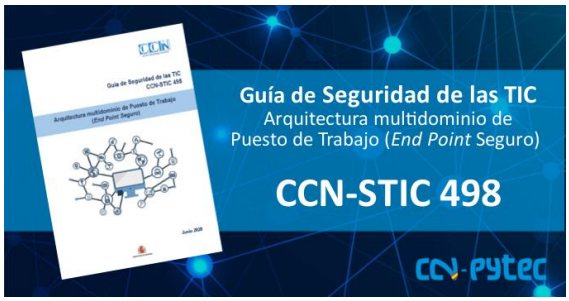
Boletín informativo del Departamento de Productos y Tecnologías de Seguridad TIC del Centro Criptológico Nacional (CCN-PYTEC).

Boletín CCN-PYTEC nº24 - 06/2020

Arquitecturas de Seguridad

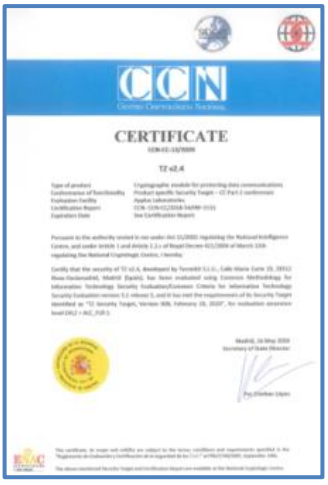
El CCN define una Arquitectura Multidominio de Puesto de Trabajo (06/2020).



El CCN ha publicado la Guía CCN-STIC-498 "Arquitectura multidominio de Puesto de Trabajo (End Point Seguro)", en la cual se plantean diferentes arquitecturas de seguridad posibles para que un terminal "End Point" puede acceder de forma segura a información con diferentes grados de clasificación y, en su caso, pertenteciente a diferentes ámbitos (nacional, OTAN, UE…). Este documento se completa con un Anexo A (CCN-STIC-498A) que incluye casos de uso específicos en los que un mismo equipo anfitrión va a manejar información clasificada de dos dominios de seguridad distintos: DIFUSIÓN LIMITADA y SIN CLASIFICAR.

Comunicaciones Tácticas Seguras

El Cifrador Personal del Combatiente, certificado Common Criteria (05/2020).



El Cifrador Personal del Combatiente (CIFPECOM) ha completado su certificación Common Criteria (EAL2+), como parte del proceso de aprobación de este producto de la empresa Tencobit. El CIFPECOM es un cifrador táctico de pequeño tamaño concebido para la protección de las comunicaciones sobre redes de bajo ancho de banda y sin estabilidad de enlace garantizada (p.ej. Red Radio de Combate, "SATCOM on the move", etc.). El CIFPECOM tiene capacidad de cifrado de voz táctica ("push to talk") según diferentes estándares (SCIP multipunto, STaC-IS NB y algunos modos TSVCIS), y también cuenta con capacidad de cifrado de datos IP sobre las redes mencionadas anteriormente. En próximas fechas, una vez se completen ciertas actividades propias de la evaluación cripto, está prevista la aprobación del primer producto disponible de esta familia (se prevé contar con varios productos adaptados a las necesidades de las FAS).

Intercambio seguro de información

PSTdiode de Autek Ingeniería incluido en el NIAPC (05/2020).

El diodo de datos hardware PSTdiode de Autek Ingeniería, certificado Common Criteria por el Organismo de Certificación del CCN, ha sido incluido en el "NATO Information Assurance Product Catalogue" (NIAPC) recientemente. Este producto, que también está incluido dentro del Catálogo de Productos STIC del CCN, es un dispositivo de protección de perímetro que permite la transferencia de información en un único sentido entre dos dominios de seguridad con garantía física de transmisión unidireccional. Su aplicación principal es la introducción de información en una red aislada en entornos clasificados. Existen modelos de transferencia de ficheros y tráfico UDP.

Novedades en el Catálogo de Productos STIC

IBM cualifica su producto IBM Secret Sever Government Edition en la familia de "Gestión de acceso privilegiado (PAM)" para ENS categoría ALTA (05/2020).

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

Gestión de acceso privilegiado (PAM)

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

- Gestión del Ciclo de Vida de las credenciales con privilegios:
  - Descubrimiento automatizado de cuentas privilegiadas y "onboarding" de las mismas en un repositorio central seguro.
  - Rotado automático de las credenciales y gestión, control y auditoria de las sesiones privilegiadas.
- Análisis del comportamiento del usuario privilegiado.
- Gestión de cuentas de servicio.
- Políticas de acceso basadas en RBAC y gestión de políticas de seguridad.
- Arquitectura escalable, alta disponibilidad y DR. Integración con múltiples plataformas "out-of-the-box".
- Módulo de "reporting" capaz de generar informes totalmente a medida.
- Securización de los procesos de DevOps.

Checkpoint cualifica su producto Checkpoint Endpoint Security (Sandblast Agent) en varias familias del CPSTIC para ENS categoría MEDIA (05/2020).

