
jtsec
Applus

I. Presentación

- Consultor de Ciberseguridad
- +2 años experiencia en LINCE
- jtsec Beyond IT Security

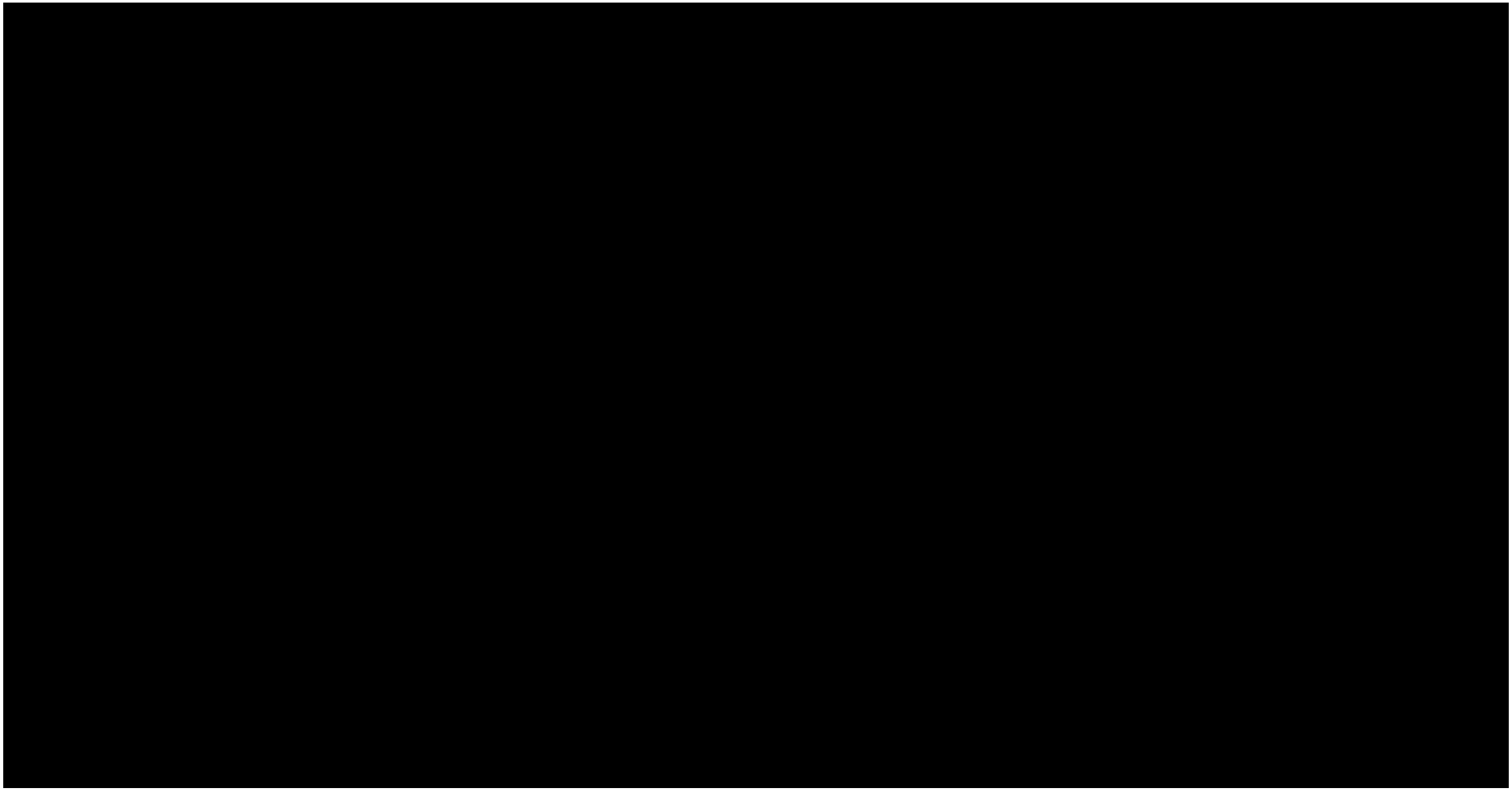
Usando el catálogo de productos CCN para mejorar la seguridad de tu empresa

26/09/2024

¿De qué va esto?

