta SmartCard de la FNMT al Pre-Boot de l'equip cosa que permet identificar unívocament els usuaris del sistema i protegir-lo davant atacs en cas de pèrdua o robatori.

Observacions

CCN-STIC-1505 Procedimiento de Empleo Seguro CRYHOD de PRIMX

ZONE CENTRE

Versió	Q.2021.1
Fabricant	PRIMX
Família	Emmagatzematge xifrat de dades
Tipus	Producte
Data Inclusió	01/05/2023
Revisió de Valides	30/04/2025

Descripció

ZONECENTRAL és un Software de xifratge de dades l'objectiu del qual és assegurar la confidencialitat de tots els arxius d'una organització (locals, a la xarxa i compartits) incloent-hi els perfils d'usuari.

ZONECENTRAL facilita la gestió de "la necessitat de conèixer", protegint l'accés a les dades sensibles i segmentant la informació entre els diferents perfils d'usuaris. Només els usuaris autoritzats poden entendre el contingut d'un determinat fitxer.

ZONECENTRAL s'instal·la en els llocs de treball com qualsevol altre Software de seguretat informàtica, integrant-se amb altres solucions del tipus PKI, targetes intel·ligents, token, etc. i aplica de forma automàtica les polítiques de seguretat de l'empresa.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació.

7.6.2. XIFRAT I COMPARTICIÓ SEGURA D'INFORMACIÓ

EP852

Versió 3.05

Fabricant Epicom

Família Xifrat i compartició segura d'informació

Tipus Producte

Data Inclusió 27/12/2021

Revisió de Validesa 31/12/2025

Descripció

L'EP852 és un xifrador de fitxers fora de línia que permet el xifratge i desxifrat de fitxers i el transport d'informació xifrada en el dispositiu. Millora les prestacions quant a emmagatzematge i velocitat de les versions anteriors dels Token USB així com la posada en marxa del dispositiu, càrrega i distribució de claus.

Observacions

Utilització segons el PE-2020-4 -Procediment d'Ocupació Segur EP852 -(ESP)

SMiD Cloud

Versió	2.1
Fabricant	ENCIFRA
Família	Xifrat i compartició segura d'informació
Tipus	Producte
Data Inclusió	01/04/2022
Revisió de Validesa	30/09/2024

Descripció

SMiD cloud és un dispositiu maquinari Plu&Play que s'integra en una xarxa local SMB de Microsoft i que s'encarrega de l'emmagatzematge xifrat dels fitxers que s'hi emmagatzemen. L'ús de SMiD cloud NO requereix la instal·lació de cap mena de Software o agent en els equips que l'utilitzen. Els fitxers xifrats poden emmagatzemar-se en local o en un o diversos proveïdors d'emmagatzematge al núvol.

Els dispositius SMiD cloud només mantenen còpies en clar dels fitxers que estan sent usats i retornen qualsevol fitxer al seu estat xifrat quan es deixen d'utilitzar.

L'arrencada de tot dispositiu SMiD cloud requereix la presència en l'arrencada d'una clau física USB d'arrencada sense la qual el dispositiu no arrenca. Si es configura explícitament per a això, els dispositius SMiD cloud poden ser clonats en el cas que l'original es deteriori, sigui sostret o destruït.

SMiD cloud és compatible amb Directori Actiu i amb qualsevol o sistema operatiu que operi a la xarxa local SMB. L'ús de diferents dispositius permet la compartimentalització automàtica del risc i dels sistemes d'emmagatzematge. L'estructura del sistema de fitxers no surt del dispositiu SMiD cloud que els va crear i no són deduïbles des de l'exterior.

SMiD cloud protegeix confidencialitat i integritat de la informació que se li lliura davant d'atacs al núvol o en emmagatzematge local. Qualsevol atac de ransomware no posa en perill les còpies xifrades en local o al núvol, ja que són inaccessibles fins i tot per als usuaris autoritzats o per a l'administrador del dispositiu.

Cada fitxer es xifra amb una clau diferent, realment aleatòria i de 256 bits de longitud, mitjançant el xifrador AES-256. La integritat de cada fitxer està controlada amb el valor SHA-256 d'aquest.

Observacions

Sense Procediment d'Ocupació Assegurança

GuardedBox

Versió	10.5
Fabricant	DinoSec
Família	Xifrat i compartició segura d'informació
Tipus	Producte
Data Inclusió	01/12/2022
Revisió de Validesa	31/05/2025

Descripció

GuardedBox és una solució per a emmagatzematge, compartició i control segurs d'informació, amb xifrat E2E, disponible per a desplegaments on-premise i en núvol públic o privat, tan autogestionats com en modalitat SaaS.

La informació emmagatzemada (denominada "secrets") i les seves metadades es guarden xifrats en el servidor mitjançant claus AES-256 bits, i es xifren i desxifren en el costat client mitjançant criptografia asimètrica de corba el·líptica reconeguda per a ENS en categoria ALTA i complementada amb sofisticats controls d'accés.

Funcionalitats:

- Intercanvi en temps real: individual o de grup, disponible tant per a usuaris registrats com externs, amb filtres per domini i mecanismes de control per conèixer els estats actuals i passats de compartició.
- Notificacions: avisa els usuaris (per email i en la interfície) dels esdeveniments que afecten els elements del seu àmbit.
- Auditoria: implementada com a blockchain, registra tots els esdeveniments sense revelar el contingut de la informació.
- Recordatoris: per definir avisos sobre accions necessàries.
- Disseny APIficat: admet integració amb altres solucions de l'entorn (SSO, logging, etc.).
- Personalitzacions a mida.
- Panell d'administració.

Observacions

CCN-STIC 1509 Procediment d'ocupació assegurança Guardedbox

EP880

Versió V2.08.36 i V2.09.35

Fabricant Epicom

Família Xifrat i compartició segura d'informació

Tipus Producte

Data Inclusió 01/07/2021

Revisió de Validesa 31/12/2026

Descripció

L'EP880 és una aplicació Software que s'executa sobre ordinador amb sistema operatiu Windows i que permet realitzar, en origen, el xifratge i signatura de fitxers de dades "off-line" emmagatzemats en el disc dur de l'ordinador o dispositius d'emmagatzematge externs connectats a l'ordinador, per al seu posterior emmagatzematge o enviament de forma segura des del correu electrònic o un altre mitjà i, en destinació, el desxifrat i verificació de la integritat de les dades.

Observacions

CCN-STIC-1506 Procediment d'Ocupació Assegurança EP880

EP852

Versió 3.04

Fabricant Epicom

Família Xifrat i compartició segura d'informació

Tipus Producte

Data Inclusió 01/04/2021

Revisió de Validesa 31/12/2025

Descripció

L'EP852 és un xifrador de fitxers fora de línia que permet el xifratge i desxifrat de fitxers i el transport d'informació xifrada en el dispositiu. Millora les prestacions quant a emmagatzematge i velocitat de les versions anteriors dels Token USB així com la posada en marxa del dispositiu, càrrega i distribució de claus.

Observacions

Utilització segons el PE-2020-4 -Procediment d'Ocupació Segur EP852 -(ESP)

7.6.3. EINES D'ESBORRAT SEGUR

Blancco Drive Eraser

Versió	7.6
Fabricant	Blancco
Família	Eines d'esborrat segur
Tipus	Producte
Data Inclusió	01/08/2020
Revisió de Validesa	30/06/2024

Descripció

Software d'esborrat assegurança de dades per a discos durs HDD i estat sòlid SSD en computadores d'escriptori, laptops i emmagatzematge massiu amb adaptadors IDE, SATA, SAS, SCSI, FIBRA CANAL FC, SSD i Emmc. Ofereix un esborrat segur del 100% del disc dur per particions físiques en realitzar una sobre escriptura en la totalitat dels sectors continguts en el disc dur. Permet un esborrat automatitzat, monitoratge de les activitats d'esborrat i informa de totes les activitats d'esborrat facilitant el compliment de les Polítiques de Seguretat i Retenció d'Informació. L'esborrat fet és conforme als criteris dels òrgans normatius gràcies al seu report certificat d'auditoria i en compliment de RGPD. Disposa d'una instal·lació flexible i senzilla.

Observacions

CCN-STIC 1504 Procediment d'ocupació segura de Blancco Drive Eraser

Blancco File Eraser

Versió	v8.5.2
Fabricant	Blancco
Família	Eines d'esborrat segur
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	31/05/2024

Descripció

La solució d'esborrat d'arxius Blancco File Eraser permet administrar i automatitzar rutines d'esborrat de dades en ordinadors de sobretaula, portàtils i servidors. BENEFICIS PRINCIPALS 1. Esborrat segur de dades en fitxers. 2. Esborrat automatitzat. 3. Monitora i informa de totes les activitats d'esborrat. 4. Esborrat conforme als criteris dels òrgans normatius gràcies al seu report certificat d'auditoria i en compliment de RGPD. 5. Senzilla instal·lació. Més informació: espana@deletetecnology.com - 91 761 23 70.

Observacions

CCN-STIC 1502 Procediment d'ocupació assegurança de Blancco File Eraser

OLVIDO Windows

Versió	1.0.6
Fabricant	authUSB
Família	Eines d'esborrat segur
Tipus	Producte
Data Inclusió	01/07/2022
Revisió de Validesa	28/02/2025

Descripció

OBLIT és una eina d'esborrat segur que acompleix tasques de sobreescriptura i esborrat sobre els sistemes d'arxius i discos reconeguts. Ofereix a l'usuari la possibilitat d'esborrar de forma segura diferents elements guardats en els dispositius d'emmagatzematge:

- Fitxers i carpetes
- Espai Lliure
- Fragments de clúster no utilitzats
- Discos i volums

Disposa d'un mòdul de planificació amb el qual es permet a l'usuari programar l'execució de les tasques d'esborrat. OBLIT implementa diferents algoritmes estàndard d'esborrat i permet a l'usuari seleccionar l'algoritme d'esborrat a aplicar en cada tasca. Així mateix, ofereix la possibilitat a l'administrador de definir algorismes d'esborrat personalitzats, especificant el nombre de passis i el patró de sobreescriptura. Permet la integració amb un servidor Syslog per a l'enviament de registres d'activitat i estat de les tasques d'esborrat fetes.

La versió aprovada permet, amb l'algoritme d'esborrat CCN-Classificat, la reclassificació i desclassificació de:

- Discos magnètics fins a RESERVAT o equivalent.
- Discos SSD fins a DIFUSIÓ LIMITADA o equivalent.

S'executa sobre Windows 10, Windows Server 2016 i Windows Server 2021.

Observacions

CCN-STIC-1508 Procedimiento de empleo seguro OLVIDO

7.6.4. SISTEMES DE PREVENCIÓ DE FUGA DE DADES

Forcepoint On-Premise Security

Versió	8.5
Fabricant	Forcepoint
Família	sistemes de prevenció de fuga de dades
Tipus	Producte
Data Inclusió	01/05/2021
Revisió de Validesa	31/10/2024

Descripció

Els dispositius Forcepoint Web Security realitzen la funció de proxy de navegació segura integrant múltiples motors de classificació de continguts i anàlisis de seguretat en temps real amb capacitat d'inspecció de trànsit segur i també anàlisi de dades sortints amb capacitat per a aplicar polítiques enfront de fugides d'informació. Les plataformes funcionen com proxies directes http, https, ftp i SOCKS per a la protecció i control d'usuaris i llocs de connexió. El propòsit d'aquests dispositius és proporcionar una capa de seguretat entre la xarxa Interna i una o més xarxes externes (típicament una xarxa corporativa i Internet), aïllant el trànsit dels usuaris a nivell d'aplicació i proporcionant a més diferents mecanismes d'optimització WAN per al trànsit que processen

Observacions

CCN-STIC-1507 Procedimiento de Empleo Seguro Forcepoint On-premise Security 8.5

7.6.5. EINES PER A SIGNATURA ELECTRÒNICA

Tarjeta Criptográfica TC-FNMT

Versió	5.6
Fabricant	FNMT-RCM
Família	Eines per a signatura electrònica
Tipus	Producte
Data Inclusió	18/01/2024
Revisió de Validesa	18/07/2024

Descripció

La TC-FNMT és una targeta criptogràfica amb la capacitat de realitzar signatures electròniques. Està compost d'un xip prèviament certificat (que proporciona la llibreria criptogràfica i el microprogramari amb el loader per a l'actualització del codi), el sistema operatiu i les llibreries biomètriques. Aquesta targeta implementa un sistema de fitxers que inclou la següent aplicació:

- eSign (aplicació de signatura [TR03110-2] conforme als perfils de protecció BSI-CC-PP-0059-2009-DT. 01, BSI-CC-PP-0075, BSI-CCPP-0071 , BSI-CC-PP-0072 I BSI-CC-PP-0076.

A més del compliment dels requisits en la funcionalitat de signatura electrònica, la TC-FNMT v5.6 també compleix amb els requisits del Reglament (UE) núm. 910/2014 (eIDAS) en matèria d'identificació electrònica, requisits derivats de la Decisió d'Execució (UE) 2016/650 de la Comissió de 25 d'abril de 2016 per la qual es fixen les normes per a l'avaluació dels dispositius qualificats de creació de signatures i segells conformement a l'article 30, apartat 3, i a l'article 39, apartat 2 del Reglament eIDAS.

Observacions

Procediment d'Ocupació Segura pendent de publicació

Ascertia ADSS Server Signature Activation Module (SAM)

Versió	7.0
Fabricant	Ascertia Limited
Família	Eines per a signatura electrònica
Tipus	Producte
Data Inclusió	01/05/2022
Revisió de Validesa	31/10/2024

Descripció

L'ADSS SAM v.7.0.2 és el nou rQSCD/rQSealCD d'Ascertia certificat Common Criteria EAL4+ EN 419 241-2 (SCAL2).

L'ADSS SAM v.7.0.2 compleix amb els estàndards FIPS 140-2 Level 3, EN 419 241-1 & 2 (SCAL1 & SCAL2), EN 419 221-5, TS 119 431-1, TS 119 431-2, TS 119 432 i Cloud Signature Consortium (CSC).

Aquest nou rQSCD/rQSealCD dona resposta a les necessitats més exigents de seguretat i confiança que necessiten els Proveïdors de Serveis de Confiança Qualificats, proporcionant un alt rendiment i una alta disponibilitat per a l'emissió de segells de temps qualificats, de signatura digital remota qualificada (reconeguda) i de segell electrònic corporatiu qualificat. L'ADSS SAM v.7 també està disponible en mode "software only" per satisfer els requisits dels Proveïdors de Serveis de Confiança Avançats.

L'ADSS SAM v.7.0.2 destaca per la seva gran flexibilitat, resiliència i escalabilitat; tot això combinat amb una seguretat interna ben dissenyada que facilita la seva administració, la seva auditoria i la generació d'informes que compleixen amb els requisits ETSI/CEN per a sistemes d'Alta Confiança. És compatible el seu ús amb HSMs de xarxa externs dels 3 principals fabricants que hagin estat certificats EN 419 221- 5.

Observacions

N/A

SIAVAL Safecert Server Signing Sistema

Versió	v.3
Fabricant	Sistemes Informàtics Oberts
Família	Eines per a signatura electrònica
Tipus	Producte
Data Inclusió	01/08/2021
Revisió de Validesa	01//03/2025

Descripció

Solució de signatura centralitzada de la família SIAVAL orientada a facilitar la gestió i l'ús de les claus privades i públiques dels usuaris finals, també identificats com a titulars o signants. Està dissenyat per funcionar com un dispositiu remot de creació de signatura rQSCD, segons els requisits especificats en el Reglament (UE) nº 910/2014 del Parlament Europeu (eIDAS: Annex II), fent possible la generació de signatures electròniques avançades (AdES) i de signatures electròniques qualificades o reconegudes (QES) en un servidor remot.

Observacions

Procediment d'ocupació pendent de publicació

7.6.5. HARDWARE SECURITY MODULE (HSM)

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

Versió	7.7.0 (bootloader versions 1.1.1, 1.1.2 i 1.1.4)
Fabricant	Thales
Família	Hardware Security Module (HSM)
Tipus	Producte
Data Inclusió	01/09/2021
Revisió de Validesa	31/03/2026

Descripció

Els Mòduls de Seguretat Maquinari (HSM) de Thales, són criptoprocessadors dedicats que estan dissenyats específicament per a la protecció del cicle de vida de les claus criptogràfiques. L'administració, el processament i l'emmagatzematge de claus criptogràfiques es realitza dins del dispositiu reforçat a prova de manipulacions, augmentant el rendiment i mantenint la seguretat. Amb els mòduls de seguretat de maquinari de Thales, pot: - Abordar els requisits de compliment amb solucions per a Blockchain, GDPR, IoT, iniciatives de paper a digital, PCI DSS, firmes digitals, eIDAS, DNSSEC, emmagatzematge de claus en maquinari, acceleració transaccional, signatura de certificats, signatura de codi o documents, generació de claus massives, xifrat de dades i més. - Les claus sempre es generen i emmagatzemen en el dispositiu validat a prova d'intrusions i manipulacions, que proporciona els nivells més alts de control d'accés. - Possibilitat de crear particions lògiques en els HSM de xarxa, amb Oficials de Seguretat dedicats per partició, i segmentant la gestió amb una separació total de les claus.

Observacions

Demanar al fabricant la guia de configuració utilitzada en la certificació Common Criteria. Configurar el producte per a la utilització de funcions, algoritmes i protocols aprovats pel Centre Criptològic Nacional, segons la guia CCN-STIC-807 Criptologia d'ocupació a l'ENS

nShield Solo XC Hardware Security Module

Versió	v12.60.15
Fabricante	Entrust Solutions
Mòdul	Hardware Security Module (HSM)
Tipus	Producte
Data Inclusió	01/11/2021
Revisió de Validesa	30/04/2024

Descripció

Els mòduls de seguretat maquinari (HSM) nShield XC són dispositius físics amb certificació FIPS 140-2 nivell 3 i Common Criteria EAL4+ (EN 419 221-5) que permeten efectuar operacions criptogràfiques de forma segura. Al seu torn, el disseny d'aquests equips, ofereix una Serie de funcionalitats que facilita la gestió de material criptogràfic: - Protecció pràcticament il·limitada de claus privades. - Flexibilitat en la creació de còpies de seguretat de les claus en no necessitar equips addicionals ni accés directe als HSM. - Capacitat d'executar codi dins de l'HSM mitjançant CodeSafe. Des d'un punt de vista funcional, els HSM nShield XC són plataformes resistents a la manipulació (tamper resistant) que fan de forma segura funcions de generació i protecció de claus i signatura digital per a una gran varietat d'aplicacions, com: - Autoritats de certificació - Processos de negoci - Signatura de codi - Serveis al núvol - Blockchain privades i públiques - Establiment de comunicacions segures

Observacions

Demanar al fabricant la guia de configuració utilitzada en la certificació Common Criteria. Configurar el producte per a la utilització de funcions, algoritmes i protocols aprovats pel Centre Criptològic Nacional, segons la guia CCN-STIC-807 Criptologia d'ocupació a l'ENS

CryptoServer CP5

Versió	5.1.0.0
Fabricant	UTIMACO
Família	Hardware Security Module (HSM)
Tipus	Producte
Data Inclusió	01/12/2022
Revisió de Validesa	31/05/2024

Descripció

Els Mòduls de Seguretat Maquinari (HSM) UTIMACO constitueixen l'arrel de confiança ideal per protegir actius sensibles crítics per a la seguretat en empreses i administracions públiques, amb casos d'ús en finances, automoció, IoT, infraestructures crítiques, telecomunicacions i proveïdors de serveis.

CryptoServer CP5 és l'HSM certificat per a la generació i emmagatzematge de Certificats Qualificats per a firmes i segells electrònics que compta amb la Certificació Common Criteria d'acord amb el Protection Profile eIDAS EN 419221-5 "Mòdul Criptogràfic per a Serveis de Confiança".

CryptoServer CP5 disposa de funcionalitats d'autorització de clau per a creació de signatures qualificades i signatures remotes compatibles amb eIDAS. Altres àrees d'aplicació inclouen l'emissió de certificats qualificats OCSP i segellament de temps.

Característiques rellevants:

- Emmagatzematge i processament segur de claus dins dels límits segurs de l'HSM
- Autenticació de doble factor amb targetes intel·ligents
- Control d'accés basat en rols configurable
- Gestió remota
- Simulador Software per a avaluació i proves.
- En format appliance i targeta PCIe
- Certificacions FIPS 140-2 nivell 3 i Common Criteria EAL4+ (EN 419 221-5)

Observacions

Procediment d'Ocupació Assegurança pendent de publicació.

7.6.6. GESTIÓ DE METADADES

metaOLVIDO Endpoint i metaOLVIDO Server

Versió	2.2.6
Fabricant	Adarsus Technologies S.L
Família	Gestió de metadades
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	30/04/2026

Descripció

metaOLVIDO EndPoint i metaOLVIDO Server: Eina de gestió de metadades que permet aplicar polítiques de seguretat corporatives de prevenció de fuites d'informació, netejant les metadades i informació sensible oculta en els fitxers ofimàtics generats en una organització.