Check Point SandBlast Agent es una solución de protección avanzada para "endpoints" y navegadores de Internet. Garantiza la protección completa contra los diferentes vectores de amenazas con capacidades de prevención, detección y respuesta. Incorpora una gestión integrada disponible en nube o instalación local. Prestaciones:

Anti-virus / EPP (Endpoint Protection Platform)

EDR (Endpoint Detection and Response)

ens Esquema Nacional de Seguridad — ALTA / MEDIA / BÁSICA — MEDIA

- Emulación de amenazas ("sandbox") y extracción (entrega archivos limpios a usuarios en tiempo real).
- "Anti-ransomware" (prevención y reparación) y defensa contra ciberextorsión.
- "Anti-bot".
- "Anti-exploit".
- "Anti-malware".
- Análisis de comportamientos (detección y bloqueo).

La herramienta EMMA cualificada en la familia "otras herramientas" para ENS categoría ALTA (05/2020).

e</emma> Visibilidad y control sobre la red

Emma es una solución de seguridad para redes corporativas (tanto IT como OT) que permite a las organizaciones tener de manera centralizada la visibilidad, contexto, control y verificación del nivel de seguridad de todos los activos que se conectan a la red (Wi-Fi, cableada y VPN), desde dispositivos de usuarios a electrónica de red.

Consulte más información sobre esta herramienta en: https://www.ccn-cert.cni.es/soluciones-seguridad/emma.html

Otras herramientas

ens Esquema Nacional de Seguridad — ALTA / MEDIA / BÁSICA — ALTA

McAfee Network Security Platform cualificado en la familia "Dispositivos de prevención y detección de intrusiones" para ENS categoría ALTA (05/2020).

McAfee™

McAfee® Network Security Platform (NSP) es un sistema de detección y prevención de intrusiones (IDPS) de próxima generación que descubre y bloquea amenazas de malware sofisticadas en la red. Emplea técnicas avanzadas de detección y emulación, y va más allá de la comparación con patrones para ofrecer protección contra los ataques ocultos con un alto grado de precisión.

Para satisfacer las necesidades de las redes más exigentes, la plataforma puede adaptarse hasta 40 Gbit/s con un solo dispositivo y hasta 100 Gbit/s con dispositivos apilados. La integración de la solución de IPS simplifica las operaciones de seguridad mediante la combinación de la información en tiempo real de McAfee Global Threat Intelligence y los datos contextuales completos sobre usuarios, dispositivos y aplicaciones, con el fin de responder de manera rápida y precisa a los ataques que se propagan por la red. Otras funciones: administración centralizada, cifrado SSL, y alta disponibilidad y protección de recuperación ante desastre.

Dispositivos de prevención y detección de intrusiones

ens Esquema Nacional de Seguridad — ALTA / MEDIA / BÁSICA — ALTA

Han sido cualificados los siguientes modelos de *McAfee Network Security Platform*:

IPS-NS9100	IPS-NS9200	IPS-NS9300 P	IPS-NS9300 S	IPS-NS7150	IPS-NS7250	IPS-NS7350	IPS-NS7100
IPS-NS7200	IPS-NS7300	PS-NS5200	IPS-NS5100	IPS-NS3200	IPS-NS3100	NSM-MAPL-NG	

Stormshield aprueba su producto *Network Security UTM/NG-Firewall* (*Appliances* desde SN200 a SN6100 en 4 compilaciones distintas: S, M, L y XL) para SISTEMAS CLASIFICADOS (06/2020).

STORMSHIELD

Cortafuegos

El firewall de *Stormshield* es un cortafuegos de nueva generación de capa 7, IPS y concentrador de túneles VPN. Con capacidades de bloqueo de amenazas avanzadas, ataques de día cero, filtrado de navegación web o gestión de vulnerabilidades.

Pulse Secure cualifica su producto *Pulse* Policy Secure (PSA-300, PSA-3000, PSA-5000, PSA-7000c/f y *appliance* virtual), versión 9.1R1 (06/2020).

Control de Acceso a Red (NAC)

Servidores de autenticación

ens Esquema Nacional de Seguridad — ALTA / MEDIA / BÁSICA — ALTA

La solución de incorpora tanto elementos de perfilado de elementos de red como de cumplimiento de políticas de seguridad corporativa (NAC). Permite autenticar tanto usuarios (RBAC), sistemas u otros dispositivos (802.1xcontrol de acceso corporativo *Pulse Policy Secure (PPS)*, Radius y TACACS+) dentro del entorno corporativo, como el posterior *enforcement* (802.1x, SNMP).

Se integra de forma nativa con diferentes elementos corporativos como pueden ser MDMs, *Firewalls* o *Switches* dentro del entorno, para así hacer cumplir las normativas de seguridad y el control de acceso.