I. Presentación
II. ¿Qué es CCN y CPSTIC?
III. Tipos de certificaciones
IV. Riesgos de utilizar productos NO certificados
V. Beneficios de utilizar productos certificados
VI. ¿Cómo elegir un producto en Catálogo?
VII. Conclusiones

I. Y… ¿ jtsec ?



II. ¿Qué es CCN y CPSTIC?

El **Centro Criptológico Nacional (CCN)** es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la **seguridad de las Tecnologías de la Información** en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

- **C**atálogo de **P**roductos y Servicios de **S**eguridad de las **T**ecnologías de la **I**nformación y la **C**omunicación del Centro Criptológico Nacional.
- Facilitan la **adquisición de productos y servicios de seguridad confiables** a los organismos de la Administración Pública.
- **Certificación** de las **funcionalidades de seguridad de los productos y servicios** conforme a unos requisitos definidos por el CCN y publicación del Procedimiento de Empleo Seguro.

III. Tipos de certificaciones

Objetivo

Adquirir la **CONFIANZA** de que el producto evaluado proporciona las características de seguridad que declara tener.

¿Se puede determinar la seguridad de un producto?

NO. Podemos determinar grados de confianza en la seguridad de un producto

¿Cómo?

Con el **examen detallado del sistema o producto a evaluar** con el fin de encontrar posibles vulnerabilidades y **confirmar el nivel de seguridad declarado**.

III. Tipos de certificaciones

CRIPTOLÓGICA

EMANACIONES

FUNCIONAL

centro criptológico nacional

III. Tipos de certificaciones

Common Criteria

Certificate Authorizing Members **18**

Certificate Consuming Members **13**

CCN
CENTRO CRIPTOLÓGICO NACIONAL

CERTIFICATE

CCN-CC-010/2015

DNIe-DSCF (dispositivo seguro de creación de firma) Versión: 2.0

Type of product	Smartcard Operating System
Conformance of functionality	PP Conformance functionality
Protection Profile Conformance	Protection Profiles for secure signature creation device - Part 2: Device with Key Generation, v 2.0.1, January 2012
Evalutaion Facility	CESTI-INTA
Certification Report	INF-1506
Expiration date	See Certification Report

In accordance with the authority granted under Act 11/2002, regulating the National Intelligence Centre, and applying articles 1 and 2, second paragraph, letter c, of Royal Decree 421/2004, March 12th, regulating the National Cryptologic Centre, I hereby:

Certify that the security **of DNIe-DSCF (dispositivo seguro de creación de firma) Versión: 2.0**, developed by **Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda**, Calle Jorge Juan 106, 28009-Madrid, fulfills its Security Target identified as "Declaración de Seguridad de la tarjeta DNIe-DSCF 2.0", version: 1.1 revision: 1, 27/03/2015, to the extent defined by the evaluation assurance level **EAL4 + AVA_VAN.5**, using the norms "Common Criteria for Information Technology Security Evaluation" and "Common Methodology for Information Technology Security Evaluation", version 3.1 R4.

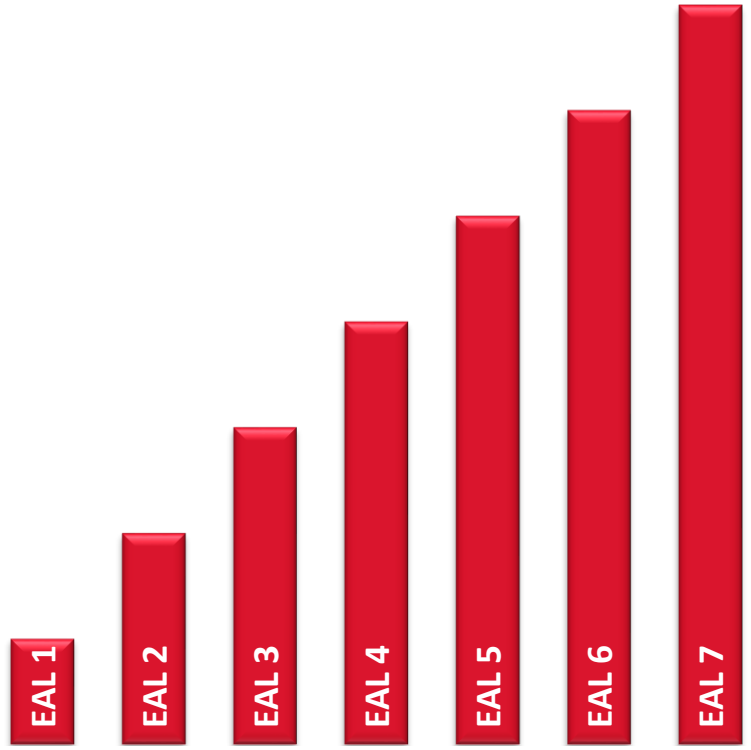
Madrid, September 16th 2015
Secretary of State Director