Realitza una protecció contínua i en temps real de les metadades d'una estació de treball o Servidor. Protegeix la informació de manera senzilla i desatesa. Permet configurar regles i posar-les en pràctica sobre els arxius documentals o multimèdia que es consideri necessari, ja sigui en els equips d'usuari -EndPoint- o en carpetes de xarxa compartides -Server-.

Observacions

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard

MetaClean Dashboard

Versió	v1.1.0
Fabricant	Adarsus Technologies S.L
Família	Gestió de metadades
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	30/04/2024

Descripció

MetaClean Dashboard: Consola d'administració de MetaClean per a les diferents modalitats de desplegament. Administra, centralitza i controla l'aplicació de polítiques preventives de seguretat corporatives. Permet obtenir estadístiques de les metadades processats i controlar l'exfiltració d'informació de forma global.

Observacions

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard

MetaClean Sync Workstation i MetaClean Sync Server

Versió	v.2.2.6
Fabricant	Adarsus Technologies S.L
Família	Gestió de metadades
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	30/04/2024

Descripció

MetaClean Sync Workstation i MetaClean Sync Server: Eina de gestió de metadades que permet aplicar polítiques de seguretat corporatives de prevenció de fuites d'informació, netejant les metadades i informació sensible oculta en els fitxers ofimàtics generats en una organització.

Realitza una protecció contínua i en temps real de les metadades d'una estació de treball o Servidor. Protegeix la informació de manera senzilla i desatesa. Permet configurar regles i posar-les en pràctica sobre els arxius documentals o multimèdia que es consideri necessari, ja sigui en els equips d'usuari -Workstation- o en carpetes de xarxa compartides -Server-.

Observacions

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard y metaOLVIDO Server

metaOLVIDO Dashboard (modalidad on-premise)

Versió	1.1.0
Fabricant	Adarsus Technologies S.L
Família	Gestió de metadades
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	30/04/2024

Descripció

metaOLVIDO Dashboard: Consola d'administració de metaOLVIDO per a les diferents modalitats de desplegament. Administra, centralitza i controla l'aplicació de polítiques preventives de seguretat corporatives. Permet obtenir estadístiques de les metadades processats i controlar l'exfiltració d'informació de forma global.

Observacions

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard y metaOLVIDO Server

7.7. PROTECCIÓ D'EQUIPS I SERVEIS

7.7.1. DISPOSITIUS MÒBILS

Samsung Galaxy Tab S8 (SM-X706B/SM-X700), Tab S8+ 5G (SM-X806B/SM-X800), Tab S8 Ultra (SM-X906B/SM-X900)

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/07/2022
Revisió de Validesa	01/02/2027

Descripció

La família de dispositius de la gamma TAB S8 són tauletes empresarials basades en Android que incorpora la Plataforma Samsung Knox, oferint capacitats i mecanismes de protecció d'integritat basats en Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Data Fi de Suport prevista:

Samsung Galaxy Tab S8 5G SM-X706B 12/01/2027

Galaxy Tab S8+ 5G SM-X806B 12/01/2027

Galaxy Tab S8 Ultra 5G SM-X906B 14/01/2027

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Samsung Galaxy Z Flip4 (SM-F721B)

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/12/2022
Revisió de Validesa	07/08/2027

Descripció

La família de dispositius de la gamma Galaxy Zflip 4 són dispositius empresarials plegables basats en Android que incorpora la Plataforma Samsung Knox, oferint capacitats i mecanismes de protecció d'integritat basats en Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Versió de Sistema Operatiu suportat actualment: Android 12

Data Fi de Suport prevista:

Samsung Galaxy Z Flip4 (SM-F721B): 01/07/2027

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Samsung Galaxy S23 5G (SM-S911B), S23+ 5G (SM-S916B), S23 Ultra 5G (SM-S918B), S23 FE (SM-S711B)

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	31/12/2026

Descripció

La família de dispositius de la gamma Galaxy S23 5G són telèfons mòbils basats en Android que incorporen la Plataforma Samsung Knox, oferint mecanismes de protecció d'integritat amb suport Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Observacions

CCN-STIC 1617 PES Samsung Galaxy Android13

Samsung Galaxy S22 5G (SM-S901B), S22+ 5G (SM-S906B), S22 Ultra 5G (SM-S908B)

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/07/2022
Revisió de Validesa	21/01/2027

Descripció

La família de dispositius de la gamma Galaxy S22 són telèfons mòbils basats en Android que incorporen la Plataforma Samsung Knox, oferint capacitats i mecanismes de protecció d'integritat basada en Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Data Fi de Suport prevista:

Samsung Galaxy S22 5G SM-S901B 21/01/2027

Samsung Galaxy S22+ 5G SM-S906B 21/01/2027

Samsung Galaxy S22 Ultra 5G SM-S908B 21/01/2027

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Samsung Galaxy Z Flip3 5G (SM-F711F)

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/07/2022
Revisió de Validesa	13/08/2026

Descripció

La família de dispositius de la gamma Galaxy Z són dispositius empresarials plegables basats en Android que incorpora la Plataforma Samsung Knox, oferint capacitats i mecanismes de protecció d'integritat basats en Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Data Fi de Suport prevista:

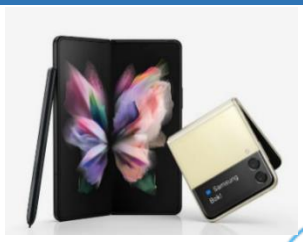
Samsung Galaxy Z Flip3 5G SM-F711B 27/07/2026

Observacions

CCN-STIC 1617 Procediment d'Ocupació Assegurança de dispositius Samsung Galaxy (Android 12)

Samsung Galaxy Z Fold3 5G (SM-F926B)

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/07/2022
Revisió de Validesa	16/08/2026



Descripció

La família de dispositius de la gamma Galaxy Z són dispositius empresarials plegables basats en Android que incorpora la Plataforma Samsung Knox, oferint capacitats i mecanismes de protecció d'integritat basats en Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Data Fi de Suport prevista:

Samsung Galaxy Z Fold3 5G SM-F926B 16/07/2026

Observacions

CCN-STIC 1631 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy Android 13)

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

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/12/2022
Revisió de Validesa	01/09/2027

Descripció

Galaxy Tab Active 4 Pro és una tauleta rugeritzada basada en Android que incorpora la Plataforma Samsung Knox, oferint mecanismes de protecció d'integritat amb suport Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Versió de Sistema Operatiu suportat actualment: Android 12

Data Fi de Suport prevista:

Samsung Galaxy Tab Active4 Pro (SM-T636): 01/08/2027

Samsung Galaxy Tab Active4 Pro (SM-T630): 01/08/2027

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Samsung Galaxy XCover6 Pro (SM-G736B)

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/12/2022
Revisió de Validesa	01/07/2027

Descripció

Galaxy Xcover6 Pro són dispositius empresarials rugeritzats basats en Android que incorpora la Plataforma Samsung Knox, oferint mecanismes de protecció d'integritat amb suport Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Versió de Sistema Operatiu suportat actualment: Android 12

Data Fi de Suport prevista:

Samsung Galaxy XCover6 Pro (SM-G736B): 01/06/2027

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Samsung Galaxy Z Fold4 5G (SM-F936B)

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/12/2022
Revisió de Validesa	01/08/2027

Descripció

La família de dispositius de la gamma Galaxy Zfold4 són dispositius empresarials plegables basats en Android que incorpora la Plataforma Samsung Knox, oferint capacitats i mecanismes de protecció d'integritat basats en Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Versió de Sistema Operatiu suportat actualment: Android 12

Data Fi de Suport prevista:

Samsung Galaxy Z Fold4 5G (SM-F936B): 01/07/2027

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Samsung Galaxy A53 5G (SM-A536B)

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/12/2022
Revisió de Validesa	01/03/2027

Descripció

Galaxy A53 5G són telèfons mòbils basats en Android que incorporen la Plataforma Samsung Knox, oferint capacitats i mecanismes de protecció d'integritat basada en Maquinari, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Versió de Sistema Operatiu suportat actualment: Android 12

Data Fi de Suport prevista:

Samsung Galaxy A53 5G (SM-A536B): 01/02/2027

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Samsung Galaxy A52 5G (SM-A526B)

Versió	Android 12
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/01/2022
Revisió de Validesa	10/02/2025

Descripció

El model Galaxy A52 5G és un telèfon mòbil basat en Android que incorpora la Plataforma Samsung Knox, oferint mecanismes de protecció d'integritat amb suport Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Galaxy A52 5G (SM-526B)

Versió	Android 13
Fabricant	Samsung Electronics Co, Ltd
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	18/12/2023
Revisió de Validesa	30/06/2024

Descripció

El model Galaxy A52 5G és un telèfon mòbil basat en Android que incorpora la Plataforma Samsung Knox, oferint mecanismes de protecció d'integritat amb suport Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Galaxy Z Fold5 5G (SM-F946B)

Versió	Android 13
Fabricant	Samsung Electronics Co., Ltd.
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	18/12/2023
Revisió de Validesa	30/06/2024

Descripció

La família de dispositius de la gamma Galaxy Z Fold 5 són dispositius empresarials plegables basats en Android que incorpora la Plataforma Samsung Knox, oferint capacitats i mecanismes de protecció d'integritat basats en Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Galaxy Z Flip5 5G (SM-F731B)

Versió Android 13

Fabricant Samsung Electronics Co., Ltd.

Família Dispositius mòbils

Tipus Producte

Data Inclusió 18/12/2023

Revisió de Validesa 31/05/2026

Descripció

La família de dispositius de la gamma Galaxy Z Flip 5 són dispositius empresarials plegables basats en Android que incorpora la Plataforma Samsung Knox, oferint capacitats i mecanismes de protecció d'integritat basats en Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Galaxy Tab S9 (SM-X716B | SM-X710), Tab S9+ (SM-X816B/SM-X810), Tab S9 Ultra (SM-X916B/SMX-910)

Versió Android 13

Fabricant Samsung Electronics Co., Ltd.

Família Dispositius mòbils

Tipus Producte

Data Inclusió 18/12/2023

Revisió de Validesa 31/05/2026

Descripció

La família de dispositius de la gamma TAB S9 són tauletes empresarials basades en Android que incorpora la Plataforma Samsung Knox, oferint capacitats i mecanismes de protecció d'integritat basats en Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Galaxy Tab Active 3 (SM-T575 | SM-T570)

Versió	Android 13
Fabricant	Samsung Electronics Co., Ltd.
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	18/12/2023
Revisió de Validesa	30/06/2024

Descripció

Galaxy Tab Active 3 és una tauleta rugeritzada basada en Android que incorpora la Plataforma Samsung Knox, oferint mecanismes de protecció d'integritat amb suport Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

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

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/10/2020
Revisió de Validesa	24/03/2025

Descripció

La família de dispositius de la gamma Galaxy S20 són telèfons mòbils basats en Android que incorporen la Plataforma Samsung Knox, oferint mecanismes de protecció d'integritat amb suport Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Data fi de suport prevista:
- SM-G986B Edició empresarial: 24/01/2025
- SM-G986B: 24/01/2024
- SM-G981B: 24/01/2024
- SM-G988B: 24/01/2024
- SM-G985F Edició empresarial: 24/01/2025
- SM-G985F: 24/01/2024
- SM-G980F Edició empresarial: 24/01/2025
- SM-G980F: 24/01/2024

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

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

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/12/2020
Revisió de Validesa	24/08/2025

Descripció

La família de dispositius de la gamma Galaxy Note20 són telèfons mòbils basats en Android que incorporen la Plataforma Samsung Knox, oferint mecanismes de protecció d'integritat amb suport Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Data fi de suport prevista:

- SM-N980F: 24/07/2024
- SM-N981B: 22/07/2024
- SM-N981B Edició empresarial: 22/07/2025
- SM-N986B: 22/07/2024

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Samsung Galaxy Z Fold2 5G (SM-F916B)

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/12/2020
Revisió de Validesa	27/09/2024

Descripció

Galaxy Z Fold2 5G és un telèfon mòbil basat en Android que incorpora la Plataforma Samsung Knox, oferint mecanismes de protecció d'integritat amb suport Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

Samsung Galaxy S21 5G (SM-G991B), S21+ 5G (SM-G996B), S21 Ultra+ 5G (SM-G998B), S21 5G FE (SM-G990B)

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/10/2021
Revisió de Validesa	28/01/2026

Descripció

La família de dispositius de la gamma Galaxy S21 són telèfons mòbils basats en Android que incorporen la Plataforma Samsung Knox, oferint mecanismes de protecció d'integritat amb suport Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

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

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/12/2020
Revisió de Validesa	23/08/2024

Descripció

Galaxy Tab S7 / S7+ és una tauleta empresarial basada en Android que incorpora la Plataforma Samsung Knox, oferint mecanismes de protecció d'integritat amb suport Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Data fi de suport prevista:

SM-T870: 23/07/2024

SM-T875: 23/07/2024

SM-T875 Edició empresarial: 23/07/2024

SM-T970: 23/07/2024

SM-T976B: 23/07/2024

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

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

Versió	Android 13
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/12/2020
Revisió de Validesa	17/10/2025

Descripció

La família de dispositius de la gamma Galaxy S20 FE són telèfons mòbils basats en Android que incorporen la Plataforma Samsung Knox, oferint mecanismes de protecció d'integritat amb suport Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Observacions

CCN-STIC 1631 PES Samsung Galaxy Android 13

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

Versió	Android 12
Fabricant	Samsung Electronics
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	01/12/2020
Revisió de Validesa	22/09/2025

Descripció

Galaxy Tab Active 3 és una tauleta rugeritzada basada en Android que incorpora la Plataforma Samsung Knox, oferint mecanismes de protecció d'integritat amb suport Hardware, protecció robusta a les Dades en Repòs i Dades en Trànsit, així com el control avançat i monitoratge del dispositiu de manera transparent i productiva per a l'usuari de l'organització.

Observacions

CCN-STIC 1617 Procediment d'Ocupació Assegurança de dispositius Samsung Galaxy (Android 12)

7.7.2. SISTEMES OPERATIUS

SUSE Linux Enterprise

Versió	Server 15 SP2
Fabricant	SUSE Software Solutions
Família	Sistemes Operatius
Tipus	Producte
Data Inclusió	01/10/2021
Revisió de Validesa	30/06/2026

Descripció

SUSE® Linux Enterprise Server (SLES) 15 SP2 és un sistema operatiu (SO) modular que ajuda a simplificar l'entorn IT, modernitzar la infraestructura IT i accelerar la innovació. SLES s'adapta a qualsevol entorn operatiu alhora que satisfà els requisits de rendiment, seguretat i confiabilitat. És una plataforma fàcil d'administrar per a desenvolupadors i administradors que permet implementar càrregues de treball crítiques per al negoci a les instal·lacions, al núvol i al perímetre.

Observacions

CCN-STIC-1615 Procediment d'ocupació assegurança SUSE 15 SP2

Windows Server 2016

Versió	Datacenter Edition
Fabricant	Microsoft Corporation
Família	Sistemes Operatius
Tipus	Producte
Data Inclusió	01/12/2018
Revisió de Validesa	09/01/2024

Descripció

Sistema Operatiu per a servidors

Observacions

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

SUSE Linux Enterprise

Versió	Server 15 SP2
Fabricant	SUSE Software Solutions
Família	Sistemes Operatius
Tipus	Producte
Data Inclusió	01/10/2021
Revisió de Validesa	31/12/2024

Descripció

SUSE® Linux Enterprise Server (SLES) 15 SP2 és un sistema operatiu (SO) modular que ajuda a simplificar l'entorn IT, modernitzar la infraestructura IT i accelerar la innovació. SLES s'adapta a qualsevol entorn operatiu alhora que satisfà els requisits de rendiment, seguretat i confiabilitat. És una plataforma fàcil d'administrar per a desenvolupadors i administradors que permet implementar càrregues de treball crítiques per al negoci a les instal·lacions, al núvol i al perímetre.

Observacions

CCN-STIC-1615 Procediment d'ocupació assegurança SUSE 15 SP2

7.7.3. PROTECCIÓ DE CORREU ELECTRÒNIC

Microsoft Defender for Office 365 (Email Protection)

Versió

Fabricant	Microsoft Iberica SRL
Família	Protecció de correu electrònic
Tipus	Servei
Data Inclusió	01/04/2023
Revisió de Validesa	31/03/2025

Descripció

Microsoft Defender per a Office 365 és una solució de seguretat al núvol que protegeix el correu electrònic a Office365 o en local i els serveis d'Office 365 (Microsoft Teams, SharePoint, OneDrive i aplicacions d'Office) contra amenaces com phishing, malware, spam i compromís de correu electrònic empresarial. També ofereix eines per educar els empleats sobre com detectar correus electrònics de phishing i protegeix contra descàrregues d'arxius maliciosos a través de navegadors web. A més, utilitza tecnologies per bloquejar remitents no desitjats i analitza el contingut dels correus electrònics per detectar i bloquejar contingut inapropiat o no desitjat. En resum, Microsoft Defender per a Office 365 és una solució completa i efectiva per protegir les empreses de les amenaces de correu electrònic i serveis d'Office 365 (Microsoft Teams, SharePoint, OneDrive i aplicacions d'Office).

Observacions

CCN-STIC 1629-Procedimiento de Empleo Seguro MS Defender for Office 365

Proofpoint Email Protection & Targeted Email Protection

Versió

Fabricant Proofpoint, Inc.

Família Protecció de correu electrònic

Tipus Servei

Data Inclusió 01/11/2023

Revisió de Validesa 31/10/2025

Descripció

Proofpoint Email Protection (PPS+TAP) és una solució avançada de Protecció del Correu Electrònic. Amb la seva aproximació centrada en les persones, permet a les organitzacions protegir els usuaris de les amenaces que arriben pel correu electrònic, tant les més bàsiques com campanyes de spam i correu massiu, suplantacions d'identitat (BEC), phishing o malware, així com aquelles més avançades que necessiten una anàlisi estàtica i dinàmica de fitxers adjunts o enllaços web. A més, aprofita tota la intel·ligència de protegir el vector més gran d'entrada d'amenaces per oferir una visibilitat centrada en les persones del panorama d'amenaces de cada client, proporcionant informació detallada en temps real dels riscos dels usuaris, les amenaces que reben i els actors maliciosos que puguin estar atacant l'organització.

Observacions

CCN-STIC-1636-Procedimiento de Empleo Seguro de Proofpoint Email Protection y Targeted Attack Protection

Cisco Email Security Appliance (C190, C195, C390, C395, C690, C690X, C695, C695F, C100v, C300v i C600v)

Versió AsyncOS 13.0

Fabricant Cisco Systems

Família Protecció de correu electrònic

Tipus Producte

Data Inclusió 01/12/2022

Revisió de Validesa 31/05/2025

Descripció

Cisco Email Security Appliance és una passarel·la de seguretat per al correu electrònic. Està dissenyat per detectar i bloquejar una àmplia varietat d'amenaces transmeses per correu electrònic, com malware, spam i intents de phishing.

Observacions

CCN-STIC 1623 Procediment d'Ocupació Segur Cisco Email Security Appliance

7.7.4. BALANCEJADORS DE CÀRREGA

A10 Networks VThunder (vTH-1Gbps, vTH-4Gbps, vTH-8Gbps, vTH-10Gbps, vTH-20Gbps, vTH-40Gbps, vTH-100Gbps, FlexPool)

Versió	ACOS 5.2.1-P3
Fabricant	A10 Networks, Inc
Família	Balancejadors de càrrega
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/11/2025

Descripció

A10 Networks Thunder Series Appliances és la família de productes necessària per assegurar la disponibilitat de servidors i aplicacions, ajuda en la protecció d'aplicacions vulnerables, optimitza i accelera l'entrega de contingut. Basat en el sistema operatiu ACOS, sistema de supercomputació que no utilitza memòria dedicada sinó compartida, atorga una alta eficiència en rendiment dels equips amb una baixa empremta energètica.

Disponible en les següents opcions:

Llicència ADC – Inclou balanceig de càrrega, GSLB, full-proxy, balanceig de línies, presentació d'aplicacions https (SSL Offloading), autenticació, routing avançat, aFlex per a programació d'opcions avançades, permet alta densitat de particions en funció del model arribant fins a 1023 particions, renovació automàtica de certificats mitjançant protocol ACME i protecció AntiDDoS.

Llicència CGN – Afegeix opcions de CGNAT avançades i ajuda a l'adopció d'IPv6.

Llicència SSLi – Permet tenir visibilitat al trànsit SSL per a elements de seguretat a la xarxa de clients i així descarregar-los d'aquesta tasca computacionalment costosa i reduir la latència.

Llicència cFW – Afegeix capacitats de FW tipus stateful i inclou capacitat de VPN IPSec i proxy de navegació.