Pulse Secure®

Incorpora la capacidad de federación de perfiles de usuarios con terceros como pueden ser la solución de VPN (PCS) de *Pulse Secure* o diferentes Firewalls a través de

diferentes tecnologías (*syslog*, IF-MAP, API) permitiendo así elevar la seguridad y el manejo del control de acceso a niveles corporativos.

Aruba cualifica sus productos *Aruba Mobility Controller Series* (7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) versión 8.2 en la familia de cortafuegos y *Aruba Mobility Controller Series* (7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM) versión 8.5 en las familias de cortafuegos, dispositivos de red inalámbricos y VPN-IPSEC (06/2020).

Los *Aruba Mobility Controllers* funcionan como *gateway* entre redes cableadas e inalámbricas y proveen funciones de comando y control sobre los puntos de acceso de Aruba (APs) dentro de una red inalámbrica Aruba. Los *Mobility Controllers (MC)* y *Virtual Mobility Controllers (VMC)* de Aruba, son *switches* inalámbricos (*Appliance* físicos o virtuales) que proporcionan una amplia gama de servicios y características de seguridad que incluyen la movilidad de red inalámbrica y cableada, seguridad, administración centralizada, auditoría, autenticación, acceso remoto seguro, auto-chequeos de integridad y operación, filtrado de tráfico y funcionalidad de Gateway VPN.

Nuevos procedimientos de empleo seguro de productos del CPSTIC (06/2020).

Se ha publicado la Guía CCN-STIC-1202 "Procedimiento de empleo seguro del UEM MobileIron CORE". El producto UEM MobileIron CORE fue cualificado para ENS categoría ALTA dentro de la familia "Herramientas de gestión de dispositivos móviles" (MDM).

También se ha publicado la Guía CCN-STIC-1410 "Procedimiento de Empleo Seguro OMNISWITCH AOS". El producto OMNISWITCH AOS, de la empresa Alcatel-Lucent, fue cualificado para ENS categoría Alta dentro de la familia "Switches".

Además, se ha publicado la Guía CCN-STIC-1413 "Procedimiento de Empleo Seguro de Cortafuegos NGFW de Palo Alto Networks" para varios modelos de las series PA y VM. Estos productos están cualificados para ENS categoría ALTA en las familias "Cortafuegos" y "Redes privadas virtuales: IPSec".

Por su parte, dentro de las familia de "Enrutadores" para ENS categoría Alta, se ha publicado la Guía CCN-STIC-1414 "Procedimiento de empleo seguro Router Cisco Systems ISR/ASR". Se trata del procedimiento de empleo seguro para las series ISR 1100, 4000 y 4400 y ASR 1000.

Dentro de la familia de "Dispositivos móviles" para ENS categoría ALTA, se ha publicado la Guía CCN-STIC-1608 "Procedimiento de Empleo Samsung Galaxy (Android 10)". Este procedimiento de empleo seguro es aplicable a las nuevas familias de dispositivos de Samsung.

En la familia de "Cortafuegos" para ENS categoría ALTA, se ha publicado la Guía CCN-STIC-1415 "Procedimiento de Empleo Seguro UTM/NG-Firewall de Stormshield".

Por último, en la familia de "SIEM" para ENS categoría ALTA, se ha publicado la Guía CCN-STIC-1203 "Procedimiento de empleo seguro IBM QRadar 7.3.2."

Esquema Nacional de Evaluación y Certificación STIC

Layakk, nuevo laboratorio Common Criteria (05/2020).

Tras superar las auditorías ENAC y del Organismo de Certificación del CCN, el laboratorio Layakk está acreditado para realizar evaluaciones funcionaldes de seguridad Common Criteria hasta nivel EAL2. La resolución de la Secretaria de Estado Directora del CCN ha sido publicada en el BOE el pasado día 26 de mayo de 2020. Este laboratorio, perteneciente al Esquema Nacional de Evaluación y Certificación STIC (ENECSTIC), también está acreditado para la realización de evaluaciones LINCE.

Eventos

CCN-PYTEC participará en varios MOOC dentro de la C1b3rWall *Academy* (06/2020).

Debido a las restricciones impuestas por la COVID-19, la edición 2020 de la C1b3rWall Academy que organiza anualmente la Escuela Nacional de Policía, se realizará de forma "online" a través de diferentes MOOC ("*Massive Open Online Course*"). CCN-PYTEC participará en los siguientes MOOC:

- La criptografía: pasado, presente, futuro.
- Soluciones de comunicación segura en situaciones de emergencia.

Las distintas charlas se compartirán en la página web *del European Cybrecrime Training and Education Gropus (ECTEG)* pertenecientes a CEPOL, y serán difundidas a nivel institucional por la UE para todas las policías e instituciones asociadas.

Contacto

Correo electrónico CCN-PYTEC	**ccn-pytec@cni.es**
Twitter	**@CCNPYTEC**
LinkedIn	**https://www.linkedin.com/company/CCN-PYTEC**
Catálogo CPSTIC	**Enlace web**

CCN-PYTEC

Praeventio sit vincere

#SALIMOS MÁS FUERTES