Félix Sanz Roldán

ENAC

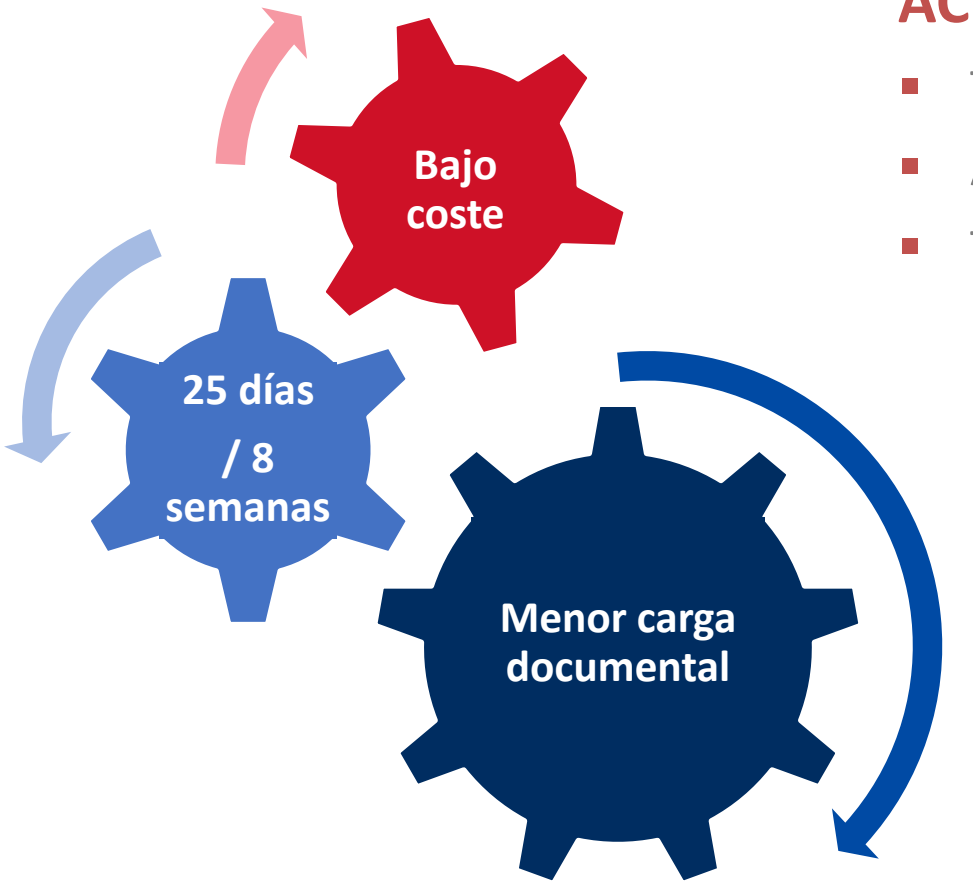
This certificate, its scope and validity are subject to the terms, conditions and requirements specified in the "Reglamento de Evaluación y Certificación de la Seguridad de las T.I.C." at PRE/2740/2007, September 19th.

The above-mentioned Security Target and Certification Report are available at the National Cryptologic Centre.



Nivel de aseguramiento (EAL)

III. Tipos de certificaciones

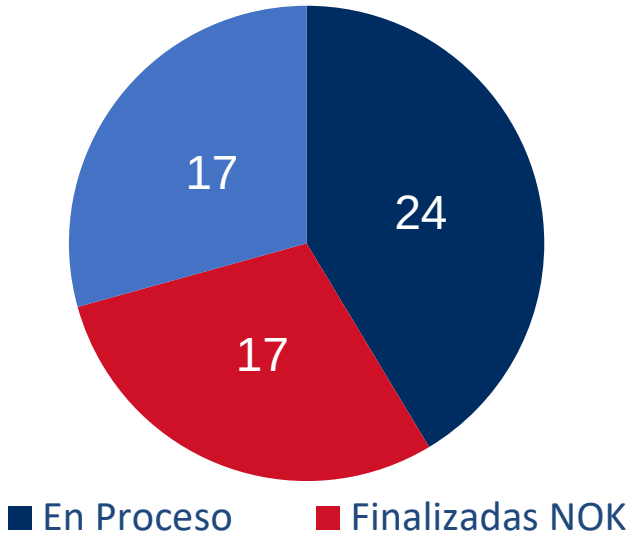


ACTIVIDADES DE EVALUACIÓN:

- Test funcionales
- Análisis de vulnerabilidades
- Test de penetración

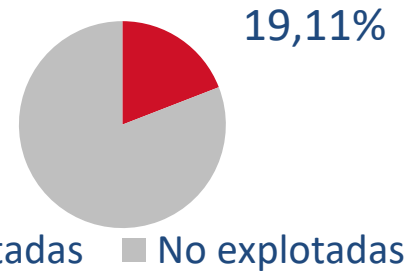
III. Tipos de certificaciones

Evaluaciones LINCE



Requisitos Funcionales

Vulnerabilidades



Aprox.: **6 vulnerabilidades corregidas** por evaluación

III. Tipos de certificaciones

Common Criteria

Certificación Nacional Esencial de Seguridad
CCN

Reconocimiento de la veracidad de su **Declaración de Seguridad** con un determinado nivel de confianza.


CERTIFICACIÓN
PRODUCTO

III. Tipos de certificaciones

- ✓ Actualmente, las certificaciones CC o LINCE no son aplicables a entornos en la nube:
  - **Imposibilidad de replicar el sistema en el laboratorio.**
  - **Imposibilidad de que este permanezca invariante.**

- ✓ **Estrategia**: **Evaluación continua** basada en **LINCE**.

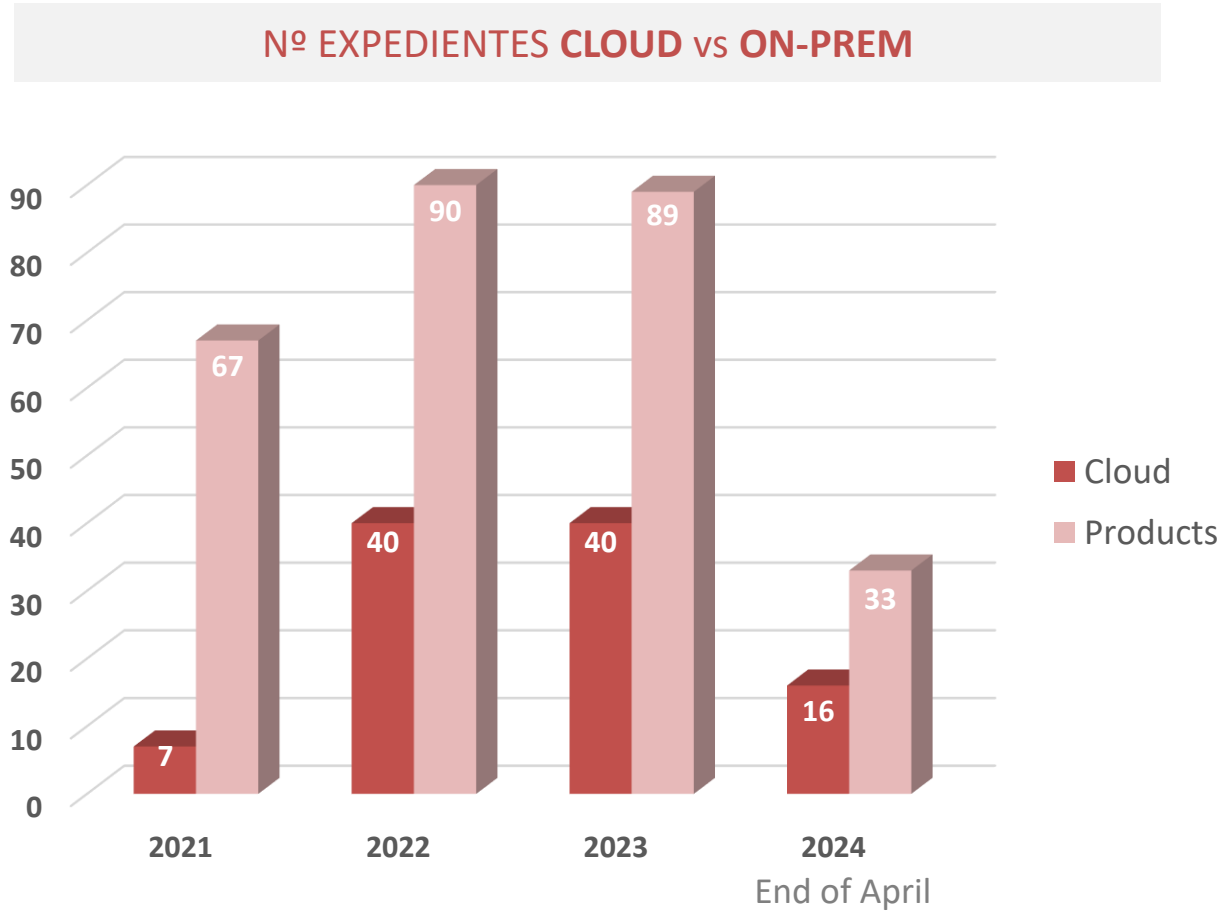
III. Tipos de certificaciones

1. El sistema que provee el servicio en la nube debe poseer la CERTIFICACIÓN DE CONFORMIDAD CON EL ENS.
2. La funcionalidad de seguridad suministrada por el servicio debe disponer de una CERTIFICACIÓN DE PRODUCTO o equivalente.
3. REQUISITOS DE TRANSPARENCIA. El proveedor deberá entregar al CCN información relativa a la arquitectura del sistema, certificación de producto, localización geográfica de datos y logs, etc.
4. PENTESTING. El servicio en la nube deberá superar con éxito un test de penetración.

III. Tipos de certificaciones

2024

48% de expedientes de **servicios de seguridad en la nube**



IV. Riesgos de utilizar productos NO certificados

¿Conoces algún caso de hackeo?

IV. Riesgos de utilizar productos NO certificados

- Ransomware
- SQL Injection
- Phishing
- Man-in-the-Middle (MITM)