Observacions

CCN-STIC-1635 Procedimiento de empleo seguro A10 Thunder

A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655, TH-940, TH-1040, TH-3350E, TH-3350, TH-4440 TH-5440, TH-5840, TH-5845, TH-6440, TH-6655S, TH-7440, TH-7440-11, TH-7650, TH-14045)

Versió	ACOS 5.2.1-P3
Fabricant	A10 Networks, Inc
Família	Balancejadors de càrrega
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	29/02/2024

Descripció

A10 Networks Thunder Series Appliances és la família de productes necessària per assegurar la disponibilitat de servidors i aplicacions, ajuda en la protecció d'aplicacions vulnerables, optimitza i accelera l'entrega de contingut. Basat en el sistema operatiu ACOS, sistema de supercomputació que no utilitza memòria dedicada sinó compartida, atorga una alta eficiència en rendiment dels equips amb una baixa empremta energètica.

Disponible en les següents opcions:

Llicència ADC – Inclou balanceig de càrrega, GSLB, full-proxy, balanceig de línies, presentació d'aplicacions https (SSL Offloading), autenticació, routing avançat, aFlex per a programació d'opcions avançades, permet alta densitat de particions en funció del model arribant fins a 1023 particions, renovació automàtica de certificats mitjançant protocol ACME i protecció AntiDDoS.

Llicència CGN – Afegeix opcions de CGNAT avançades i ajuda a l'adopció de IPv6.

Llicència SSLi – Permet tenir visibilitat al trànsit SSL per a elements de seguretat a la xarxa de clients i així descarregar-los d'aquesta tasca computacionalment costosa i reduir la latència.

Llicència cFW – Afegeix capacitats de FW tipus stateful i inclou capacitat de VPN IPSec i proxy de navegació.

Observacions

CCN-STIC-1635 Procedimiento de empleo seguro A10 Thunder

7.7.6. HIPERCONVERGÈNCIA

KATUA SDI PLATFORM

Versió	1.0
Fabricant:	KRC ESPAÑOLA, S.A.
Família	Hiperconvergència
Tipus	Producte
Data Inclusió	01/09/2021
Revisió de Validesa	31/01/2025

Descripció

Katua®SDI Platform és una plataforma hiperconvergent escalable i segura, basada en el concepte Software Defineix Infraestructure, on tots els elements que conformen un CPD es defineixen en una única plataforma maquinari i Software . Permet el desplegament ràpid de serveis (xaaS), consolidació de CPDs, SDN i té capacitat d'instal·lació des d'equips mòbils fins a grans centres de processos de dades. La seva flexibilitat permet que es puguin desplegar serveis cloud sobre la plataforma de forma senzilla i eficient. Disposa de la capacitat per generar biblioteques de sistemes preconfigurats per al seu desplegament amb un click a través de la seva interfície web. Les capacitats d'optimització de l'hipervisor asseguren un rendiment màxim de la plataforma, fent ús de tots els recursos disponibles i oferint d'aquesta forma capacitat d'instal·lació en nodes petits i configuracions hardware bàsiques. La seva capacitat per integrar-se amb sistemes d'emmagatzematge massius, siguin locals o remots permet escapolir la solució en funció de les necessitats. Per a més informació de la plataforma, vista la nostra web https://www.krc.es

Observacions

CCN-STIC-1610 Procediment d'Ocupació Segur KATUA SDI Platform

7.7.7. EINES DE VIDEOIDENTIFICACIÓ

NebulaID Engine

Versió	v2.0
Fabricant	VINTEGRIS
Família	Eines de videoidentificació
Tipus	Servei
Data Inclusió	01/06/2023
Revisió de Validesa	31/05/2025

Descripció

nebulaID és la solució Software desenvolupada per Víntegris que permet l'execució de processos de vídeo identificació per a l'emissió de certificats electrònics qualificats.

nebulaID fa les funcions de Portal de Registre i està integrat en la solució SaaS nebulaSUITE desenvolupada per Víntegris, la qual cosa permet la gestió del cicle de vida dels certificats electrònics i ofereix els serveis de signatura electrònica avançada i qualificada.

La solució combina diversos mecanismes d'identificació biomètrica i d'autenticació multi factor, la qual cosa la converteix en una opció vàlida per a l'obtenció de certificats qualificats amb validesa legal. Aquest procediment permet als usuaris verificar la seva identitat des de qualsevol lloc per mitjà d'un dispositiu electrònic amb càmera, aportant la tranquil·litat d'estar complint amb el reglament europeu eIDAS i la regulació específica espanyola (Ordre Ministerial ETD/743/2022). Per vídeo identificar-se, només es necessita d'uns minuts i de la utilització del document d'identitat acreditatiu de l'usuari.

Observacions

CCN-STIC-1634 NebulaID Engine

Signaturit VideoID by Ivnosys

Versió	v1.0
Fabricant	IVNOSYS SOLUCIONES
Família	Eines de videoidentificació
Tipus	Servei
Data Inclusió	01/07/2023
Revisió de Validesa	29/02/2024

Descripció

Signaturit VideoID by Ivnosys', és una solució API desenvolupada per IVNOSYS SOLUCIONES, SLU (Grup Signaturit), que realitza processos desassistits (o asíncrons) de videotrucades d'individus, per a onboarding remot i per a identificació de sol·licitants de certificats electrònics qualificats (conforme l'Ordre ETD/465/2021, de 6 de maig), utilitzant el component biomètric de l'eina "Veridas Identity Verification Service".

Permet generar i gestionar processos de vídeo identificació i procedir mitjançant intermediació manual d'un operador si ho requereix la norma, a la validació o el rebuig de les identificacions en funció de les evidències biomètriques recaptades (imatges, vídeos) i scores processats per Veridas.

Està constituït per dos components: 'Signaturit VideoID API', que permet fer integracions de forma senzilla i adaptar-se a panells de tercers amb personalització pròpia, garantint la configuració requerida per la normativa aplicable al cas d'ús, i 'Signaturit VideoID Gateway', aplicació web que desplega la funcionalitat necessària per realitzar la videotrucada d'un individu.

Observacions

CCN-STIC-1638 Procedimiento de Empleo Seguro Signaturit VideoID

LOQR Platform

Versió	Backoffice 3.1, SDK 3.0
Fabricant	LOQR, SA
Família	Eines de videoidentificació
Tipus	Servei
Data Inclusió	01/05/2024
Revisió de Validesa	31/106/2024

Descripció

LOQR és una empresa de tecnologia en l'àmbit de la identitat digital. LOQR ofereix una plataforma que utilitza intel·ligència artificial per a ampliar i diversificar el perfil dels clients que accedeixen a serveis digitals, amb l'objectiu d'enfortir a les organitzacions i accelerar el seu negoci digital. La Plataforma de LOQR proporciona fluxos de treball (Journeys) de Verificació d'Identitat i per a millorar l'experiència del client i proporcionar informació única que pugui evolucionar cap a una transformació digital proactiva. La solució de LOQR compleix amb tots els requisits reguladors i estàndards de qualitat.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

IQP VideoID and SelfID_BO products

Versió	V13.3.0
Fabricant	Infocert Spa
Família	Eines de videoidentificació
Tipus	Servei
Data Inclusió	19/05/2023
Revisió de Validesa	30/06/2024

Descripció

Remote-ID by InfoCert és un sistema de verificació d'identitat remota que guia el subjecte en la presa de selfi i fotografies del seu document d'identitat perquè puguin ser processats i comparats amb la seva biometria facial i així verificar si és qui diu ser.

Hi ha dos processos d'identificació disponibles:

- assistit amb operador (videoID)
- desatès sense operador (selfID)

El resultat es posa a disposició dels operadors a través de la plataforma Identity Qualification Plaform, IQP, on poden dur a terme la revisió de les evidències i així concloure la identificació del subjecte.

Els processos han estat dissenyats per complir amb l'Ordre Ministerial ETD/743/2022, de 26 de juliol, on queden regulats els mètodes d'identificació remota per a l'emissió de certificats electrònics qualificats.

La solució es pot contractar a través d'AC Camerfirma S.A.

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

Inetum Digital Onboarding

Versió 1.0

Fabricant INETUM

Família Eines de videoidentificació

Tipus Servei

Data Inclusió 01/09/2023

Revisió de Validesa 30/09/2025

Descripció

Producte en modalitat SaaS que implementa la video-identificació per al procediment que s'ha de seguir en la identificació remota per vídeo d'un ciutadà. Aquest servei incorpora la tecnologia per verificar l'autenticitat, vigència i integritat dels documents d'identificació, verificar la correspondència del titular amb la persona que realitza el procés i verificar que aquest és una persona viva que no està sent suplantada.

S'inclou també el portal de revisió manual de les evidències dut a terme per un operador especialista. A més, aquesta eina permet l'ús en canal Web del procediment de video- identificació. Està dissenyat especialment per complir l'Ordre Ministerial ETD/743/2022, de 26 de juliol, per la qual es regulen els mètodes d'identificació remota per vídeo.

Observacions

CCN-STIC 1630 Procedimiento de Empleo Seguro Inetum Digital Onboarding Platform

certificadoelectronico.es

Versió 1.0

Fabricant Bewor Tech

Família Eines de videoidentificació

Tipus Servei

Data Inclusió 01/04/2023

Revisió de Validesa 31/03/2025

Descripció

Solució de verificació d'identitat per videoidentificació a través de la qual, de manera automàtica, és verificada la identitat de la persona que realitza el procés. Aquesta verificació consisteix en la comparació biomètrica entre la foto del document acreditatiu i el rostre de la persona que fa el procés, aquesta verificació biomètrica conté prova de vida passiva. A més, han estat desenvolupades comprovacions amb relació a la veracitat del document acreditatiu mostrat durant el procés, analitzant les dues cares del document i l'holograma. La solució compta amb una plataforma de verificació a través de la qual, un agent format per a això fa una revisió manual de totes les evidències recollides durant cada procés de videoidentificació. En definitiva, amb aquesta solució, Bewor verifica de manera remota la identitat de la persona que fa el procés.

Observacions

CCN-STIC-1627 Procediment d'ocupació assegurança CertificadoElectronico.es

Alice Onboarding

Versió

Fabricant Alice Biometrics

Família Eines de videoidentificació

Tipus Servei

Data Inclusió 01/04/2023

Revisió de Validesa 31/03/2025

Descripció

Alice Onboarding és un sistema de verificació d'identitat remota no assistit i multiplataforma per a un cas d'ús desatès, en el qual l'usuari interactua directament amb el sistema sense necessitat d'establir una videoconferència amb un operador. Això s'aconsegueix mitjançant la captura guiada i processat automàtic de selfie i document d'identitat, que són analitzats amb tecnologia d'intel·ligència artificial desenvolupada per Alice Biometrics. També es proporciona un dashboard de supervisió en el qual un operador disposa de tota la informació necessària per a la revisió del procés i les seves evidències.

Totes les tecnologies involucrades han estat desenvolupades per Alice Biometrics, entre elles: extracció del perfil biomètric facial per acarar la identitat contra les fotografies del document; anàlisi PAD i actiu (Presentation Attack Detection o Liveness) per detectar atacs de suplantació d'identitat; lectura automàtica de l'anvers i el revers del document; i anàlisi automàtica de seguretat documental.

Observacions

CCN-STIC-1626 Procediment d'Ocupació Assegurança Alice Biometrics

MobbScan 2.25

Versió	2.25
Fabricant	Mobbeel, SL
Família	Eines de videoidentificació
Tipus	Servei
Data Inclusió	11/07/2023
Revisió de Validesa	31/07/2024

Descripció

MobbScan és una eina que permet l'autenticació i videoidentificació remota d'usuaris de manera segura i confiable. Per a això incorpora una Serie de mòduls que possibiliten recaptar i validar la informació personal d'un usuari mitjançant l'anàlisi del seu document d'identitat i posteriorment comprovar mitjançant biometria facial que la persona que realitza el tràmit és la propietària del mateix. Durant tot el procés es generen una Serie de mostres i evidències que són emmagatzemades temporalment de manera segura fins que un agent autoritzat pugui revisar-les i validar-les a través d'un portal web que assisteix en aquesta tasca (procés desatès o asíncron). El sistema utilitza tecnologies d'intel·ligència artificial per realitzar comprovacions sobre el document d'identitat que permetin determinar la seva integritat (validesa de les dades) o possible ús fraudulent (ús de còpies o reproduccions digitals). El motor biomètric compta amb tecnologies avançades que permeten detectar intents d'atacs de suplantació mitjançant l'ús d'instruments com màscares, pantalles, caracterització o deepfake. Les conclusions d'aquestes anàlisis es mostren igualment a l'agent encarregat de prendre la decisió sobre la validesa del procés per facilitar la seva tasca i afegir una capa extra de seguretat i robustesa a la solució."

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

Veridas Identity verification service

Versió

Fabricant Veridas Digital Authentication Solutions, S.L.

Família Eines de videoidentificació

Tipus Servei

Data Inclusió 01/09/2022

Revisió de Validesa 31/08/2024

Descripció

Solució biomètrica de verificació digital de la identitat consistent en una validació del document acreditatiu de la identitat presentat (DNI, passaport, etc.), una comparació biomètrica entre la foto inclosa en el document i un selfie de la persona que realitza el procés, una prova de vida activa i un procés de vídeo identificació. Addicionalment, la solució també inclou una eina de monitoratge preparada per a la revisió manual de tots els processos realitzats per part d'un agent.

A través de tots aquests passos, Veridas és capaç de verificar, de manera completament automàtica, la identitat de la persona que realitza aquest procés en remot. Tota la tecnologia inclosa en la solució, sense excepció, ha estat dissenyada i produïda per Veridas, apostant per la privacitat per defecte i des del disseny com un pilar fonamental.

Observacions

CCN-STIC-1619 Procediment d'Ocupació Assegurança Veridas Identity Verification Service

Mi eID eSIGN

Versió	1.2
Fabricant	ANF Certification Authority
Família	Eines de videoidentificació
Tipus	Producte
Data Inclusió	31/10/2023
Revisió de Validesa	30/06/2024

Descripció

Sistema d'identificació remota no assistit, multiplataforma i multi-idioma per a l'emissió de certificats qualificats, onboarding, contractació en línia, certificació de manifestacions de voluntat i actes de presència en remot. Incorpora intel·ligència artificial i tecnologia NFC (lectura xip DNIe i en NIE).

Verifica de manera automàtica la identitat de la persona; comprova l'autenticitat, vigència i integritat dels documents d'identificació i la seva correspondència amb la persona que està en la seva possessió, obté evidència certificada de vídeo i so. Comprova que el subjecte és viu, no utilitza màscares, ni empra instruments de falsificació d'imatge.

Compleix l'Ordre ETD/743/2022, relativa als mètodes d'identificació remota per a l'expedició de certificats electrònics qualificats.

Incorpora servei de signatura i segellament electrònic qualificat, estampació de temps electrònic qualificat, servei qualificat de conservació d'evidències a llarg termini, i servei qualificat de validació de signatures i segells electrònics, en la generació de les seves evidències amb plena eficàcia jurídica.

Observacions

Procediment d'ocupació assegurança pendent de publicació

ElectronicID VideoID High Solution

Versió	3.1
Fabricante	Signicat SLU (anteriorment ElectronicID)
Família	Eines de videoidentificació
Tipus	Servei
Data Inclusió	01/12/2022
Revisió de Validesa	01/12/2024

Descripció

Solució de videoidentificació i verificació d'identitat que permet la identificació remota del sol·licitant mitjançant la comparació de la informació biomètrica facial extreta del document d'identitat i la biometria facial de la persona que realitza el procés. VideoID combina tecnologies de transmissió de vídeo amb algoritmes d'intel·ligència artificial per garantir la identificació biomètrica del subjecte, així com l'avaluació de certes característiques del document d'identitat.

El procés a seguir inclou l'acreditació d'identitat mitjançant la mostra de les dues cares del document, el seu holograma i una prova de vida. Addicionalment, el sistema permet la validació d'una OTP dins del propi procés de videoidentificació.

S'inclou també la plataforma de verificació d'identitat per part d'un agent on es realitza la revisió manual de les evidències registrades, així com l'avaluació de diferents elements de seguretat que donin suport a la verificació. El procés d'identificació, per tant, és desatès i asíncron.

Observacions

CCN-STIC-1620 Procediment d¡ocupació assegurança ElectronicID VideoID High Solution

Entrust VIRA

Versió	13.7.0 (VIRA) / 9.4.7 (JIRA)
Fabricant	Entrust Solutions
Família	Eines de videoidentificació
Tipus	Producte
Data Inclusió	01/11/2022
Revisió de Validesa	31/10/2024

Descripció

Producte Software que implementa la gestió segura d'evidències de vídeo identificació obtingudes des del Servei de Verificació de la Identitat de Verides. Entrust VIRA ha estat dissenyat per complir amb totes les mesures de seguretat aplicables a aquest tipus de productes, i per al seu ús en un QTSP que compleixi amb l'Ordre Ministerial ETD/743/2022, de 26 de juliol, per la qual es regulen els mètodes d'identificació remota per vídeo per a l'expedició de certificats electrònics qualificats.

El producte Entrust VIRA està basat en un cas d'ús en el qual l'operador no està present en el procés d'identificació (procés desatès). En aquest cas, l'operador de videotrucades no interacciona amb l'usuari que s'ha d'identificar, sinó que aquest només consulta i analitza les evidències (imatges, vídeos i resultats de les validacions automàtiques) prèviament emmagatzemades en els sistemes d'informació de la plataforma. L'operador accedeix al panell de control en el qual es mostren les evidències necessàries per a l'aprovació, i aprova o rebutja la identificació de la persona, basant-se en l'anàlisi de les evidències.

Observacions

No es considera necessària la publicació del Procediment d'Ocupació Assegurança associada.

7.7.8. COMMUTADORS KVM

KVS4-4004DHVX

Versió	4.11.111
Fabricant	Black Box
Família	Commutadors KVM
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	31/05/2025

Descripció

Commutadors KVM (Keyboard, Video and Mouse) assegurances de Black Box, amb connectivitat de vídeo DVI/HDMI/DisplayPort, que proporcionen aïllament de ports entre xarxes garantint que no existeixin fuites de dades entre els ports segurs i el món exterior. Aquests dispositius permeten controlar múltiples ordinadors des d'un sol teclat, monitor i ratolí, fins i tot amb diversos canals de vídeo i una combinació de perifèrics USB.

A més, disposen d'un port CAC (Common Access Card), que permet als administradors autenticats registrar i assignar dispositius perifèrics específics al port CAC.

Observacions

Black Box Secure KVM Administration and Security Management Tool Guide (CAC) (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd1.pdf) ADVANCED 4-PORT DP, HDMI & DVI-I SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd2.pdf)

KVS4-2002VX, KVS4-2002HVX, KVS4-1004HVX, KVS4-2004HVX

Versió	4.11.202
Fabricant	Black Box
Família	Commutadors KVM
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	31/05/2025

Descripció

Commutadors KVM (Keyboard, Video and Mouse) assegurances de Black Box, amb connectivitat de vídeo DisplayPort/HDMI, que proporcionen aïllament de ports entre xarxes garantint que no hi hagi fuites de dades entre els ports segurs i el món exterior. Aquests dispositius permeten controlar múltiples ordinadors des d'un sol teclat, monitor i ratolí, fins i tot amb diversos canals de vídeo i una combinació de perifèrics USB.

A més, disposen d'un port CAC (Common Access Card), que permet als administradors autenticats registrar i assignar dispositius perifèrics específics al port CAC.

Observacions

Black Box Secure KVM Administration and Security Management Tool Guide (CAC) (https://www.niapccevs.org/MMO/Product/st_vid11240-agd1.pdf) ADVANCED 4-PORT DP, HDMI & DVI-I SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd2.pdf) ADVANCED 2/4/8-PORT DISPLAYPORT SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd3.pdf) ADVANCED 2/4-PORT DP/HDMI SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd4.pdf) ADVANCED 2/4-PORT DP MST SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd5.pdf) ADVANCED 2/4/8-PORT DVI-I SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd7.pdf)

KVS4-8004VPX

Versió 4.11.004

Fabricant Black Box

Família Commutadors KVM

Tipus Producte

Data Inclusió 01/01/2023

Revisió de Validesa 31/01/2024

Descripció

Commutadors KVM (Keyboard, Video and Mouse) segurs de Black Box, amb connectivitat de vídeo DisplayPort i funcionalitat de multivisor, que proporcionen aïllament de ports entre xarxes garantint que no existeixin fuites de dades entre els ports segurs i el món exterior. Aquests dispositius permeten controlar múltiples ordinadors des d'un sol teclat, monitor i ratolí, fins i tot amb diversos canals de vídeo i una combinació de perifèrics USB.

A més, disposen d'un port CAC (Common Access Card), que permet als administradors autenticats registrar i assignar dispositius perifèrics específics al port CAC.