- DDoS (Distributed Denial of Service)
- Cross-Site Scripting (XSS)
- Ataque de Fuerza Bruta
- Robo de Credenciales
- Ataques Zero Day
- Ingeniería Social
- Troyanos, Virus, …
- Exfiltración de Datos
- Eavesdropping
- Ataques a Proveedores de Servicios Cloud

V. Beneficios de utilizar productos certificados

1 **Reducción** del riesgo y **protección** de activos

Protección de datos sensibles

Prevención de vulnerabilidades

Evitar interrupciones de negocio

Esquema Nacional de Seguridad

Cumplimiento normativo

- **Productos certificados/cualificados**
- **Evaluaciones periódicas**

V. Beneficios de utilizar productos certificados

2 Mejora de la **reputación** y **confianza** en el mercado

Confianza del cliente

Ventaja competitiva

Reputación de la marca

- **Comunicación de las medidas de seguridad**
- **Cumplimiento de estándares**

V. Beneficios de utilizar productos certificados

3 **Ahorro** de **tiempo** y **recursos**

Reducción de auditorías y pruebas

Enfoque en el negocio principal

Automatización de tareas

- **Implementación de productos cualificados**
- **Tercerización de la seguridad**

V. Beneficios de utilizar productos certificados

4 Mejora de la **confianza de los socios** y **nuevas oportunidades** comerciales

Confianza de los socios comerciales

Oportunidades internacionales

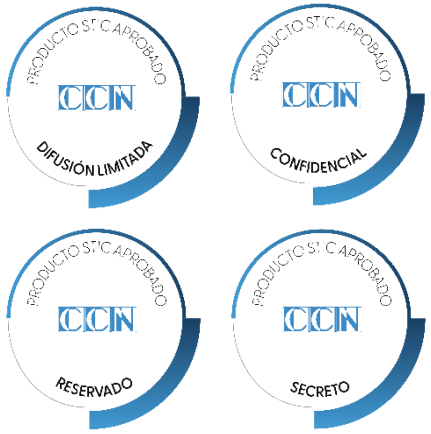
- **Compromiso con la seguridad**
- **Demostración de cumplimiento**

VI. ¿Cómo elegir un producto de catálogo?

El Catálogo de productos STIC se divide en **tres listados de productos y servicios**:

Cualificados

Adecuados para sistemas de información bajo el alcance del **Esquema Nacional de Seguridad**.