Observacions

Black Box Secure KVM Administration and Security Management Tool Guide (CAC) (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd1.pdf) ADVANCED 4-PORT DP, HDMI & DVI-I SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd2.pdf)

KVS4-2002VX, KVS4-2004VX, KVS4-4004VX, KVS4-1008VX, KVS4-2008VX

Versió	4.11.001
Fabricant	Black Box
Família	Commutadors KVM
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	31/01/2024

Descripció

Commutadors KVM (Keyboard, Video and Mouse) assegurances de Black Box, amb connectivitat de vídeo DisplayPort, que proporcionen aïllament de ports entre xarxes garantint que no hi hagi fuites de dades entre els ports segurs i el món exterior. Aquests dispositius permeten controlar múltiples ordinadors des d'un sol teclat, monitor i ratolí, fins i tot amb diversos canals de vídeo i una combinació de perifèrics USB.

A més, disposen d'un port CAC (Common Access Card), que permet als administradors autenticats registrar i assignar dispositius perifèrics específics al port CAC.

Observaciones

Black Box Secure KVM Administration and Security Management Tool Guide (CAC) (https://www.niapccevs.org/MMO/Product/st_vid11240-agd1.pdf) ADVANCED 4-PORT DP, HDMI & DVI-I SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd2.pdf) ADVANCED 2/4/8-PORT DISPLAYPORT SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd3.pdf) ADVANCED 2/4-PORT DP/HDMI SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd4.pdf) ADVANCED 2/4-PORT DP MST SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd5.pdf) ADVANCED 2/4/8-PORT DVI-I SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd7.pdf)

KVS4-2004DX, KVS4-1008DX, KVS4-2008DX

Versió	4.11.010
Fabricant	Black Box
Família	Commutadors KVM
Tipus	Producte
Data Inclusió	01/01/2023
Revisió de Validesa	31/05/2025

Descripció

Commutadors KVM (Keyboard, Video and Mouse) segurs de Black Box, amb connectivitat de vídeo DVI, que proporcionen aïllament de ports entre xarxes garantint que no hi hagi fuites de dades entre els ports segurs i el món exterior. Aquests dispositius permeten controlar múltiples ordinadors des d'un sol teclat, monitor i ratolí, fins i tot amb diversos canals de vídeo i una combinació de perifèrics USB.

A més, disposen d'un port CAC (Common Access Card), que permet als administradors autenticats registrar i assignar dispositius perifèrics específics al port CAC.

Observacions

Black Box Secure KVM Administration and Security Management Tool Guide (CAC) (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd1.pdf) ADVANCED 4-PORT DP, HDMI & DVI-I SECURE KVM SWITCH (https://www.niap-ccevs.org/MMO/Product/st_vid11240-agd2.pdf)

7.7.9. SISTEMES DE GESTIÓ DE BASES DE DADES (DBMS)

Oracle Database 19c Enterprise Edition - Relational Database Management System

Versió	19.11 with Critical Patch Update April 2021
Fabricant	Oracle America Inc.
Família	Sistemes de Gestió de Bases de Dades (DBMS)
Tipus	Producte
Data Inclusió	01/07/2023
Revisió de Validesa	31/01/2024

Descripció

La base de dades (BD) és una recopilació organitzada d'informació o dades estructurades, que normalment s'emmagatzema de manera electrònica en un sistema informàtic. Normalment, una base de dades està controlada per un sistema de gestió de bases de dades (DBMS). En conjunt, les dades i el DBMS, juntament amb les aplicacions associades a ells, reben el nom de sistema de bases de dades, abreujat normalment a simplement base de dades. Un DBMS serveix com a interfície entre la base de dades i els seus programes o usuaris finals, la qual cosa permet als usuaris recuperar, actualitzar i gestionar com s'organitza i s'optimitza la informació.

La DB de Oracle d'autogestió està preparada per a proporcionar un impuls significatiu a aquestes capacitats. Atès que les bases de dades d'autogestió automatitzen processos manuals costosos i tediosos, alliberen els usuaris empresarials perquè puguin ser més proactius amb les seves dades. En tenir control directe sobre la capacitat de crear i utilitzar bases de dades, els usuaris guanyen control i autonomia al mateix temps que mantenen importants estàndards de seguretat.

Observacions

Procediment d'Ocupació Segura pendent de publicació

7.8. ALTRES EINES

7.8.1. ALTRES EINES

AWS Security Hub	
Versió	
Fabricant	AWS
Família	Altres Eines
Tipus	Servei
Data Inclusió	01/02/2024
Revisió de Validesa	31/07/2024

Descripció

AWS Secrets Manager l'ajuda a protegir els secrets necessaris per a accedir a les seves aplicacions, serveis i recursos de IT. El servei li permet girar, administrar i recuperar fàcilment les credencials de les bases de dades, les claus de API i altres dades secretes al llarg del seu cicle de vida. Els usuaris i les aplicacions recuperen les dades confidencials amb una anomenada a les API de Secrets Manager, la qual cosa elimina la necessitat de codificar la informació confidencial en text pla. Secrets Manager ofereix una rotació de secrets amb una integració incorporada per a Amazon RDS, Amazon Redshift i Amazon DocumentDB. El servei també es pot estendre a altres tipus de secrets, incloses les claus de API i els tokens de OAuth. A més, Secrets Manager li permet controlar l'accés a les dades secretes mitjançant permisos detallats i auditar la rotació de secrets de forma centralitzada per als recursos en els Núvol de AWS serveis de tercers i en les instal·lacions.

Per a més informació: https://aws.amazon.com/es/secrets-manager/

Observacions

Procediment d'Ocupació Assegurança pendent de publicació.

Amazon Macie

Versió	2020-01-01
Fabricante	AWS
Família	Altres Eines
Tipus	Servei
Data Inclusió	07/05/2024
Revisió de Validesa	31/10/2024

Descripció

Amazon Macie és un servei de seguretat i privacitat de dades totalment administrat que utilitza avaluacions d'inventari, aprenentatge automàtic i coincidència de patrons per a descobrir dades confidencials i accessibilitat en el seu entorn de Amazon S3. Macie suporta treballs escalables de descobriment de dades confidencials sota demanda i automatitzats que rastregen automàticament els canvis en el bucket i només avaluen els objectes nous o modificats al llarg del temps. Amb Macie, pot detectar una llista àmplia i creixent de tipus de dades confidencials per a molts països i regions, inclosos diversos tipus de dades financeres, informació sanitària personal (PHI) i informació d'identificació personal (PII), així com tipus personalitzats. Macie també avalua contínuament el seu entorn Amazon S3 per a proporcionar un resum de recursos S3 i una avaluació de la seguretat en tots els seus comptes. Pot buscar, filtrar i ordenar els buckets de S3 per variables de metadades, com a noms de buckets, etiquetes i controls de seguretat com l'estat de xifratge o l'accessibilitat pública. En el cas dels buckets sense xifrar, els buckets d'accés públic o els buckets compartits amb comptes de AWS que no siguin les que ha definit en Organitzacions de AWS, pot rebre una alerta perquè actuï. Per a més informació: https://aws.amazon.com/es/macie/

Observacions

Procediment d'Ocupació Segura pendent de publicació

AWS Config

Versió

Fabricant AWS

Família Altres Eines

Tipus Servei

Data Inclusió 01/08/2022

Revisió de Validesa 30/06/2024

Descripció

AWS Config és un servei totalment administrat que proporciona un inventari de recursos d'AWS, un historial de configuració i notificacions de canvis de configuració per permetre la seguretat i la governança. La funció AWS Config Rules permet crear regles que comproven automàticament la configuració dels recursos d'AWS registrats per AWS Config. El servei permet descobrir els recursos d'AWS existents i eliminats, determinar la seva conformitat general amb les regles i aprofundir en els detalls de configuració d'un recurs en qualsevol moment. Aquestes capacitats permeten l'auditoria de conformitat, l'anàlisi de seguretat, el seguiment dels canvis en els recursos i la resolució de problemes.

Per a més informació sobre AWS Config, vegi https://aws.amazon.com/config/?nc1=h_ls

Observacions

CCN-STIC-887A Guía de configuración segura AWS

Amazon S3 Glacier

Versió

Fabricante AWS

Família Altres Eines

Tipus Servei

Data Inclusió 01/02/2024

Revisió de Validesa 31/07/2024

Descripció

AWS S3 Glacier és un servei d'emmagatzematge segur, durador i de baix cost que habilita l'arxivat i la realització de còpies de seguretat de les dades a llarg termini en magatzems (anomenats volts). Per a més informació, consultar https://docs.aws.amazon.com/es_es/amazonglacier/latest/dev/introduction.html

Observacions

Procediment d'ocupació segura pendent de publicació

Amazon EC2 Auto Scaling

Versió

Fabricante AWS

Família Altres Eines

Tipus Servei

Data Inclusió 01/02/2024

Revisió de Validesa 31/07/2024

Descripció

Amazon EC2 Acte Scaling l'ajuda a mantenir la disponibilitat de les aplicacions i li permet afegir o eliminar automàticament instàncies d'EC2 segons les condicions que defineixi. Pot utilitzar les funcions d'administració de flotes de Amazon EC2 Acte Scaling per a mantenir l'estat i la disponibilitat de la seva flota. També pot utilitzar les funcions d'escalat dinàmic i predictiu de Amazon EC2 Acte Scaling per a afegir o eliminar instàncies d'EC2. L'escalat dinàmic respon als canvis en la demanda i l'escalat predictiu programa automàticament el nombre correcte d'instàncies d'EC2 en funció de la demanda prevista. Per a més informació: https://aws.amazon.com/es/ec2/autoscaling/

Observacions

Procediment d'ocupació segura pendent de publicació

Microsoft Defender for Identity

Versió

Fabricant Microsoft Iberica SRL

Família Altres Eines

Tipus Servei

Data Inclusió 01/02/2023

Revisió de Validesa 30/11/2024

Descripció

Microsoft Defender for Identity és una solució de seguretat basada en el núvol que aprofita els senyals d'Active Directory locals per identificar, detectar i investigar amenaces avançades, identitats compromeses i accions internes malicioses dirigides a una organització.

Microsoft Defender for Identity permet als analistes d'operacions de seguretat i als professionals de la seguretat, que poden tenir problemes per detectar atacs avançats en entorns híbrids, identificar i investigar les activitats sospitoses d'usuaris i atacs avançats. Defensar for Identity utilitza perfils del comportament de l'usuari i l'aprenentatge automàtic per crear una línia base normalitzada per a cada usuari. A continuació, identifica anomalies amb indicadors adaptatius que assignen un pes a cada anomalia segons el nivell de risc associat.

Microsoft Defender for Identity és una solució que s'integra amb altres solucions de seguretat com Microsoft 365 Defender, Microsoft Cloud App Security o Azure Sentinel per oferir una visió més completa de l'estat de seguretat i facilitar la resposta a incidents. Es pot implementar mitjançant sensors instal·lats en controladors de domini o mitjançant un agent integrat a Windows Server 2019 o posterior. Defensar for Identity és un producte que s'utilitza per protegir les infraestructures crítiques contra atacs sofisticats com el robatori o l'ús indegut de credencials, el moviment lateral o l'accés no autoritzat a recursos sensibles ajudant a prevenir aquests atacs en alertar sobre activitats sospitoses, proporcionant informació detallada sobre els actors i les tècniques involucrades i suggerir accions correctives per mitigar l'impacte.

Observacions

CCN-STIC-885F Guia de configuració segura per a Microsoft Defender for Identity (Guia en procés d'adaptació)

Cloud Trail

Versió

Fabricant AWS

Família Altres Eines

Tipus Servei

Data Inclusió 01/06/2022

Revisió de Validesa 30/06/2024

Descripció

AWS CloudTrail és un servei web que registra les trucades a l'API d'AWS del seu compte i li entrega arxius de registre. La informació registrada inclou la identitat de la persona que truca a l'API, l'hora de la trucada a l'API, l'adreça IP d'origen de la persona que truca a l'API, els paràmetres de la sol·licitud i els elements de resposta retornats pel servei d'AWS.

Amb CloudTrail, es pot obtenir un historial de trucades a l'API d'AWS per al seu compte, incloses les trucades a l'API realitzades mitjançant la consola d'administració d'AWS, els SDK d'AWS, les eines de línia de comandaments i els serveis d'AWS de nivell superior (com AWS CloudFormation). L'historial de trucades a l'API d'AWS produït per CloudTrail permet l'anàlisi de seguretat, el seguiment dels canvis en els recursos i l'auditoria de conformitat.

Observacions

CCN-STIC-887A Guia de configuració segura AWS

Cisco Unified Communications Manager IM & Presence Service (C220 M5 y C240 M5)

Versió 12.5 y 14 (con Centos 7.7)

Fabricant Cisco Systems

Família Altres Eines

Tipus Servei

Data Inclusió 01/03/2023

Revisió de Validesa 31/08/2025

Descripció

Sistema de comunicacions empresarial que subministra veu i videotelefonades sobre una xarxa IP.

Observacions

CCN-STIC-1460 Procedimiento de Empleo Seguro Cisco Unified Communications Manager (C220 M5 y C240 M5)

TrustCloud

Versió	4
Fabricante	TrustCloud Tech SL
Família	Altres Eines
Tipus	Servei
Data Inclusió	01/01/2023
Revisió de Validesa	31/12/2024

Descripció

La plataforma Trustcloud és un 'Coreògraf de Transaccions digitals segures'. Trustcloud és un Orquestrador d'orquestradors, i els Serveis són proporcionats en model SaaS: Software as a Service. TrustCloud orquestra i blinda les transaccions digitals dutes a terme entre els diferents casos d'ús dels clients. És una plataforma única d'orquestració i custòdia de totes les evidències generades per les transaccions digitals, que permet preservar qualificadament els actius digitals, garantint la seva identitat, integritat i intenció de tots els participants arreu del món, i amb això s'aconsegueix que siguin segures, ja que per si soles no ho són.

Observacions

CCN-STIC-1622 Procediment d'ocupació assegurança TrustCloud

AWS Organizations

Versió

Fabricant AWS

Família Altres Eines

Tipus Servei

Data Inclusió 01/03/2023

Revisió de Validesa 29/02/2024

Descripció

AWS Organizations l'ajuda a administrar i governar de forma centralitzada el seu entorn a mesura que creix i escala els seus recursos d'AWS. Amb AWS Organizations, es pot crear mitjançant programació nous comptes d'AWS i assignar recursos, agrupar comptes per organitzar els seus fluxos de treball, aplicar polítiques a comptes o grups per i simplificar la facturació utilitzant un únic mètode de pagament per a tots els seus comptes.

A més, AWS Organizations s'integra amb altres serveis d'AWS perquè pugui definir configuracions centrals, mecanismes de seguretat, requisits d'auditoria i recursos compartits entre els comptes de la seva organització. AWS Organizations està disponible pera tots els clients d'AWS sense càrrec.

Per a més informació apropa AWS Organizations, visiteu https://aws.amazon.com/es/organizations/

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

Amazon EC2

Versió

Fabricant AWS

Família Altres Eines

Tipus Servei

Data Inclusió 01/02/2024

Revisió de Validesa 31/07/2024

Descripció

Amazon Elastic Computi Cloud (Amazon EC2) és un servei web que proporciona una capacitat informàtica segura i de grandària variable en el núvol. Està dissenyat per a facilitar als desenvolupadors recursos de computació escalables basats en Web. La senzilla interfície web de Amazon EC2 li permet obtenir i configurar la capacitat amb una fricció mínima. Proporciona un control complet sobre els recursos de computació i pot executar-se a l'entorn de computació de Amazon.

Per a més informació: https://aws.amazon.com/es/ec2/

Observacions

CCN-STIC-887A Guía de configuración segura AWS

Amazon EC2

Versió

Fabricant AWS

Família Altres Eines

Tipus Servei

Data Inclusió 01/02/2024

Revisió de Validesa 30/06/2024

Descripció

Amazon CloudFront és un servei de xarxa de lliurament de contingut (CDN) ràpid que envia de manera segura dades, vídeos, aplicacions i API a clients de tot el món amb baixa latència i altes velocitats de transferència, tot això en un entorn fàcil d'usar per als desenvolupadors. CloudFront està integrat amb AWS, tant amb ubicacions físiques connectades directament a la infraestructura global de AWS com amb altres serveis de AWS. CloudFront funciona a la perfecció amb serveis com AWS Shield per a la mitigació de DDoS, Amazon S3, Elastic Lloeu Balancing o Amazon EC2 com a orígens per a les seves aplicacions, i Lambda per a executar codi personalitzat més prop dels usuaris dels clients i personalitzar l'experiència de l'usuari.

Pot començar a utilitzar la xarxa de lliurament de contingut en qüestió de minuts, utilitzant les mateixes eines de AWS amb les quals ja està familiaritzat: API, consola d'administració de AWS, AWS CloudFormation, CLI i SDK. Amazon CDN ofereix un model de preus senzill, de pagament per ús, sense quotes inicials ni contractes a llarg termini, i el suport per a la CDN està inclòs en la seva subscripció existent a AWS Support.

Per a més informació consulti https://aws.amazon.com/es/cloudfront/

Observacions

Procediment d'Ocupació Segura pendent de publicació

AWS Security Hub

Versió

Fabricant AWS

Família Altres Eines

Tipus Servei

Data Inclusió 01/09/2022

Revisió de Validesa 30/06/2024

AWS Security Hub

Descripció

AWS Security Hub és un servei de gestió de la seguretat al núvol que realitza comprovacions automatitzades i contínues de les millors pràctiques de seguretat dels recursos dels seus comptes AWS d'acord a l'estàndard AWS Foundational Security Best Practices i altres marcs de conformitat.

Per mantenir una visió completa de la seva postura de seguretat, Security Hub genera una puntuació de seguretat consolidada en tots els seus comptes d'AWS, per a la qual cosa necessita integrar múltiples eines i serveis, incloses deteccions d'amenaces d'Amazon GuardDuty, vulnerabilitats d'Amazon Inspector, classificacions de dades confidencials d'Amazon Macie, problemes de configuració de recursos d'AWS Config i productes de la xarxa de socis d'AWS.

Security Hub agrega totes aquestes troballes de seguretat en un sol lloc i format a través del format de troballes de seguretat d'AWS, i redueix el seu temps mitjà de reparació (MTTR) amb resposta automatitzada i suport de reparació.

També es pot integrar amb eines d'emissió de tiquets, xat, SIEM, SOAR, GRC i gestió d'incidents per proporcionar als seus usuaris un flux de trabaix complet d'operacions de seguridad. Per a més informació sobre AWS Security Hub, visiteu: https://aws.amazon.com/es/security-hub/

Observacions

CCN-STIC-887A Guía de configuración segura AWS

authUsb safeDoor

Versió 2.0.0.11

Fabricant authUSB

Família Altres Eines

Tipus Producte

Data Inclusió 01/05/2019

Revisió de Validesa 30/06/2024

Descripció

AuthUsb safeDoor és un dispositiu maquinari que actua com a barrera entre les memòries USB i els equips d'una organització, identificant amenaces a tres nivells:

- Elèctric: identificant i detenint atacs destructius de sobretensió tipus UsbKiller.
- Hardware: detectant i desactivant atacs de la família BadUsb, atacs HID (rubber ducky i similars), falses targetes de xarxa, interfícies compostes, etc.
- Software: antivirus integrat que realitza una anàlisi prèvia a la descàrrega de qualsevol contingut.

Observacions

CCN-STIC 1201 Procediment d'Ocupació Assegurança AuthUsb SafeDoor

Personal Code

Versió 2020.3

Fabricant HUBOX

Família Altres Eines

Tipus Producte

Data Inclusió 01/09/2021

Revisió de Validesa 31/03/2026

PERSONAL CODE©

Descripció

PERSONAL CODE és una solució d'identitat digital que resol el problema de fraus per suplantació d'identitat. Vegeu la solució com una seqüència de bits que emmagatzema, de forma segura, característiques biomètriques i informació biogràfica d'un individu. Aquestes dades són signes i reconegudes per una autoritat i es protegeixen mitjançant criptografia asimètrica per a la seva posterior verificació a través d'una aplicació que no requereix connectivitat ni consultes a bases de dades. PERSONAL CODE implementa la seva solució en forma de dues llibreries o DLLs, una llibreria de generació que s'encarrega de processar la informació de l'individu i una altra de verificació per a la posterior extracció i validació de les dades.

Observacions

CCN-STIC-1218 Procediment d'ocupació assegurança Personal Code d'HUBOX

7.9. SEGURETAT OT

7.9.1. SEGURETAT OT

Àgata	
Versió	2.3.3
Fabricant	Àgata Technology
Família	Seguretat OT
Tipus	Producte
Data Inclusió	01/12/2021
Revisió de Validesa	30/06/2024

Descripció

Àgata és una plataforma Software que permet la digitalització, optimització i automatització de processos de negoci, posant la tecnologia al servei de les persones. Àgata integra en un únic entorn tecnològic tots els processos i serveis d'una organització permetent gestionar-los de manera senzilla, eficient, sostenible i segura.