Aprobados

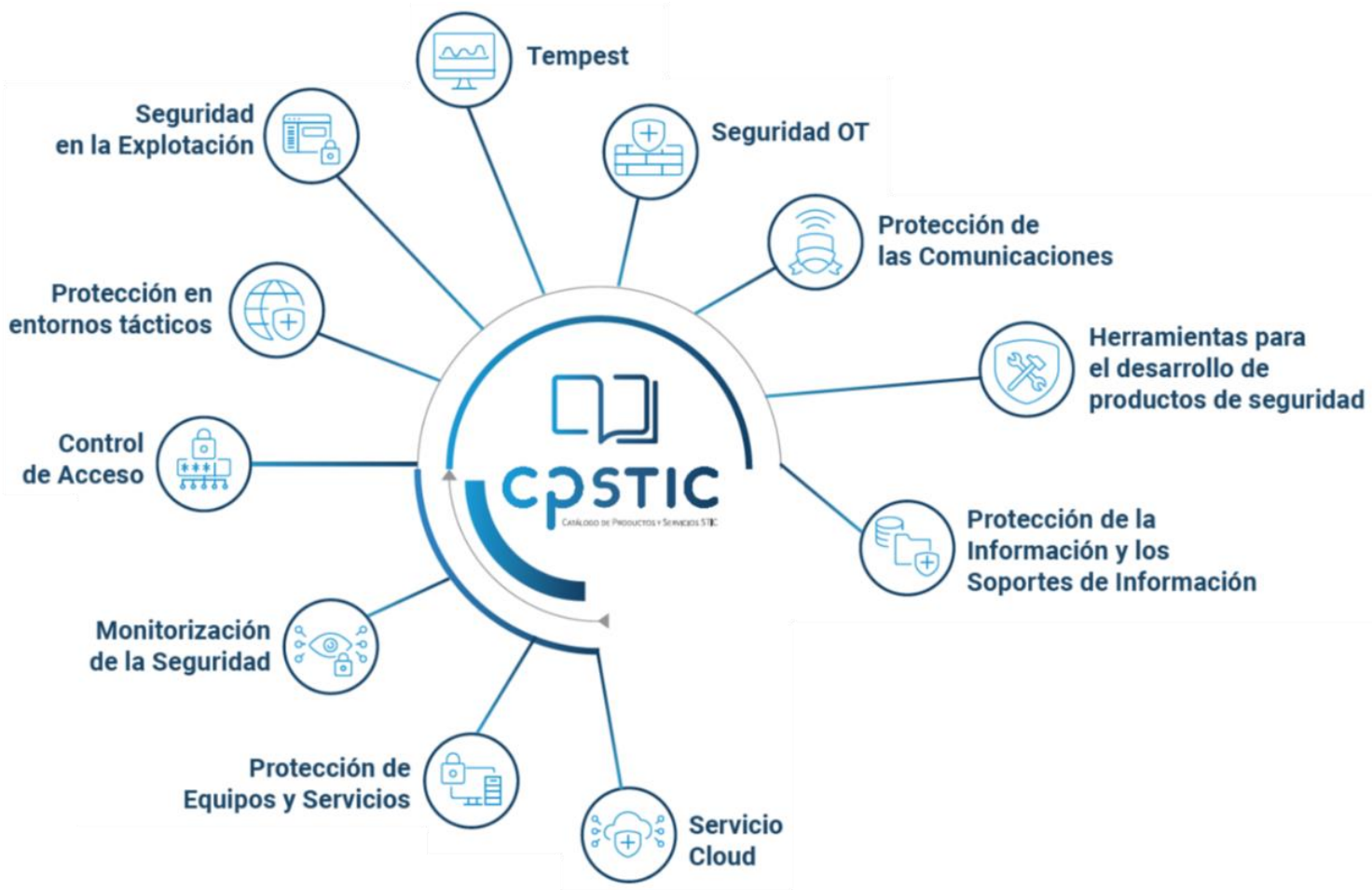
Adecuados para el manejo de **información clasificada**.

Conformidad y Gobernanza de la seguridad

Facilitan la gestión o implementación de **medidas de seguridad de un sistema de información**.

VI. ¿Cómo elegir un producto de catálogo?

TAXONOMÍA



VI. ¿Cómo elegir un producto de catálogo?

Organizado por "**familias**":

Protección de las comunicaciones	•Enrutadores / Switches •Cortafuegos •WAF •…
Protección de la Información y los Soportes de Información	•Cifrado de datos •Herramientas de borrado seguro •Dispositivos de gestión de claves •Gestión de metadatos •…
Controles de acceso	•Dispositivos biométricos •Gestión de Identidades •Servidores de Autenticación •…

RFS

Para cada familia se define un conjunto de **Requisitos Fundamentales de Seguridad**.