Observacions

CCN-STIC 1305 Procediment d'ocupació assegurança AGATA

8. PRODUCTES APROVATS

8.1 EINES PER AL DESENVOLUPAMENT DE PRODUCTES DE SEGURETAT

Mòdul criptogràfic per aplicacions mòbils Telcryp

Versió	1.11
Fabricant	Cryptographic and Security System (CS2)
Família	-
Tipus	Producte
Data Inclusió	01/10/2023
Revisió de Validesa	31/10/2025

Descripció

Aquest mòdul proveeix els serveis de xifrat i seguretat per garantir la comunicació tant amb el servidor IMS com amb els terminals remots amb un xifrat extrem a extrem.

Aquest mòdul criptogràfic està dissenyat com una llibreria criptogràfica i incorporat a aplicacions de comunicacions en entorn de mobilitat degudament aprovades, i instal·lades en plataformes confiables.

Observacions

Procediment d'ocupació pendent de publicació

8.2 CONTROL D'ACCÉS

8.2.1 CONTROL D'ACCÉS A XARXA (NAC)

Forescout 8.3 (CT-R, CT-100, CT-1000, CT-2000, CT-4000, CT-10000, CEM-5, CEM-10, CEM-25, CEM-50,CEM-100, CEM-150, CEM-200, 4130, 5110, 5120, 5140, 5160)

Versió	8.4
Fabricant	Forescout
Família	Control d'accés a xarxa (NAC)
Tipus	Producte
Data Inclusió	01/05/2023
Revisió de Validesa	31/10/2025

Descripció

La plataforma Forescout és una plataforma unificada de seguretat que permet a les empreses i organismes oficials obtenir informació completa sobre l'estat dels seus entorns empresarials ampliats i orquestrar mesures destinades a reduir el risc operatiu i de ciberseguretat. Es desplega de forma ràpida i segura en entorns de campus, centres de dades, el núvol i xarxes d'OT. Ofereix descobriment, classificació en temps real i avaluació continua d'estat, sense necessitat d'agents. Per a més informació, vegeu: https://forescouttechnologies.es

Observacions

CCN-STIC-1106 Procediment d'ocupació assegurança Forescout

8.2.2. GESTIÓ D'IDENTIATS (IM)

CyberArk Privileged Account Security Solution

Versió	V8.3p2
Fabricant	Sailpoint
Família	Gestió d'accés privilegiat (PAM)
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	31/12/2025

Descripció

Sailpoint és una plataforma de Gestió d'Identitats i Accessos que ofereix una àmplia gamma de funcionalitats, la qual cosa ho converteix en una solució integral per a la gestió de les identitats en les organitzacions:

- Provisionamiento: onboarding de nous usuaris, canvis i donis provisionament, automatització en els processos. Per a usuaris interns, col·laboradors i/o proveïdors.
- Govern d'accés: Visibilitat completa dels accessos de l'organització, certificació d'accés, compliment d'accés segons polítiques d'usuaris a aplicacions i dades.
- Gestió de contrasenyes.
- Segregació de funcions.
- Govern de núvol.

Observacions

CCN-STIC-1111 SAILPOINT IdentityIQ

8.3.SEGURETAT A L'EXPLOTACIÓ

8.3.1 ANTI-VIRUS / EPP (ENDPOINT PROTECTION PLATFORM)

Deep Security (Manager i Agent/Relay Linux/Windows)	
Versió	11.0
Fabricant	Trend Micro
Família	Anti-virus / EPP (Endpoint Protection Platform)
Tipus	Producte
Data Inclusió	01/12/2021
Revisió de Validesa	31/07/2024
Descripció	

Deep Security és la resposta de Trend Micro per protegir el cloud híbrid siguin servidors físics o virtuals.

Gràcies al seu agent lleuger, el qual incorpora funcionalitats: EDR (amb resposta enfront d'amenaces conegudes, zero-day), enviament de telemetria a la plataforma XDR de Trend Micro (VisionOne), reputació web, control d'aplicacions, supervisió de logs, Supervisió d'Integritat (FIM), Firewall de Host i Host IPS (que incorpora la tecnologia de apedaçament virtual), ajuda a millorar la postura de seguretat proporcionant seguretat, visibilitat i control. La qualificació abasta els següents components: Manager, Agent/Relay Linux i l'Agent/Relay Windows. El Virtual Appliance no està qualificat.

Observacions

CCN-STIC-1216 PES Trendmicro Deep Security

8.3.2 EDR (ENDPOINT DETECTION AND RESPONSE)

Deep Security (Manager i Agent/Relay Linux/Windows)	
Versió	11.0
Fabricant	Trend Micro
Família	EDR (Endpoint Detection and Response)
Tipus	Producte
Data Inclusió	01/12/2021
Revisió de Validesa	31/05/2024
Descripció	

Deep Security és la resposta de Trend Micro per protegir el cloud híbrid siguin servidors físics o virtuals.

Gràcies al seu agent lleuger, el qual incorpora funcionalitats: EDR (amb resposta enfront d'amenaces conegudes, zero-day), enviament de telemetria a la plataforma XDR de Trend Micro (VisionOne), reputació web, control d'aplicacions, supervisió de logs, Supervisió d'Integritat (FIM), Firewall de Host i Host IPS (que incorpora la tecnologia de apedaçament virtual), ajuda a millorar la postura de seguretat proporcionant seguretat, visibilitat i control. La qualificació abasta els següents components: Manager, Agent/Relay Linux i l'Agent/Relay Windows. El Virtual Appliance no està qualificat.

Observacions

CCN-STIC-1216 PES Trendmicro Deep Security

8.3.3 EINES DE FILTRATGE DE NAVEGACIÓ

Cisco Web Security Appliance (S690, S690X, S695, S695F, S680, S390, S380, S395, S190, S195)	
Versió	AsyncOS 11.8
Fabricant	Cisco Systems
Família	Eines de filtratge de navegació
Tipus	Producte
Data Inclusió	01/12/2022
Revisió de Validesa	31/05/2025

Descripció

Cisco Secure Web Appliance proxy protegeix les organitzacions quant a navegació es refereix, avaluant les webs desconegudes abans de permetre que els usuaris hi accedeixin i bloquejant automàticament les pàgines de risc. Utilitzant funcions d'alt rendiment, Cisco Secure Web Appliance manté segurs els usuaris.

Observacions

CCN-STIC-1625 Procediment d'Ocupació Segur Cisco Web Security Appliance

8.3.4 SISTEMES DE GESTIÓ D'ESDEVENIMENTS DE SEGURETAT (SIEM)

MONICA

Versió	7.1
Fabricant	Grupo ICA Sistemas y Seguridad
Familia (SIEM)	Sistemes de gestió d'esdeveniments de seguretat
Tipus	Producte
Data Inclusió	01/05/2023
Revisió de Validesa	30/06/2024

Descripció

La plataforma espanyola Mónica permet als analistes de ciberseguretat recopilar logs i informació il·limitada de seguretat, detectar atacs basats en anomalies i comportaments desconeguts, així com automatitzar la resposta davant incidents en entorns IT, OT i IoT. Mónica recopila informació de qualsevol font interna i externa a l'empresa (comercial, propietària, aplicacions, cloud), correlando i analitzant en temps real aquesta informació, permetent contextualitzar i prioritzar els incidents de seguretat tant interns com externs. Combina els casos d'ús de detecció més sofisticats amb la informació més precisa d'amenaces i vulnerabilitats zero day gràcies a la informació de fonts externes d'intel·ligència, threat hunting i anomalies de xarxa/usuari

Observacions

CCN-STIC-1206 PES NGSIEM LogICA

MONSE

Versió	Probe 1.0, Agente 8.3.2
Fabricant	GRUPO CIES
Familia (SIEM)	Sistemes de gestió d'esdeveniments de seguretat
Tipus	Producte
Data Inclusió	N/A
Revisió de Validesa	01/11/2024

Descripció

MONSE (Monitoratge de la Seguretat) és una solució SIEM que permet recopilar i correlacionar de forma centralitzada múltiples fonts d'esdeveniments de seguretat. La solució permet analitzar esdeveniments basats en logs, processos, comportament i IOCs. Disposa de tècniques d'Intel·ligència Artificial que faciliten la detecció d'anomalies, integració de fonts d'intel·ligència d'amenaces, possibilitat de definir regles d'alerta adaptades a la particularitat de cada organització, així com la possibilitat de crear quadres de comandament personalitzables. La plataforma permet un desplegament modular en funció del tipus de maduresa de l'organització. Disposa de múltiples funcionalitats orientades a la millora en el compliment de l'Esquema Nacional de Seguretat.

Observacions

CCN-STIC 1223 Procedimiento de empleo seguro MONSE

NetWitness Platform

Versió	11.6
Fabricant	Netwitness, an RSA Business.
Familia	Sistemes de gestió d'esdeveniments de seguretat (SIEM)
Tipus	Producte
Data Inclusió	01/07/2022
Revisió de Validesa	31/12/2024

Descripció

La plataforma XDR de Netwitness (an RSA Business), és la solució de SIEM o XDR (eXtended Detection and Response), amb capacitats de visibilitat completa gràcies al seu model de dades unificat podent capturar logs, netflows, trànsit de xarxa, activitat en els end points, a més d'informació d'intel·ligència de seguretat, de forma integrada, sota un únic motor d'anàlisi i correlació avançada. A més, inclou funcionalitats necessàries per un SOC per fer front a amenaces complexes. Netwitness Platform XDR compta a més amb components addicionals com UEBA (User and Entity Behaviour Analitics) i SOAR (Security Orchestration and Automation Response). La solució permet capturar tot tipus d'informació, permetent l'anàlisi avançada d'amenaces, priorització en base al context de negoci i fent més eficient el treball de l'analista. És una plataforma que, gràcies a la seva capacitat d'anàlisi, mostra l'abast complet d'un atac als analistes. A més, gràcies a la seva estratègia Run Anywhere, la plataforma es pot desplegar en qualsevol entorn (virtual, cloud, físic o híbrid), així com fer front a arquitectures altament distribuïdes. RSA Netwitness inclou en tots els seus clients +50 feeds d'intel·ligència, agent per a endpoints il·limitats, així com el desplegament il·limitat de dispositius per a quantesforma de desplegament. https://www.netwitness.com/en-us /solutions/evolved-siem/

Observacions

CCN-STIC-1210 Procediment d'Ocupació Segur RSA Netwitness Platform

Gloria

Versió	v5.8.1
Fabricant	S2 GRUPO / CCN
Família	Sistemes de gestió d'esdeveniments de seguretat (SIEM)
Tipus	Producte
Data Inclusió	01/10/2023
Revisió de Validesa	30/06/2024

Descripció

Glòria és una plataforma per a la gestió d¡incidents i amenaces de ciberseguretat a través de tècniques de correlació complexa d'esdeveniments. Basat en els sistemes SIEM, va un pas més enllà de les capacitats de monitoratge, emmagatzematge i interpretació de les dades rellevants. Així, mitjançant tècniques de correlació complexa de diverses fonts d'esdeveniments o anàlisi de patrons per a la identificació d'anomalies, permet una orientació molt flexible cap a la vigilància del món IP. La plataforma permet les següents funcionalitats a través de diferents mòduls:

- Monitoratge d'entorns tecnològics (IT/OT).
- Intel·ligència.
- Gestió del servei.
- Automatització, orquestració i reducció de temps de resposta.

Per a més informació, (https://ccn-cert.cni.es/soluciones-seguridad/gloria.html)

Observacions

CCN-STIC-1215 Procediment d'ocupació segur GLORIA

LogICA5 Next Generation SIEM

Versió	v7.1
Fabricant	Grup ICA Sistemes i Seguretat
Família	Sistemes de gestió d'esdeveniments de seguretat (SIEM)
Tipus	Producte
Data Inclusió	01/01/2020
Revisió de Validesa	30/06/2024

Descripció

La plataforma espanyola Next Generation SIEM LogICA permet als analistes de ciberseguretat recopilar logs i informació il·limitada de seguretat, detectar atacs basats en anomalies i comportaments desconeguts així com automatitzar la resposta davant incidents en entorns IT, OT i IoT. LogICA NG SIEM recopila informació de qualsevol font interna i externa a l'empresa (comercial, propietària, aplicacions, cloud), correlant i analitzant en temps real aquesta informació, permetent contextualitzar i prioritzar els incidents de seguretat tant interns com externs. Combina els casos d'ús de detecció més sofisticats amb la informació més precisa d'amenaces i vulnerabilitats gràcies a la informació de fonts externes d'intel·ligència, threat hunting i anomalies de xarxa/usuari. Incorpora, a més, un quadre de comandament de gestió del servei, centralitzant la informació i facilitant el seu consum per part de l'organització. LogICA permet adaptar-se a les necessitats de desplegament de les organitzacions, en mode on-premise, virtual o entorn cloud.

Observacions

CCN-STIC-1206 PES NGSIEM LogICA

8.3.5 DISPOSITIUS PER A GESTIÓ DE CLAUS CRIPTOGRÀFIQUES

EP543N

Versió V.1.7

Fabricant Epicom

Família Dispositius per a gestió de claus criptogràfiques **Tipu**

Producte

Data Inclusió 27/12/2021

Revisió de Validesa 31/12/2024

Descripció

Centre de Gestió de xifradors IP EP430GN sobre ordinador segur EP1140.

Observacions

EP543X

Versió SW v 4.15

Fabricant Epicom

Família Dispositius per a gestió de claus criptogràfiques

Tipus Producte

Data Inclusió 01/12/2017

Revisió de Validesa 31/12/2024

Descripció

Centre de Gestió sobre la plataforma EP1140, que dona suport als xifradors de la família EP430, inclosos els models EP430TX i EP430GX.

Observacions

Utilització segons PE-2012-49 Procediment d'Ocupació EP430GX v2

8.4 MONITORITZACIÓ DE LA SEGURETAT

8.4.1 CAPTURA, MONITORATGE I ANÀLISI DE TRÀNSIT

CARMEN	
Versió	Versió 7.16.2
Fabricant	S2 GRUPO / CCN
Família	Captura, Monitoratge i Anàlisi de Trànsit
Tipus	Producte
Data Inclusió	01/06/2022
Revisió de Validesa	30/06/2024

Descripció

CARMEN (Centre d'Anàlisi de Registres i Mineria d'EveNtos) és una solució Software d'adquisició, processament i anàlisi d'informació per suportar el procés d'identificació d'Amenaces Persistents Avançades (APT) a partir del trànsit de xarxa intern i sortint d'una forma eficient, donant suport a la presa de decisions a partir de la informació generada i processada. Es compon d'agents que recopilen els fluxos de trànsit, un motor d'emmagatzematge en el qual s'insereix la informació, un sistema de detecció d'anomalies que s'encarrega de processar la informació emmagatzemada i una aplicació web que permet la representació i consulta tant de la informació obtinguda com de la processada. Per a més informació, es potconsultar el web del CCN-CERT (https://ccn-cert.cni.es/soluciones-seguridad/carmen.html)

Observacions

CCN-STIC-1304 Procediment d'ocupació assegurança CARMEN

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

Versió	6.1
Fabricant	Gigamon
Família	Captura, Monitoratge i Anàlisi de Trànsit
Tipus	Producte
Data Inclusió	28/06/2023
Revisió de Validesa	30/06/2024

Descripció

Network Packet Brokers HC Series. Network Packet Brokers d'alt rendiment amb suport de ports 1g/10g/25g/40g/100g en fibra multimode o/i monomode i 100m/1g/10g en coure i funcionalitats de filtratge de tràfic L2-3-4-7 amb motor de DPI, generació de Netflow/IPFix/Metadatos, Xifrat/Desxifrat de SSL/TLS (incloent-hi protocols RSA, DHE, ECC, i PFS), Terminació de túnels (GRE, VXLAN, ERSPAN, GMIP), Truncat de paquets, Eliminació de capçaleres, Emmascarat, De-Duplicació, Clustering, Balanceig, Captura de trànsit per a entorns virtuals (VMWare ESX/NSX, Openstack, Kubernetes, AWS, GCP, Azure, Nutanix), simetrització de trànsit per a arquitectura HA, Inline Bypass amb Heartbeat positiu i negatiu, Canvi de mitjà i velocitat, Bypass HW, TAPs integrats.

Observacions

CCN-STIC-1301 Procediment d'Ocupació Segur GigaVUE-OS

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

Versió	6.1
Fabricant	Gigamon
Família	Captura, Monitoratge i Anàlisi de Trànsit
Tipus	Producte
Data Inclusió	28/06/2023
Revisió de Validesa	30/06/2024

Descripció

Network Packet Brokers HC Series. Network Packet Brokers d'alt rendiment amb suport de ports 1g/10g/25g/40g/100g en fibra multimode o/i monomode i 100m/1g/10g en coure i funcionalitats de filtratge de tràfic L2-3-4-7 amb motor de DPI, generació de Netflow/IPFix/Metadatos, Xifrat/Desxifrat de SSL/TLS (incloent-hi protocols RSA, DHE, ECC, i PFS), Terminació de túnels (GRE, VXLAN, ERSPAN, GMIP), Truncat de paquets, Eliminació de capçaleres, Emmascarat, De-Duplicació, Clustering, Balanceig, Captura de trànsit per a entorns virtuals (VMWare ESX/NSX, Openstack, Kubernetes, AWS, GCP, Azure, Nutanix), simetrització de trànsit per a arquitectura HA, Inline Bypass amb Heartbeat positiu i negatiu, Canvi de mitjà i velocitat, Bypass HW, TAPs integrats.

Observacions

CCN-STIC-1301 Procediment d'Ocupació Segur GigaVUE-OS

8.5.PROTECCIÓ DE LES COMUNICACIONS

8.5.1 ENRUTADORES

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

Versió	OS10.5.4
Fabricant	DELL COMPUTER, S.A.
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2024
Revisió de Validesa	31/03/2026

Descripció

Dell EMC Smart Fabric OS10 és el sistema operatiu de xarxa (ENS) que s'utilitza en les famílies d'encaminadors i commutadors de les seriï N (alguns models), seriï S, seriï Z i sèrie MX de Dell EMC Networking (les plataformes HW que actualment suporten OS10 són N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON,S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n i MX9116n). Dell EMC SmartFabric OS10 és un sistema operatiu de xarxa (ENS) que admet múltiples arquitectures i entorns. La solució SmartFabric OS10 permet la desagregació en diverses capes de la funcionalitat de xarxa. SmartFabric OS10 comprèn l'administració, monitoratge i funcionalitat completa i estàndard de la indústria de xarxes de nivell 2 i nivell 3 a través d'interfícies CLI, SNMP i REST. Els usuaris poden triar les seves pròpies aplicacions d'organització, gestió, supervisió i xarxes de tercers. Per a desenvolupar xarxes escalables L2 i L3, SmartFabric OS10 ofereix una solució modular i desagregada en una única imatge binària.

Observacions

CCN-STIC-1429 PES DELL EMC Networking

Cisco ASR9000 Series i NCS4200 Series (ASR902, ASR903, ASR907, ASR920 i NCS4201, NCS4202, NCS4206, NCS4216)	
Versió	IOS-XE 16.9
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/09/2023
Revisió de Validesa	30/04/2025
Descripció	

Les famílies ASR900 i NCS4200 són equips fets a propòsit com plataformes de routing, suportant addicionalment xifrat MACsec.

Observacions

CCN-STIC 1454 Procediment d'Ocupació Assegurança Routers CISCO ASR9000 i NCS4200 Series

Cisco Nexus 9200 Series Switches (92348GC-X, 92160YC-X, 92300YC, 9272Q)	
Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	10/04/2025
Descripció	

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	ArubaOS 16.08
Fabricant	Aruba
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	31/05/2024

Descripció

Equips dissenyats per utilitzar-se en tasques d'accés i agregació, o nucli de xarxa d'accés. Són equips que proporcionen connexions de totes les velocitats i tipus de mitjans. Equips amb capacitat de commutació sense bloqueig (non-blocking). Segons la família, ofereixen solucions escalables mitjançant constitució de stacks via port de xarxa, port dedicat, així com exiten models de xassís. Totes les funcions del sistema operatiu s'ofereixen amb l'equip. Ofereixen diversos tipus d'interfícies i velocitats. Ofereixen PoE en alguns models, a diferents potències.

Poden ser gestionables, tant localment (gestió on-premise) com poden arribar a administrar-se en modalitat Software-as-a-Service

Observacions

CCN-STIC-647C Seguretat en commutadors HPE Aruba

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	04/10/2025

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

Cisco Nexus 9500 Series Switches (9504, 9508, 9516, Supervisor 9500-Sup-A , Supervisor 9500-Sup-A +, Supervisor 9500-Sup-B , Supervisor 9500-Sup-B +, System Controller N9k-SC-A)	
Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Enrutadors
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	04/10/2025
Descripció	

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

Dell EMC Networking SmartFabric (Models: S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, MX5108n, S4248FB-ON, S4248FBL-ON, S6010-ON, Z9100-ON, MX9116n, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9264F-ON i Z9332F-ON)

Versió	OS 10 Build: 10.5.1.3.
Fabricant	Dell Computer
Família	Enrutadors
Tipus	Producte
Data Inclusió	04/01/2022
Revisió de Validesa	31/08/2024

Descripció

Dell EMC Smart Fabric OS10 és el sistema operatiu de xarxa (NOS) que s'utilitza en les famílies d'enrutadors i commutadors de la Serie N (alguns models), Serie S, Serie Z i Serie MX de Dell EMC Networking (les plataformes HW que actualment suporten OS10 són N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n i MX9116n). Dell EMC SmartFabric OS10 és un sistema operatiu de xarxa (NOS) que admet múltiples arquitectures i entorns. La solució SmartFabric OS10 permet la desagregació en diverses capes de la funcionalitat de xarxa. SmartFabric OS10 comprèn l'administració, monitoratge i funcionalitat completa i estàndard de la indústria de xarxes de nivell 2 i nivell 3 a través d'interfícies CLI, SNMP i REST. Els usuaris poden triar les seves pròpies aplicacions d'organització, gestió, supervisió i xarxes de tercers. Per desenvolupar xarxes escalables L2 i L3, SmartFabric OS10 ofereix una solució modular i desagregada en una única imatge binària.

Observacions

CCN-STIC-1429 PES DELL EMC Networking

8.5.2 SWITCHES

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	10/04/2025
Descripció	

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	ArubaOS 16.08
Fabricant	Aruba
Família	Switches
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	31/05/2024
Descripció	

Equips dissenyats per utilitzar-se en tasques d'accés i agregació, o nucli de xarxa d'accés. Són equips que proporcionen connexions de totes les velocitats i tipus de mitjans. Equips amb capacitat de commutació sense bloqueig (non-blocking). Segons la família, ofereixen solucions escalables mitjançant constitució de stacks via port de xarxa, port dedicat, així com existen models de xassís. Totes les funcions del sistema operatiu s'ofereixen amb l'equip. Ofereixen diversos tipus d'interfícies i velocitats. Ofereixen PoE en alguns models, a diferents potències.

Poden ser gestionables, tan localment (gestió on-premise) com poden arribar a administrar-se en modalitat Software-as-a-Service

Observacions

CCN-STIC-647C Seguretat en commutadors HPE Aruba

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

Versió	EXOS 31.3.100
Fabricant	Extreme Networks
Família	Switches
Tipus	Producte
Data Inclusió	01/09/2023
Revisió de Validesa	31/05/2025

Descripció

Família de commutadors apilables d'alt rendiment, que proporcionen connectivitat gigabit, multigigabit, 10G, 25G, 40G i 100G. Els equips poden posicionar-se tant en l'accés com en l'agregació en el nucli, suportant protocols de routing avançat (BGP, MPLS, VXLAN, etc). També proporciona solucions d'implementació de Fabric

Observacions

CCN-STIC-1446 PES Switches EXoS

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

Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/05/2022
Revisió de Validesa	28/02/2026

Descripció

OS6360: Família de commutadors L2+ apilables amb ports 1G i enllaços 1G/10G. Dissenyats com a equips d'accés en xarxes convergents d'alta capacitat.

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	31/07/2024

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	04/10/2025

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

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

Versió	NX-OS 9.3
Fabricant	Cisco Systems
Família	Switches
Tipus	Producte
Data Inclusió	01/11/2023
Revisió de Validesa	04/10/2025

Descripció

Aquests switches proporcionen a les organitzacions arquitectures flexibles, avançada programabilitat, visibilitat i telemetria en temps real, alta escalabilitat i excepcional disponibilitat.

Observacions

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

Dell EMC Networking SmartFabric (Models: S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, MX5108n, S4248FB-ON, S4248FBL-ON, S6010-ON, Z9100-ON, MX9116n, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9264F-ON i Z9332F-ON)

Versió	OS 10 Build: 10.5.1.3.
Fabricant	Dell Computer
Família	Switches
Tipus	Producte
Data Inclusió	04/01/2022
Revisió de Validesa	31/08/2024

Descripció

Dell EMC Smart Fabric OS10 és el sistema operatiu de xarxa (NOS) que s'utilitza en les famílies d'enrutadors i commutadors de les series N (alguns models), Serie S, Serie Z i Serie MX de Dell EMC Networking (les plataformes HW que actualment suporten OS10 són N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n i MX9116n). Dell EMC SmartFabric OS10 és un sistema operatiu de xarxa (NOS) que admet múltiples arquitectures i entorns. La solució SmartFabric OS10 permet la desagregació en diverses capes de la funcionalitat de xarxa. SmartFabric OS10 comprèn l'administració, monitoratge i funcionalitat completa i estàndard de la indústria de xarxes de nivell 2 i nivell 3 a través d'interfícies CLI, SNMP i REST. Els usuaris poden triar les seves pròpies aplicacions d'organització, gestió, supervisió i xarxes de tercers. Per desenvolupar xarxes escalables L2 i L3, SmartFabric OS10 ofereix una solució modular i desagregada en una única imatge binària.

Observacions

CCN-STIC-1429 PES DELL EMC Networking

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

Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	28/02/2026

Descripció

OS6900: Família de commutadors L3 + compactes apilables d'alta densitat 10GE, 25GE, 40GE i 100GE. Dissenyades perquè siguin flexibles. Poden instal·lar-se com a commutadors convergents situats a la part superior del bastidor (TOR) o tipus spine per a entorns de Data Centers i també com a dispositius de agregació i de nucli en una xarxa de campus.

https://www.al-enterprise.com/es-es/productes/commutadors

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6560 (OS6560-P24Z8, OS6560-P24Z24, OS6560-P48Z16, OS6560-24Z8, OS6560-24Z24, OS6560-24X4, OS6560-P24X4, OS6560-48X4, OS6560-P48X4 i OS656 X10)

Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	28/02/2026

Descripció

Família de commutadors L3 compactes apilables amb alta densitat de ports 1GE, Multigigabit ethernet 1/2.5 GigE i enllaços 10GE, dissenyats com a equips d'accés en xarxes convergents d'alta capacitat. https://www.al-enterprise.com/es-es/productos/conmutadores

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

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

Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	28/02/2026

Descripció

Família de commutadors L3 compactes apilables amb alta densitat de ports 1GE, Multigigabit ethernet 1/2.5 GigE i enllaços 10GE, dissenyats com a equips d'accés en xarxes convergents d'alta capacitat. https://www.al-enterprise.com/es-es/productos/conmutadores

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

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

Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	28/02/2026

Descripció

OS6865: Família de commutadors L3 + amb ports 1G i 10G, preparats per a entorn industrial o xarxes de missió crítica com transports i utilities, amb ampli rang de temperatures de funcionament (-40ºC a +75ºC). https://www.al-enterprise.com/es-es/productos/conmutadores

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6860 (OS6860E-24, OS6860E-P24, OS6860E-48, OS6860E-P48, OS6860E-U28, OS6860E-P24Z8, TA6860E-P48, OS6860N-U28, OS6860N-P48Z, OS6860N-P48M, O6860N-P24M, OS6860N-P24Z)

Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	28/02/2026

Descripció

OS6860: Família de commutadors L3+ compactes apilables amb alta densitat de ports 1GE, Multigigabit ethernet 1/2.5/5/10 GigE i enllaços 10GE, 25GE i 100GE, dissenyades per a xarxes convergents. Amb funcions d'Accés unificat avançades que permeten la creació de xarxes orientades a les aplicacions. Pot supervisar i controlar les aplicacions de la xarxa mitjançant capacitats de Deep Packet Inspection (DPI). https://www.al-enterprise.com/es-es/productos/conmutadores

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

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

Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	28/02/2026

Descripció

OS9900: Commutador LAN L3 + amb xassís modular d'alta capacitat d'interfícies 1GE, 10GE i 100GE per commutació segura i amb alta disponibilitat al nucli de les xarxes, campus i xarxes Metro Ethernet. https://www.al-enterprise.com/es-es/productos/conmutadores

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

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

Versió	AOS 8.9.R01
Fabricant	Alcatel-Lucent Enterprise
Família	Switches
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	28/02/2026

Descripció

OS6465: Família de commutadors L2+ amb ports 1G i 10G, preparats per a entorn industrial, amb ampli rang de temperatures de funcionament (-40ºC a + 75ºC). Dissenyats amb equips d'accés en xarxes de tipus industrial, transports o utilities. https://www.al-enterprise.com/es-es/productes/commutadors

Observacions

CCN-STIC-1410 Procediment d'Ocupació Segur OMNISWITCH AOS

8.5.3 TALLAFOCS

Stormshield Network Security UTM/NG-Firewall (Appliances des de SN200 a SN6100 en 4 compilacions diferents: S, M, L i XL).	
Versió	3.11.LTSB
Fabricant	Stormshield SAS
Família	Tallafocs
Tipus	Producte
Data Inclusió	01/12/2022
Revisió de Validesa	30/06/2024
Descripció	

Firewalls de nova generació de capa 7, IPS i concentrador de túnels VPN. Amb capacitats de bloqueig d'amenaces avançades, atacs de dia zero, filtratge de navegació web o gestió de vulnerabilitats. El mateix equipament realitza inspecció profunda de protocols OT, a més d'IT.

Observacions

CCN-STIC-1415 Procediment d'Ocupació Segur Tallafocs UTMNG Stormshield

8.5.4 PASSAREL·LES SEGURES D'INTERCANVI DE DADES

Passarel·les d'intercanvi segur d'informació per a sistemes específics militars

Versió

Fabricant Autek Ingenería

Família Passarel·les segures d'intercanvi de dades

Tipus Producte

Data Inclusió 01/12/2022

Revisió de Validesa 01/05/2025

Descripció

Passarel·les desenvolupades ad-hoc per a sistemes / protocols específics. ISR, Asterix, Datalink, ADEXP, et Consultar disponibilitat i estat d'aprovació en itsec.ccn@cni.es o cpstic.ccn@cni.es.

Observacions

N/A

PSTfile

Versió v4.4.2

Fabricant Autek Ingenería

Família Passarel·les segures d'intercanvi de dades

Tipus Producte

Data Inclusió 01/12/2017

Revisió de Validesa 31/05/2025

Descripció

PSTfile és un dispositiu de protecció de perímetre de la família PSTgateways. Permet l'intercanvi controlat de fitxers entre dominis de seguretat. S'estableix una correspondència entre carpetes, en servidors de fitxers d'ambdues xarxes i PSTfile, automàticament, mou o copia els fitxers de l'origen a la destinació. Suporta els protocols FTP, FTPS, SFTP i SMB. La transferència de fitxers des del domini d'alta seguretat al de baixa requereix autorització mitjançant signatura digital.

Observacions

Procediment d'ocupació segura: CCN-STIC-1401 Configuració segura de passarel·les d'AUTEK

PSTmail

Versió	v3.0.5
Fabricant	Autek Ingenería
Família	Passarel·les segures d'intercanvi de dades
Tipus	Producte
Data Inclusió	01/12/2017
Revisió de Validesa	31/05/2025

Descripció

PSTmail és un dispositiu de protecció de perímetre de la família PSTgateways. Permet l'intercanvi controlat de correu electrònic entre dominis de seguretat. Possibilita l'ús d'adreces de correu de xarxes externes, des d'una xarxa interna, més segura. Suporta les versions segures dels protocols de correu. Els missatges de sortida requereixen autorització mitjançant signatura digital (S/MIME).

Observacions

Procediment d'ocupació segura: CCN-STIC-1401 Configuració segura de passarel·les d'AUTEK

8.5.5 DÍODES DE DADES

PSTdiode

Versió	v1.3.1-A
Fabricant	Autek Ingenería
Família	Díodes de dades
Tipus	Producte
Data Inclusió	01/09/2019
Revisió de Validesa	31/08/2024

Descripció

El díode de dades maquinari PSTdiode és un dispositiu de protecció de perímetre que permet la transferència d'informació en un únic sentit entre dos dominis de seguretat amb garantia física de transmissió unidireccional. La seva aplicació principal és la introducció d'informació en una xarxa aïllada en entorns classificats. També es pot aplicar per extreure informació d'una xarxa de control industrial en entorns d'infraestructures crítiques. En ambdós casos es garanteix que no hi ha trànsit en el sentit invers. Existeixen models de transferència de fitxers i trànsit UDP.

Observacions

Procedimeint d'ocupació assegurança:CCN-STIC 1408 Procediment d'ocupació assegurança Díode Autek Enginyeria

8.5.6 EINES PER A COMUNICACIONS MÒBILS SEGURES

Versió	v4.2
Fabricant	Indra
Família	Eines per a comunicacions mòbils segures
Tipus	Producte
Data Inclusió	01/05/2021
Revisió de Validesa	30/06/2024

Descripció

COMSec Admin+ és una solució global de comunicacions segures que proporciona serveis xifrats de veu, missatgeria instantània i videoconferència sobre telèfons mòbils emprant qualsevol xarxa cel·lular, sense fil o satelital. Amb el seu alt nivell de seguretat, gran qualitat d'àudio i facilitat d'ús protegeix de forma eficaç informació classificada (fins a difusió limitada) de l'organització. Les trucades i les dades intercanviades per COMSec són segudes, independentment de l'operador mòbil utilitzat i el país on es trobi. Més informació: comsec.indracompany.com

Observacions

Utilització segons el PE-2018-24 Procediment d'ocupació COMSec Admin + v2 Per a la seva ocupació en entorns tàctics o desplegables, aquest producte s'haurà d'emprar sobre un dispositiu mòbil pertanyent a la família "plataformes i dispositius tàctics confiables"

8.5.7 EINES DE MISSATGERIA INSTANTÀNIA (IM)

COMSec Admin +

Versió v5.0

Fabricant Indra

Família Eines de missatgeria instantània (IM)

Tipus Producte

Data Inclusió 01/05/2021

Revisió de Validesa 30/06/2024

Descripció

COMSec Admin+ és una solució global de comunicacions segures que proporciona serveis xifrats de veu, missatgeria instantània i videoconferència sobre telèfons mòbils emprant qualsevol xarxa cel·lular, sense fil o satelital. Amb el seu alt nivell de seguretat, gran qualitat d'àudio i facilitat d'ús protegeix de forma eficaç informació classificada (fins a difusió limitada) de l'organització. Les trucades i les dades intercanviades per COMSec són segudes, independentment de l'operador mòbil utilitzat i el país on es trobi. Més informació: comsec.indracompany.com

Observacions

Utilització segons el PE-2018-24 Procediment d'ocupació COMSec Admin + v2 Per a la seva ocupació en entorns tàctics o desplegables, aquest producte s'haurà d'emprar sobre un dispositiu mòbil pertanyent a la família "plataformes i dispositius tàctics confiables"

8.5.8 EINES VEU IP

COMSec Admin +

Versió	v5.0
Fabricant	Indra
Família	Eines Veu IP
Tipus	Producte
Data Inclusió	01/05/2021
Revisió de Validesa	30/06/2024

Descripció

COMSec Admin+ és una solució global de comunicacions segures que proporciona serveis xifrats de veu, missatgeria instantània i videoconferència sobre telèfons mòbils emprant qualsevol xarxa cel·lular, sense fil o satelital. Amb el seu alt nivell de seguretat, gran qualitat d'àudio i facilitat d'ús protegeix de forma eficaç informació classificada (fins a difusió limitada) de l'organització. Les trucades i les dades intercanviades per COMSec són segudes, independentment de l'operador mòbil utilitzat i el país on es trobi. Més informació: comsec.indracompany.com

Observacions

Utilització segons el PE-2018-24 Procediment d'ocupació COMSec Admin + v2 Per a la seva ocupació en entorns tàctics o desplegables, aquest producte s'haurà d'emprar sobre un dispositiu mòbil pertanyent a la família "plataformes i dispositius tàctics confiables"

8.5.9 XIFRADORS IP

EP430GU/B

Versió 2.01

Fabricant Epicom

Família Xifradors IP

Tipus Producte

Data Inclusió 01/09/2020

Revisió de Validesa 30/06/2024

Descripció

El xifrador IP EP430 GU/B està basat en el xifrador IP EP430GU, sobre el qual s'han substituït els mecanismes criptogràfics per algoritmes tipus B. Està compost per una plataforma de comunicacions EP430G+ i un mòdul cripto EP940+ programat com a EP940U/B (software i firmware). És un xifrador a 1Gpbs, dissenyat per operar a la capa 3 del model OSI, cosa que permet el desplegament de xarxes privades virtuals (VPN, Virtual Private Networks) d'una forma completament segura.

Observacions

Utilització segons PE-2019-9 Procediment d'Ocupació EP430GU/B

EP430TX

Versió 1.04

Fabricant Epicom

Família Xifradors IP

Tipus Producte

Data Inclusió 01/12/2017

Revisió de Validesa 31/12/2024

Descripció

Xifrador de comunicacions IP fins a 200 Mbps, interoperable amb la resta de xifradors de la família EP430.

Observacions

Utilització segons PE-2016-28 Procediment d'ocupació EP430TX.

EP430GX

Versió v.1.08

Fabricant Epicom

Família Xifradors IP

Tipus Producte

Data Inclusió 27/12/2021

Revisió de Validesa 31/12/2024

Descripció

Xifrador de xarxes IP a 2 Gbps (agregats), interoperable amb la resta de xifradors de la família EP430.

Observacions

Utilització segons PE-2012-49 Procediment d'Ocupació EP430GX.

EP430GN

Versió v2.04

Fabricant Epicom

Família Xifradors IP

Tipus Producte

Data Inclusió 01/12/2022

Revisió de Validesa 31/12/2024

Descripció

Xifrador de xarxes IP a 2 Gbps (agregats).

Observacions

Aquest model no és compatible amb la resta de la família de xifradors EP430 d'EPICOM. Utilització segons P029-PE-2011-33 Operational doctrine EP430GN v2.

EP430GN

Versió 1.08.29

Fabricant Epicom

Família Xifradors IP

Tipus Producte

Data Inclusió 01/12/2017

Revisió de Validesa 31/12/2024

Descripció

Xifrador de xarxes IP a 2 Gbps (agregats).

Observacions

Aquest model no és compatible amb la resta de la família de xifradors EP430 d'EPICOM. Utilització segons P029-PE-2011-33 Operational doctrine EP430GN v2.

Centre de gestió 543U/B

Versió 2.01

Fabricant Epicom

Família Xifradors IP

Tipus Producte

Data Inclusió 01/09/2020

Revisió de Validesa 30/06/2024

Descripció

El Centre de Gestió EP543U/B és l'element de gestió remota del xifrador EP430 GU/B. L'únic procediment permès per gestionar de manera remota un EP430GU/B és a través d'una connexió remota segura (Canal Segur) des de l'aplicació del Centre de Gestió.

Observacions

Utilització segons PE-2019-9 Procediment d'Ocupació EP430GU/B

8.6 PROTECCIÓ DE LA INFORMACIÓ I ELS SUPORTS DE LA INFORMACIÓ

8.6.1 XIFRAT I COMPARTICIÓ SEGURA D'INFORMACIÓ

EP852

Versió	3.05
Fabricant	Epicom
Família	Xifrat i compartició segura d'informació
Tipus	Producte
Data Inclusió	27/12/2021
Revisió de Validesa	31/12/2025

Descripció

L'EP852 és un xifrador de fitxers fora de línia que permet el xifrat i desxifrat de fitxers i el transport d'informació xifrada en el dispositiu. Millora les prestacions quant a emmagatzematge i velocitat de les versions anteriors dels Token USB així com la posada en marxa del dispositiu, càrrega i distribució de claus.

Observacions

Utilització segons el PE-2020-4 -Procediment d'Ocupació Segur EP852 -(ESP)

EP880

Versió	V2.08.36 i V2.09.35
Fabricant	Epicom
Família	Xifrat i compartició segura d'informació
Tipus	Producte
Data Inclusió	01/07/2021
Revisió de Validesa	31/12/2026

Descripció

L'EP880 és una aplicació Software que s'executa sobre ordinador amb sistema operatiu Windows i que permet realitzar, en origen, el xifrat i signatura de fitxers de dades "off-line" emmagatzemats en el disc dur de l'ordinador o dispositius d'emmagatzematge externs connectats a l'ordinador, per al seu posterior emmagatzematge i/o enviament de forma segura des del correu electrònic o un altre mitjà i, en destinació, el desxifrat i verificació de la integritat de les dades.

Observacions

CCN-STIC-1506 Procediment d'Ocupació Assegurança EP880

EP852

Versió	3.04
Fabricant	Epicom
Família	Xifrat i compartició segura d'informació
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	31/12/2025

Descripció

L'EP852 és un xifrador de fitxers fora de línia que permet el xifratge i desxifrat de fitxers i el transport d'informació xifrada en el dispositiu. Millora les prestacions quant a emmagatzematge i velocitat de les versions anteriors dels Token USB així com la posada en marxa del dispositiu, càrrega i distribució de claus.

Observacions

Utilització segons el PE-2020-4 -Procediment d'Ocupació Segur EP852 -(ESP)

8.6.2 EINES D'ESBORRAT ASSEGURANÇA

OBLIT Windows	
Versió	1.0.6
Fabricant	authUSB
Família	Eines d'esborrat segur
Tipus	Producte
Data Inclusió	01/09/2022
Revisió de Validesa	28/02/2025

Descripció

OBLIT és una eina d'esborrat segur que acompleix tasques de sobreescriptura i esborrat sobre els sistemes d'arxius i discos reconeguts. Ofereix a l'usuari la possibilitat d'esborrar de forma segura diferents elements guardats en els dispositius d'emmagatzematge:

- Fitxers i carpetes
- Espai Lliure
- Fragments de clúster no utilitzats
- Discos i volums

Disposa d'un mòdul de planificació amb el qual es permet a l'usuari programar l'execució de les tasques d'esborrat. OBLIT implementa diferents algoritmes estàndard d'esborrat i permet a l'usuari seleccionar l'algoritme d'esborrat a aplicar en cada tasca. Així mateix, ofereix la possibilitat a l'administrador de definir algorismes d'esborrat personalitzats, especificant el nombre de passis i el patró de sobreescriptura. Permet la integració amb un servidor Syslog per a l'enviament de registres d'activitat i estat de les tasques d'esborrat realitzades.

La versió aprovada permet, amb l'algoritme d'esborrat CCN-Classificat, la reclassificació i desclassificació de:

- Discos magnètics fins a RESERVAT o equivalent.
- Discos SSD fins a DIFUSIÓ LIMITADA o equivalent.

S'executa sobre Windows 10, Windows Server 2016 i Windows Server 2021.

Observacions

CCN-STIC-1508 Procedimiento de empleo seguro OLVIDO

8.6.3 GESTIÓ DE METADADES

metaOLVIDO Dashboard (modalidad on-premise)

Versió	1.3.0
Fabricant	Adarsus Technologies S.L
Família	Gestió de metadades
Tipus	Producte
Data Inclusió	01/05/2024
Revisió de Validesa	30/04/2026
Descripció	

metaOLVIDO Dashboard: Consola d'administració de metaOLVIDO per a les diferents modalitats de desplegament. Administra, centralitza i controla l'aplicació de polítiques preventives de seguretat corporatives. Permet obtenir estadístiques de les metadades processades i controlar la exfiltració d'informació de manera global.

Observacions

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard

MetaClean Dashboard

Versió	1.3.0
Fabricant	Adarsus Technologies S.L
Família	Gestió de metadades
Tipus	Producte
Data Inclusió	01/05/2024
Revisió de Validesa	30/04/2026
Descripció	

metaOLVIDO Dashboard: Consola d'administració de metaOLVIDO per a les diferents modalitats de desplegament. Administra, centralitza i controla l'aplicació de polítiques preventives de seguretat corporatives. Permet obtenir estadístiques de les metadades processades i controlar la exfiltració d'informació de manera global.

Observacions

CCN-STIC 1510 Procedimiento de Empleo Seguro metaOLVIDO Dashboard

MetaClean Dashboard

Versió	2.3.0
Fabricant	Adarsus Technologies S.L
Família	Gestió de metadades
Tipus	Producte
Data Inclusió	01/05/2024
Revisió de Validesa	30/04/2026
Descripció	

MetaClean Sync Workstation i MetaClean Sync Server: Eina de gestió de metadades que permet aplicar polítiques de seguretat corporatives de prevenció de fugides d'informació, netejant les metadades i informació sensible oculta en els fitxers ofimàtics generats en una organització. Realitza una protecció contínua i en temps real de les metadades d'una estació de treball o Servidor. Protegeix la informació de manera senzilla i desatesa. Permet configurar regles i posar-les en pràctica sobre els arxius documentals o multimèdia que es consideri necessari, ja sigui en els equips d'usuari -Workstation- o en carpetes de xarxa compartides -Server-.

Observacions

CCN-STIC 1511 Procedimiento de Empleo Seguro metaOLVIDO EndPoint y metaOLVIDO Server

metaOLVIDO Endpoint y metaOLVIDO Server

Versió	2.3.0
Fabricant	Adarsus Technologies S.L
Família	Gestió de metadades
Tipus	Producte
Data Inclusió	01/05/2024
Revisió de Validesa	30/04/2026
Descripció	

MetaClean Sync Workstation i MetaClean Sync Server: Eina de gestió de metadades que permet aplicar polítiques de seguretat corporatives de prevenció de fugides d'informació, netejant les metadades i informació sensible oculta en els fitxers ofimàtics generats en una organització. Realitza una protecció contínua i en temps real de les metadades d'una estació de treball o Servidor. Protegeix la informació de manera senzilla i desatesa. Permet configurar regles i posar-les en pràctica sobre els arxius documentals o multimèdia que es consideri necessari, ja sigui en els equips d'usuari -Workstation- o en carpetes de xarxa compartides -Server-.

Observacions

CCN-STIC 1511 Procedimiento de Empleo Seguro metaOLVIDO EndPoint y metaOLVIDO Server

8.7.PROTECCIÓ D'EQUIPS I SERVEIS

8.7.1 DISPOSITIUS MÒBILS

Färist Mobile en Bittium Tough Mobile 2 (FM T200)	
Versió	7.4
Fabricant	Tutus
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	26/01/2024
Revisió de Validesa	26/04/2026
Descripció	

Sistema de comunicació segur de terminals mòbils basat en S.O. Android. El Färist Mobile System a més de protegir la comunicació protegeix la plataforma (Bittium Tough Mobile 2) per emmagatzemar informació classificada fins al grau de Difusió Limitada.

Observacions

Utilització segons PE-2022-2 Comercialitzat a Espanya per l'empresa Epicom.

Färist Mobile en Bittium Tough Mobile 2 (FM T200)	
Versió	7.4
Fabricant	Tutus
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	26/01/2024
Revisió de Validesa	26/04/2026
Descripció	

Sistema de comunicació segur de terminals mòbils basat en S.O. Android. El Färist Mobile System a més de protegir la comunicació protegeix la plataforma (Bittium Tough Mobile 2) per emmagatzemar informació classificada fins al grau de Difusió Limitada.

Observacions

Utilització segons PE-2022-2 Comercialitzat a Espanya per l'empresa Epicom.

Färist Mobile a Google Pixel 4A 5G (FM T120)

Versió	7.4
Fabricant	Tutus
Família	Dispositius mòbils
Tipus	Producte
Data Inclusió	26/01/2024
Revisió de Validesa	14/07/2025

Descripció

Sistema de comunicació segur de terminals mòbils basat en S.O. Android. El Färist Mobile System a més de protegir la comunicació protegeix la plataforma (Google Pixel 4A 5G) per emmagatzemar informació classificada fins al grau de Difusió Limitada.

Observacions

Utilització segons PE-2022-2 Comercialitzat a Espanya per l'empresa Epicom.

8.7.2 SISTEMES OPERATIUS

Windows Server 2016

Versió	Datacenter Edition
Fabricant	Microsoft Corporation
Família	Sistemes Operatius
Tipus	Producte
Data Inclusió	01/12/2018
Revisió de Validesa	12/01/2027

Descripció

Sistema Operatiu per a servidors.

Observacions

CCN-STIC-570A, CCN-STIC-570B Annex A

SUSE Linux Enterprise

Versió	Server 15 SP2
Fabricant	SUSE Software Solutions
Família	Sistemes Operatius
Tipus	Producte
Data Inclusió	01/10/2022
Revisió de Validesa	31/12/2024

Descripció

SUSE® Linux Enterprise Server (SLES) 15 SP2 és un sistema operatiu (SO) modular que ajuda a simplificar l'entorn IT, modernitzar la infraestructura IT i accelerar la innovació. SLES s'adapta a qualsevol entorn operatiu alhora que satisfà els requisits de rendiment, seguretat i confiança. És una plataforma fàcil d'administrar per a desenvolupadors i administradors que permet implementar càrregues de treball crítiques per al negoci a les instal·lacions, al núvol i al perímetre.

Observacions

CCN-STIC-1615 Procediment d'ocupació assegurança SUSE 15 SP2

8.7.3 PROTECCIÓ DE CORREU ELECTRÒNIC

Cisco Email Security Appliance (C190, C195, C390, C395, C690, C690X, C695, C695F, C100v, C300v i C600v)	
Versió	AsyncOS 13.0
Fabricant	Cisco Systems
Família	Protecció de correu electrònic
Tipus	Producte
Data Inclusió	01/09/2023
Revisió de Validesa	31/05/2025
Descripció	

Cisco Email Security Appliance és una passarel·la de seguretat per al correu electrònic. Està dissenyat per detectar i bloquejar una àmplia varietat d'amenaces transmeses per correu electrònic, com malware, spam i intents de phishing.

Observacions

CCN-STIC 1623 Procediment d'Ocupació Segur Cisco Email Security Appliance

8.7.4 HIPERCONVERGÈNCIA

KATUA SDI PLATFORM

Versió	1.0
Fabricant	KRC ESPAÑOLA S.A.
Família	Hiperconvergència
Tipus	Producte
Data Inclusió	01/12/2021
Revisió de Validesa	31/01/2025

Descripció

Katua®SDI Platform és una plataforma hiperconvergent escalable i segura, basada en el concepte Software Define Infraestructure, on tots els elements que conformen un CPD es defineixen en una única plataforma maquinari i Software. Permet el desplegament ràpid de serveis (xaaS), consolidació de CPDs, SDN i té capacitat d'instal·lació des d'equips mòbils fins a grans centres de processos de dades. La seva flexibilitat permet que es puguin desplegar serveis cloud sobre la plataforma de forma senzilla i eficient. Disposa de la capacitat per generar biblioteques de sistemes preconfigurats per al seu desplegament amb un click a través de la seva interfície web. Les capacitats d'optimització de l'hipervisor asseguren un rendiment màxim de la plataforma, fent ús de tots els recursos disponibles i oferint d'aquesta forma capacitat d'instal·lació en nodes petits i configuracions maquinari bàsiques. La seva capacitat per integrar-se amb sistemes d'emmagatzematge massius, siguin locals o remots permet escapolir la solució en funció de les necessitats. Per a més informació de la plataforma, vista la nostra web https://www.krc.es

Observacions

CCN-STIC-1610 Procediment d'Ocupació Segur KATUA SDI Platform

8.8.ALTRES EINES

8.8.1 ALTRES EINES

authUsb safeDoor	
Versió	2.0.0.11
Fabricant	authUSB
Família	Altres Eines
Tipus	Producte
Data Inclusió	01/05/2019
Revisió de Validesa	30/06/2024
Descripció	

AuthUsb safeDoor és un dispositiu maquinari que actua com a barrera entre les memòries USB i els equips d'una organització, identificant amenaces a tres nivells:

- Elèctric: identificant i detenint atacs destructius de sobretensió tipus UsbKiller.
- Hardware: detectant i desactivant atacs de la família BadUsb, atacs HID (rubber ducky i similars), falses targetes de xarxa, interfícies compostes, etc.
- Software: antivirus integrat que realitza una anàlisi prèvia a la descàrrega de qualsevol contingut.

Observacions

CCN-STIC 1201 Procediment d'Ocupació Assegurança AuthUsb SafeDoor

8.9 COMUNICACIONS TÀCTIQUES SEGURES

8.9.1 PLATAFORMES I DISPOSITIUS TÀCTICS CONFIABLES

GETAC F110

Versió G6 amb firmware 15.0.35.1951

Fabricant GETAC

Família Plataformes i dispositius tàctics confiables

Tipus Producte

Data Inclusió 01/10/2023

Revisió de Validesa 14/10/2025

Descripció

Tauleta robusta dissenyada per donar suport a usuaris civils i militars. Aquest dispositiu es considera una plataforma confiable on executar aplicacions Software de forma protegida (p.ex.: aplicacions de comandament i control). El sistema operatiu de la tauleta és Windows 10 IoT Enterprise 21H2 LTSB. La tauleta inclou un TPM 2.0.

Observacions

CCN-STIC-1628 Procediment d'ocupació assegurança GETAC F110G6

GETAC F110

Versió G5 amb firmware GETAC 12.0.45.1509

Fabricant GETAC

Família Plataformes i dispositius tàctics confiables

Tipus Producte

Data Inclusió 01/06/2021

Revisió de Validesa 14/10/2025

Descripció

Tauleta robusta dissenyada per donar suport a usuaris civils i militars. Aquest dispositiu es considera una plataforma confiable on executar aplicacions Software de forma protegida (p.ex.: aplicacions de comandament i control). El sistema operatiu de la tauleta és Windows 10 Enterprise 1607 LTSB. La tauleta inclou un TPM 2.0.

Observacions

Configuració i ocupació segura segons la CCN-STIC-1609. Per a protecció de les comunicacions en trànsit és necessari un producte aprovat pertanyent a la família "solucions per a protecció de les comunicacions tàctiques".

GETAC F110

Versió G4 amb firmware GETAC R1.12.070520

Fabricant GETAC

Família Plataformes i dispositius tàctics confiables

Tipus Producte

Data Inclusió 01/06/2019

Revisió de Validesa 14/10/2025

Descripció

Tauleta robusta dissenyada per donar suport a usuaris civils i militars. Aquest dispositiu es considera una plataforma confiable on executar aplicacions Software de forma protegida (p.ex.: aplicacions de comandament i control). El sistema operatiu de la tauleta és Windows 10 Enterprise 1607 LTSB. La tauleta inclou un TPM 2.0.

Observacions

Configuració i ocupació segura segons la CCN-STIC-1605. Per a protecció de les comunicacions en trànsit és necessari un producte aprovat pertanyent a la família "solucions per a protecció de les comunicacions tàctiques".

HP Elitebook 840

Versió G7 i G8

Fabricant HP PRINTING AND COMPUTING SOLUTIONS SL

Família Plataformes i dispositius tàctics confiables

Tipus Producte

Data Inclusió 01/09/2021

Revisió de Validesa 14/10/2025

Descripció

Equips portàtils amb sistema operatiu Windows 10 Enterprise, Versió 20H2, Compilació (19042.1023) securitzable mitjançant l'aplicació de les guies STIC per a maneig d'informació classificada.

Observacions

Plataforma bastionada segons CCN-STIC 599B19

8.9.2 SOLUCIONS PER A PROTECCIÓ DE LES COMUNICACIONS TÀCTIQUES

Bittium SafeMove VPN Client for Android

Versió	Android (genèric): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb
Fabricant	Bittium
Família	Solucions per a protecció de les comunicacions tàctiques
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	30/06/2024

Descripció

SafeMove Mobile VPN forma part de la Bittium Secure Suite. Proporciona els serveis de firewall i VPN IPSec a les plataformes Android i Windows connectades de forma remota a la infraestructura corporativa, i està concebut per ser un servei sempre actiu i aplicat a tot el trànsit de xarxa que entra i surt del dispositiu. Res sensible s'escapa, res malmès pot entrar. La SafeMove Mobile VPN és una solució client-servidor. El client instal·lat en el dispositiu es connecta a la porta d'enllaç Bittium SafeMove VPN Gateway instal·lada en el servidor, amb la resta dels components de la Bittium Secure Suite, que són el gestor de dispositius (MDM), el gestor de les aplicacions instal·lades en els dispositius (només Android) i els serveis de comprovació de la integritat (només Android). Usat en combinació amb els smartphones de la família Bittium Tough Mobile proporciona serveis de recuperació dels registres d'auditoria i acíOTA del firmware dels dispositius. Més informació de Bittium SafeMove® Mobile VPN: https://www.bittium.com/secure-communications-connectivity/bittium-safemove-mobile-vpn

Observacions

PE-2021-7-Procediment d'ocupació assegurança Bittium SafeMove VPN (Android i Windows)

Bittium Tough SDR Handheld – Soldier Radio

Versió	9400132
Fabricant	Bittium
Família	Solucions per a protecció de les comunicacions tàctiques
Tipus	Producte
Data Inclusió	01/08/2021
Revisió de Validesa	30/06/2024

Descripció

El producte Bittium Tough SDR Handheld és una ràdio tàctica militar V-UHF de mà basada en tecnologia SDR conforme a l'arquitectura ESSOR SCA. Aquesta ràdio, en funció de la forma d'ona emprada, proporciona diferents serveis de comunicacions de veu i dades amb unes prestacions determinades en termes d'amplada de banda, abast, nombre de nodes suportats a la xarxa ràdio, etc. La Tough SDR Handheld cobreix la banda de freqüències des de 30 MHz fins a 2,5 GHz i pot executar formes d'ona tant de banda estreta com de banda ampla, les quals inclouen diferents mecanismes de protecció COMSEC, TRANSEC i NETSEC. L'aprovació per a la protecció d'informació classificada nacional de grau DIFUSIÓ LIMITADA és aplicable quan el producte s'empri amb la forma d'ona ESSOR High Data Rate Waveform.

Observacions

Utilització segons el PE-2021-21 "Procediment d'ocupació segura de la ràdio tàctica Bittium Tough SDR Hand-Held"

TZ-2001R-MC

Versió	SW 1.8 i 1.8.1
Fabricant	TECNOBIT
Família	Solucions per a protecció de les comunicacions tàctiques
Tipus	Producte
Data Inclusió	01/02/2023
Revisió de Validesa	30/06/2025

Descripció

El TZ-2001R-MC és una aplicació de xifrat Software per a sistemes Windows que s'executa com un servei del Sistema Operatiu a disposició d'altres aplicacions (típicament aplicacions de comandament i control). Proporciona les següents capacitats de xifrat:

a) Xifrat de veu tàctica ("push to talk") segons diversos estàndards (SCIP multipunt, STaC-IS 2400, TSVCIS 600, TSVCIS 1200, TSVCIS 600/2400 i TSVCIS 1200/2400).

b) Xifrat de dades IP en mode transport (només "payload"), estant disponible una manera autenticat (AES- GCM) i una manera no autenticat (AES-CTR).

c) Xifrat no autenticat (AES-CTR) de les dades DAP del Sistema BMS-ET que es transmeten pel TDMA de la ràdio F@stnet PR4G.

En els seus modes de xifra de veu tàctica i dades IP, el TZ-2001R-MC és interoperable amb altres productes de la família CIFPECOM, com ara el TZ-1001R o la Unitat de Comunicacions Segures amb mòdul de seguretat TZ-501. El TZ-2001R-MC es configura amb el mateix centre de gestió (CMAP) que el TZ-1001R i el TZ-501.

Observacions

Segons el seu procediment d'ocupació, el TZ-2001R-MC haurà d'executar-se sobre una plataforma Windows qualificada de confiable, o bé en una estació de treball bastionada conforme al requerit en la CCN-STIC-599 per manejar informació DIFUSIÓ LIMITADA. La major part de les funcions de seguretat lògica resideixen a la plataforma Windows que s'empri. Utilització segons el Procediment d'Ocupació Assegurança T00741700PDE001 Ed. 01.

TZ-1001R

Versió	V4.26
Fabricant	TECNOBIT
Família	Solucions per a protecció de les comunicacions tàctiques
Tipus	Producte
Data Inclusió	01/10/2020
Revisió de Validesa	31/12/2024

Descripció

El TZ-1001R és un xifrador tàctic de petita mida per a la protecció de les comunicacions sobre xarxes de baix ample de banda i sense estabilitat d'enllaç garantida. Compta amb dos modes d'operació diferenciats: com a xifrador en línia (mode "tactical crypto"), o alternativament en mode "slave crypto" com a element de xifra esclau d'un altre element que gestiona la interacció amb els mitjans de transmissió i amb l'usuari (cas del Gestor de Comunicacions de l'ET). El TZ-1001R té capacitat per xifrar de forma simultània diversos fluxos de veu tàctica ("push to talk") segons diversos estàndards OTAN, podent triar-se en cada cas el més adequant segons el tipus de ràdio pel qual es realitzarà la transmissió. Simultàniament també pot xifrar dades IP unicast i multicast. Quan el xifrador es configura en mode "tactical crypto" implementa IPSec amb associacions de seguretat manuals. En configuració "slave crypto" el TZ-1001R implementa un protocol específic de xifra IP per facilitar la integració amb els sistemes CIS de dotació. En mode "slave crypto" la xifra del TZ-1001R és interoperable amb la xifra del TZ-501 (mòdul de seguretat de la UCS) i amb l'aplicació de xifrat per a S.O. Windows TZ-2001.

Observacions

Utilització segons el Procediment d'ocupació T90431000PDE003 v2.0

Bittium SafeMove VPN Client for Windows

Versió	4.11.722
Fabricant	Bittium
Família	Solucions per a protecció de les comunicacions tàctiques
Tipus	Producte
Data Inclusió	01/04/2021
Revisió de Validesa	30/06/2024

Descripció

SafeMove Mobile VPN forma part de la Bittium Secure Suite. Proporciona els serveis de firewall i VPN IPSec a les plataformes Android i Windows connectades de forma remota a la infraestructura corporativa, i està concebut per ser un servei sempre actiu i aplicat a tot el trànsit de xarxa que entra i surt del dispositiu. Res sensible s'escapa, res malmès pot entrar. La SafeMove Mobile VPN és una solució client-servidor. El client instal·lat en el dispositiu es connecta a la porta d'enllaç Bittium SafeMove VPN Gateway instal·lada en el servidor, amb la resta dels components de la Bittium Secure Suite, que són el gestor de dispositius (MDM), el gestor de les aplicacions instal·lades en els dispositius (només Android) i els serveis de comprovació de la integritat (només Android). Usat en combinació amb els smartphones de la família Bittium Tough Mobile proporciona serveis de recuperació dels registres d'auditoria i acíOTA del firmware dels dispositius. Més informació de Bittium SafeMove® Mobile VPN: https://www.bittium.com/secure-communications-connectivity/bittium-safemove-mobile-vpn

Observacions

PE-2021-7-Procediment d'ocupació assegurança Bittium SafeMove VPN (Android i Windows)

COMSec Admin +

Versió v4.2

Fabricant Indra

Família Solucions per a protecció de les comunicacions tàctiques

Tipus Producte

Data Inclusió 01/05/2021

Revisió de Validesa 29/02/2024

Descripció

COMSec Admin+ és una solució global de comunicacions segures que proporciona serveis xifrats de veu, missatgeria instantània i videoconferència sobre telèfons mòbils emprant qualsevol xarxa cel·lular, sense fil o satelital. Amb el seu alt nivell de seguretat, gran qualitat d'àudio i facilitat d'ús protegeix de forma eficaç informació classificada (fins a difusió limitada) de l'organització. Les trucades i les dades intercanviades per COMSec són segudes, independentment de l'operador mòbil utilitzat i el país on es trobi. Més informació: comsec.indracompany.com

Observacions

Utilització segons el PE-2018-24 Procediment d'ocupació COMSec Admin + v2 Per a la seva ocupació en entorns tàctics o desplegables, aquest producte s'haurà d'emprar sobre un dispositiu mòbil pertanyent a la família "plataformes i dispositius tàctics confiables"

Unitat de Comunicacions Segures (UCS) amb mòdul de seguretat TZ-501

Versió UCS v2.4 amb TZ-501 (versió SW 4.26)

Fabricant TECNOBIT i RF Espanyola

Família Solucions per a protecció de les comunicacions tàctiques

Tipus Producte

Data Inclusió 01/09/2021

Revisió de Validesa 31/12/2024

Descripció

La UCS és un gestor de comunicacions per al seu ús en entorns tàctics militars en els quals es requereix comptar amb comunicacions segures tant de veu tàctica CNR com de de dades IP. La UCS permet la connexió de diverses ràdios tàctiques, o altres mitjans CIS, que actuen com a mitjà de transport. El sistema incorpora un mòdul de gestió de radiofonia, un mòdul per a la gestió de la interfonia i un servidor de telefonia de Veu IP per a la integració amb equips telefònics SIP, tot això acompanyat d'un mòdul de xifrat segur, denominat TZ-501. El TZ-501 és el mòdul encarregat de xifratge la veu tàctica segons estàndards OTAN, així com les dades IP unicast i multicast. La UCS compta amb una "Crypto Ignition Key" (CIK) per a l'arrencada segura de l'equip, i que a més facilita el transport i emmagatzematge de l'equip (sense la CIK la UCS es considera un equip no classificat). La xifra del TZ-501 és compatible amb la xifra del TZ-1001R en mode "slave-crypto" i amb la xifra del TZ-2001.

Observacions

Utilització segons el Procediment d'Ocupació Assegurança T00741600PDE001 V3

8.10 TEMPEST

8.10.1 ARMARIS APANTALLATS

P.AT07D

Versió _
Fabricant CONSUEGRA S. COOP.
Família Armaris apantallats
Tipus Producte
Classificació Apte ZONA 0
Data Inclusió 01/04/2019
Revisió de Validesa 31/10/2024
Descripció

Armari Tempest de sobretaula de dimensions reduïdes amb dues possibles opcions. L'armari PAT 07D ofereix alta protecció electromagnètica perquè el client inclogui la seva pròpia CPU, convertint el conjunt en una CPU Tempest acceptada per processar informació classificada en locals ZONA 0. CONSUEGRA s'ocupa de les adaptacions necessàries per a la seva correcta instal·lació i funcionament. Posteriorment, si el client desitgés canviar la CPU per una de més actualitzada, CONSUEGRA també pot ocupar-se de la seva instal·lació i funcionament. CONSUEGRA també ofereix la possibilitat de subministrar i instal·lar la CPU sol·licitada pel client com a part de la comanda, en aquest cas, el producte es codifica com a P.COMPT0-03.

Observacions

P.AT-06E

Versió
Fabricant CONSUEGRA S. COOP.
Família Armaris apantallats
Tipus Producte
Classificació Apte ZONA 0
Data Inclusió 01/12/2017
Revisió de Validesa 30/06/2024
Descripció

Armari apantallat cec de 38U. Dimensions 2102x625x1000 mm. Reordenació a través de 2 ventiladors amb termòstats independents amb cabal de fins a 2.700 m3/h.Distribuïdor intern amb diferencial i automàtic. Apte per instal·lació en locals amb classificació de ZONA 0.

Observacions

P.AT-02D

Versió

Fabricant CONSUEGRA S. COOP.

Família Armaris apantallats

Tipus Producte

Classificació Apte ZONA 0

Data Inclusió 01/12/2017

Revisió de Validesa 31/05/2024

Descripció

Armari apantallat de 19" i fins a 730 mm de longitud. Portes davanteres envidrades i portes laterals cegues. Filtres d'alimentació independents de 6A. Ventilació mitjançant electroventiladors. Apte per instal·lació en locals amb classificació de ZONA 0 amb equips classificats ZONA 2.

Observacions

P.AT-07

Versió _

Fabricant CONSUEGRA S. COOP.

Família Armaris apantallats

Tipus Producte

Classificació Apte ZONA 0

Data Inclusió 01/12/2017

Revisió de Validesa 31/05/2024

Descripció

Armari apantallat per a CPU. Disposa de safata extraible, ventilació i filtratge de les línies de dades i alimentació. Apte per instal·lació en locals amb classificació ZONA 0.

Observacions

SHATEM - SHELTER ARPA TEMPEST MULTIPROPOSITO

Versió

Fabricant	ARPA, EQUIPS MÒBILS DE CAMPANYA
Família	Armaris apantallats
Tipus	Producte
Classificació	Apte ZONA 0
Data Inclusió	01/01/2020
Revisió de Validesa	31/05/2024

Descripció

Contenidor shelter per a allotjament i/o operació d'equips informàtics, electrònics, optrònics de telecomunicacions i assimilables per a entorns CIS. Equipat amb els elements de filtratge i protecció EMI necessaris en escomeses de potència, dades i serveis per disposar d'apantallament intergral TEMPEST enfront d'emanacions comprometedores radiades i conduïdes.

Observacions

P.AT-06D

Versió

Fabricant	CONSUEGRA S. COOP.
Família	Armaris apantallats
Tipus	Producte
Classificació	Apte ZONA 0
Data Inclusió	01/12/2017
Revisió de Validesa	31/05/2024

Descripció

Armari apantallat cec de 25U. Dimensions 1524x625x1000 mm. Reordenació a través de 2 ventiladors amb termòstats independents amb cabal de fins a 2.700 m3/h. Distribuïdor intern amb diferencial i automàtic. Apte per instal·lació en locals amb classificació de ZONA 0.

Observacions

8.10.2 MONITORS

P.MONT0-11

Versió _
Fabricant CONSUEGRA S. COOP.
Família Monitors
Tipus Producte
Classificació SDIP-27 Level A
Data Inclusió 01/12/2021
Revisió de Validesa 31/05/2024
Descripció

Monitor LED Full HD de 22" i resolució 1920 x 1080p amb format panoràmic.
Observacions

8.10.3 PERIFÈRICS

P.KVMT0-01

Versió

Fabricant CONSUEGRA S. COOP.

Família Perifèrics

Tipus Producte

Classificació SDIP-27 Level A

Data Inclusió 01/12/2017

Revisió de Validesa 31/05/2024

Descripció

Commutador KVM per a dos sistemes. Basat en BELKIN SECURE OMNIVIEW F1DN102Uea amb certificació NIAP EAL 4+.

Observacions

P.TECT0-07

Versió

Fabricant CONSUEGRA S. COOP.

Família Perifèrics

Tipus Producte

Classificació SDIP-27 Level A

Data Inclusió 01/12/2017

Revisió de Validesa 31/05/2024

Descripció

Teclat QWERTY espanyol. Connexió USB.

Observacions

P.RATT0-04	
Versió	_
Fabricant	CONSUEGRA S. COOP.
Família	Perifèrics
Tipus	Producte
Classificació	SDIP-27 Level A
Data Inclusió	01/12/2017
Revisió de Validesa	31/05/2024
Descripció	
Ratolí òptic USB	
Observacions	

8.10.4 CPU

P.COMPT0-06	
Versió	_
Fabricant	CONSUEGRA S. COOP.
Família	CPU
Tipus	Producte
Classificació	SDIP-27 Level A
Data Inclusió	01/12/2021
Revisió de Validesa	31/05/2024

Descripció

CPU de sobretaula tempestitzada del model comercial HP PRODESK 600 G5 SFF. Aprovat per al seu ús combinat amb perifèrics TEMPEST de l'empresa CONSUEGRA S.COOP. en locals amb classificació de ZONA 0.

Observacions

P.COMT0-01	
Versió	-
Fabricant	CONSUEGRA S. COOP.
Família	CPU
Tipus	Producte
Classificació	SDIP-27 Level A
Data Inclusió	01/06/2018
Revisió de Validesa	30/11/2024

Descripció

CPU de sobretaula tempestitzada del model comercial HP ELITE 8000. Aprovat per al seu ús combinat amb perifèrics TEMPEST de l'empresa CONSUEGRA S. COOP. en locals amb classificació de ZONA 0.

Observacions

8.10.5 IMPRESSORES

P.IMPT0-04	
Versió	_
Fabricant	CONSUEGRA S. COOP.
Família	Impressores
Tipus	Producte
Classificació	SDIP-27 Level A
Data Inclusió	01/12/2021
Revisió de Validesa	31/05/2024
Descripció	

Impressora TEMPEST basada en el model HP Color LaserJet Enterprise M553dn.

Observacions

8.10.6 SERVIDOR

SOC-1-TP	
Versió	-
Fabricant	KRC ESPAÑOLA S.A.
Família	Servidor
Tipus	Producte
Classificació	SDIP-27/2 Level B
Data Inclusió	15/10/2023
Revisió de Validesa	26/10/2025

Descripció

Servidor multipropòsit d'alt rendiment orientat a desplegaments en entorns mòbils, on el consum i l'espai són elements crítics.

Les seves capacitats li permeten actuar com a servidor multifuncional i fins i tot oferir serveis de virtualització en una xarxa amb requisits mitjans. Compatible amb diferents sistemes operatius.

Observacions

N/A

9.PRODUCTES I SERVEIS DE CONFORMITAT I GOVERNANÇA DE LA SEGURETAT

9.1.GOVERNANÇA I PLANIFICACIÓ DE LA SEGURETAT

LightHouse Vulnerability Manager

Versió

Fabricant INNOTEC SYSTEM

Família Governança i Planificació de la Seguretat

Tipus Servei

Data Inclusió 01/04/2023

Revisió de Validesa 31/03/2025

Descripció

LightHouse VM (Vulnerability Management) d'Innotec Security és la plataforma d'auditoria contínua per a la detecció i priorització de riscos d'una organització, permetent optimitzar esforços i personalitzar la gestió, escurçant el temps d'exposició davant les amenaces.
LightHouse és l'eina perfecta per a la gestió de vulnerabilitats i la reducció de la superfície d'exposició dels organismes minimitzant els temps de gestió a través d'una eficient detecció de vulnerabilitats i notificació d'alertes, així com, oferint recomanacions per a un tractament oportú d'aquestes.
Amb el seu enfocament Asset Centric, LightHouse VM permet, entre d'altres:

- Gestionar vulnerabilitats durant el seu cicle de vida.
- Obtenir el nivell de risc d'una organització.
- Alertar i avaluar el risc d'una organització de forma primerenca.
- Agrupar en grups lògics de gestió a mida.
- Planificar els cicles de revisió de vulnerabilitats.
- Mesurar el nivell d'acompliment en la mitigació de les vulnerabilitats amb els seus quadres de comandaments de seguiment i SLAs.
- Integrar-se amb sistemes d'escaneig líders del mercat i les principals eines de ticketing per a la gestió directa de les vulnerabilitats.

Observacions

No aplica Procediment d'Ocupació Assegurança

9.2.ANÀLISI I GESTIÓ DE RISCOS

Archer Suite

Versió	6.11 (amb IRM Mobile v1.4)
Fabricant	RSA
Família	Anàlisi i Gestió de Riscos
Tipus	Producte
Data Inclusió	01/06/2023
Revisió de Validesa	30/06/2024

Descripció

Archer és una solució de Gestió Integral de Riscos (o també coneguda com a GRC) que permet unificar les activitats de govern corporatiu, risc i compliment de normes en una sola plataforma integrada. Actua com una protecció perimetral per aplicar una cultura d'administració de risc i responsabilitat compartida en tota la institució. Els permet instituir programes eficaços per fomentar les millors pràctiques i estandarditzar els processos directament a través de la seva tecnologia. Té plena visibilitat per respondre preguntes de la junta directiva i generar claredat entorn de l'estat del compliment de normes i dels riscos per a tota la institució. Disposem de modalitat servei SaaS i també on-premisses.

Dins d'Archer, els dominis de risc principals que es cobreixen són:

- Gestió de Riscos de Seguretat i IT (incloent gestió per a compliment de l'ENS)
- Continuïtat de Negoci i Resiliència Operacional
- Gestió de Riscos de Tercers
- Compliment (incloent-hi GDPR)
- Gestió de Risc Operacional
- Auditoria Interna
- ESG (Environmental, Social and Governance)
- Quantificació de Riesgos

Per a més informació: https://www.archerirm.com/

Observacions

Procediment d'Ocupació Assegurança pendent de publicació

9.3.NOTIFICACIÓ I GESTIÓ DE CIBERINCIDENTS

LUCIA

Versió	4.1
Fabricant	Centre Criptològic Nacional
Família	Notificació i Gestió de Ciberincidents
Tipus	Producte
Data Inclusió	01/10/2021
Revisió de Validesa	30/06/2024

Descripció

LUCIA és una eina per a la Gestió de Ciberincidents en les entitats de l'àmbit d'aplicació de l'Esquema Nacional de Seguretat. Amb ella, es pretén millorar la coordinació entre el CERT Governamental Nacional i els diferents organismes i organitzacions amb les quals col·labora. LUCIA ofereix un llenguatge comú de perillositat i classificació de l'incident i manté la traçabilitat i el seguiment del mateix. El sistema permet, a més, automatitzar les tasques i integrar-se amb altres sistemes ja implantats.

Observacions

Per a més informació, contactar amb lucia@ccn-cert.cni.es.

9.4.FORMACIÓ I CONCENCIACIÓ

Kymatio	
Versió	Kymatio 4.6.1
Fabricant	Kymatio
Família	Formació i Concenciació
Tipus	Servei
Data Inclusió	01/02/2024
Revisió de Validesa	31/07/2024
Descripció	

Kymatio® automatitza la conscienciació dels empleats i l'avaluació del seu estat d'alerta de forma desatesa i personalitzada, al mateix temps que proporciona una eina de gestió de risc associat a l'element humà, proporcionant mètriques, evolució en el temps i plans d'acció. Permet aconseguir la visibilitat necessària sobre l'exposició de la plantilla a incidents de seguretat de la informació i la seva mitigació incloent els següents serveis:

- Servei automàtic d'avaluació i conscienciació personalitzada, dissenyat per a augmentar el nivell d'alerta dels empleats en aquelles àrees clau com són: lloc de treball, compliment, protecció de dades, comunicacions, malware, gestió de contrasenyes i enginyeria social.
- Account Breach Escàner (ABS), que connecta la vigilància de credencials exposades amb el programa de conscienciació, analitzant repositoris en línia per a detectar filtracions i notificant a l'organització i empleats per a la seva mitigació.
- Les Simulacions d'Enginyeria Social (Trickster) permeten avaluar la preparació dels empleats davant diferents tipus d'atacs, incloent phishing, spear phishing, smishing, i QRs entre altres, identificant ràtios de resposta i àrees de millora.

La plataforma de gestió del ciberisc humà integra dades dels serveis descrits anteriorment, proporcionant insights valuosos per a la millora contínua. Amb mètriques en temps real i avaluació 360è, Kymatio enforteix la cultura de ciberseguretat, reduint riscos i assegurant la conformitat normativa per a una gestió proactiva del ciberisc humà.

Observacions

Procediment d'ocupació segura pendent de publicació

PSAT – Proofpoint Security Awareness Training

Versió

Fabricant Proofpoint

Família Formació i Concenciació

Tipus Servei

Data Inclusió 01/03/2022

Revisió de Validesa 31/05/2024

Descripció

PSAT -Proofpoint Security Awareness Training- és una solució de formació i capacitació de conscienciació en matèria de seguretat.

La solució, basada en un enfocament cíclic d'avaluació, educació, reforç i mesurament, ensenya als usuaris les millors pràctiques i els mostra com emprar-les quan s'enfronten a amenaces de seguretat, ajudant-los a evitar que els ciberatacs aconsegueixin el seu objectiu i convertint-los en l'última línia de defensa de les organitzacions.

Característiques Principals:

- Identifica el risc dels usuaris mitjançant Simulacions de Phishing i avaluacions de coneixement.
- Permet canviar el comportament dels usuaris, mitjançant més 350 mòduls de formació interactius que ofereixen exercicis pràctics perquè els usuaris reconeguin i evitin els atacs de phishing i altres fraus d'enginyeria social.
- Redueix l'exposició de l'organització, mitjançant un complement per a client de correu, els usuaris poden denunciar els missatges sospitosos amb un sol clic
- Avalua i analitza els resultats, la solució ofereix una visibilitat detallada i d'alt nivell que permet mesurar el progrés, avaluar l'acompliment i identificar el risc a nivell d'organització, departament i usuari.

Observacions

CCN-STIC-1701 Procediment d'Ocupació Assegurança PSAT

SMARTFENSE

Versió 3 i 4

Fabricant Defense Balance

Família Formació i Concenciació

Tipus Servei

Data Inclusió 01/10/2022

Revisió de Validesa 31/10/2024

Descripció

SMARTFENSE és la plataforma online de conscienciació en Seguretat de la Informació que permet generar comportaments segurs en els usuaris, afavorint la creació d'una cultura cibersegura. SMARTFENSE proveeix catàlegs de continguts predefinits 100% editables per adequar-se a la cultura de l'organització i a més, possibilita la creació de contingut propi. Ofereix també eines de simulació de Phishing i Ransomware per mesurar l'efectivitat de les accions realitzades i conèixer l'evolució en les respostes dels usuaris.

Observacions

No aplica la publicació de procediment d'ocupació assegurança.

Ángeles

Versió 1.0

Fabricant CSA / CCN

Família Formació i Concenciació

Tipus Servei

Data Inclusió 22/09/2023

Revisió de Validesa 31/08/2024

Descripció

Ángeles, plataforma de formació, capacitació i talent en ciberseguretat, amb una oferta formativa completa, que inclosa cursos online, webinars i diferent documentació en funció del perfil de l'usuari. La plataforma, disponible a Google Play i App Store, disposa d'una àrea privada, amb accés a través del sistema Cl@ve, des del qual accedir a l'expedient de cada alumne, amb les hores de formació rebudes, així com els cursos i sessions de conscienciació realitzades a la plataforma.

Observacions

N/A

10. REFERÈNCIES

[1]	CCN-STIC-106 Procediment d'inclusió de productes de seguretat TIC qualificats en el *CPSTIC.
[2]	CCN-STIC-140 Taxonomia de referència per a productes de Seguretat TIC.
[3]	CCN-STIC-102 Procediment per a l'Aprovació de Productes de seguretat TIC per a manejar informació Nacional classificada.
[4]	CCN-STIC-130 Requisits d'Aprovació de Productes de Xifra per a Manejar Informació Nacional Classificada.
[5]	CCN-STIC-151 Avaluació i Classificació *TEMPEST d'equips

11. ABREVIATURES

CC	*Common Criteria*
EDR	*Endpoint Detection and Response*
EPP	*Endpoint Protection Platform*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
PES	Procediment d'Ocupació Segura
RFS	Requisits Fonamentals de Seguretat
TIC	Tecnologies de la Informació i la Comunicació