Guías CCN-STIC-140

VI. ¿Cómo elegir un producto de catálogo?

Descripción

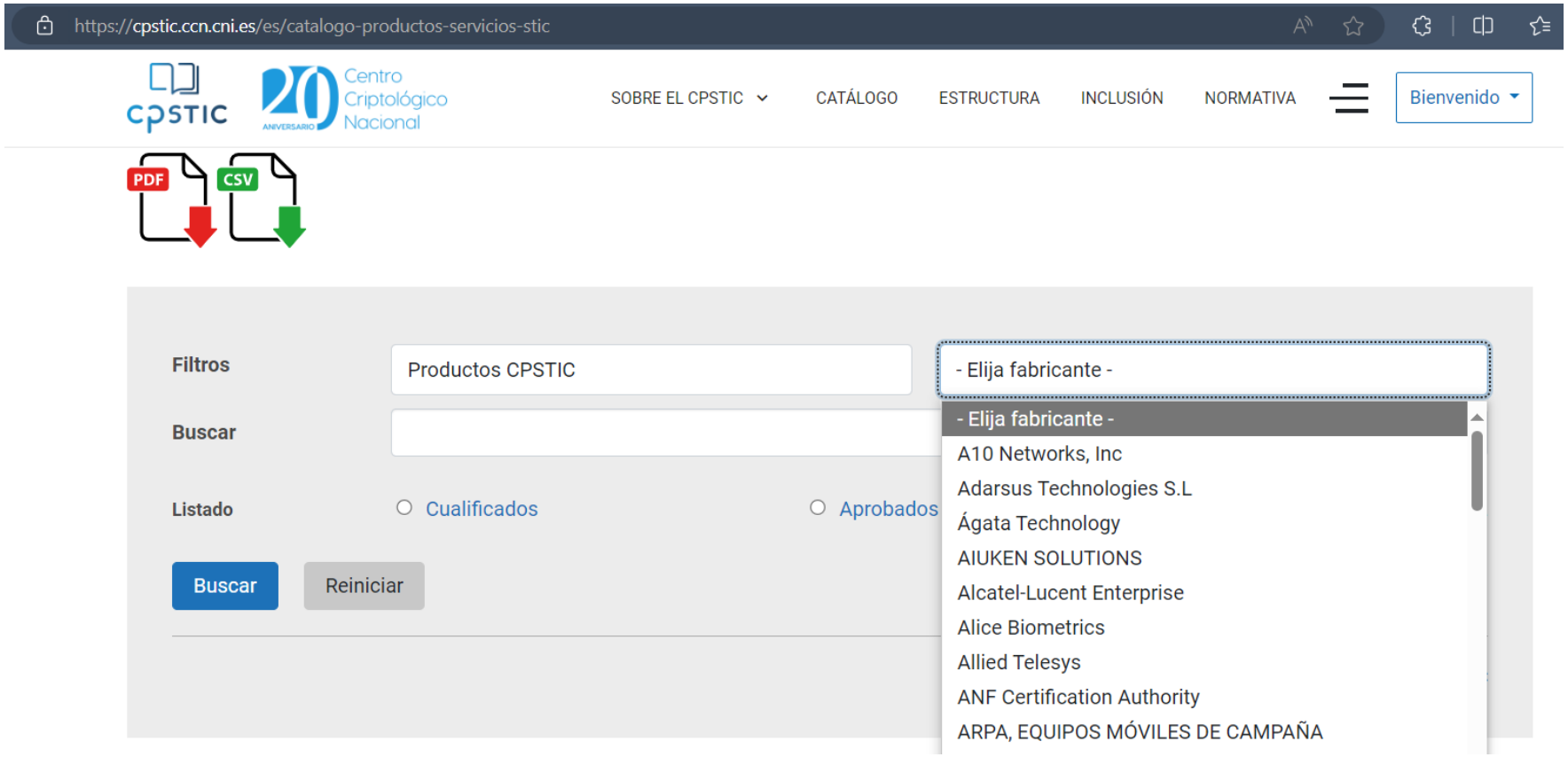
- Funcionalidad
- Caso de uso
- Alcance
- Certificaciones requeridas

Problema de Seguridad

- Hipótesis de entorno
- Activos
- Amenazas

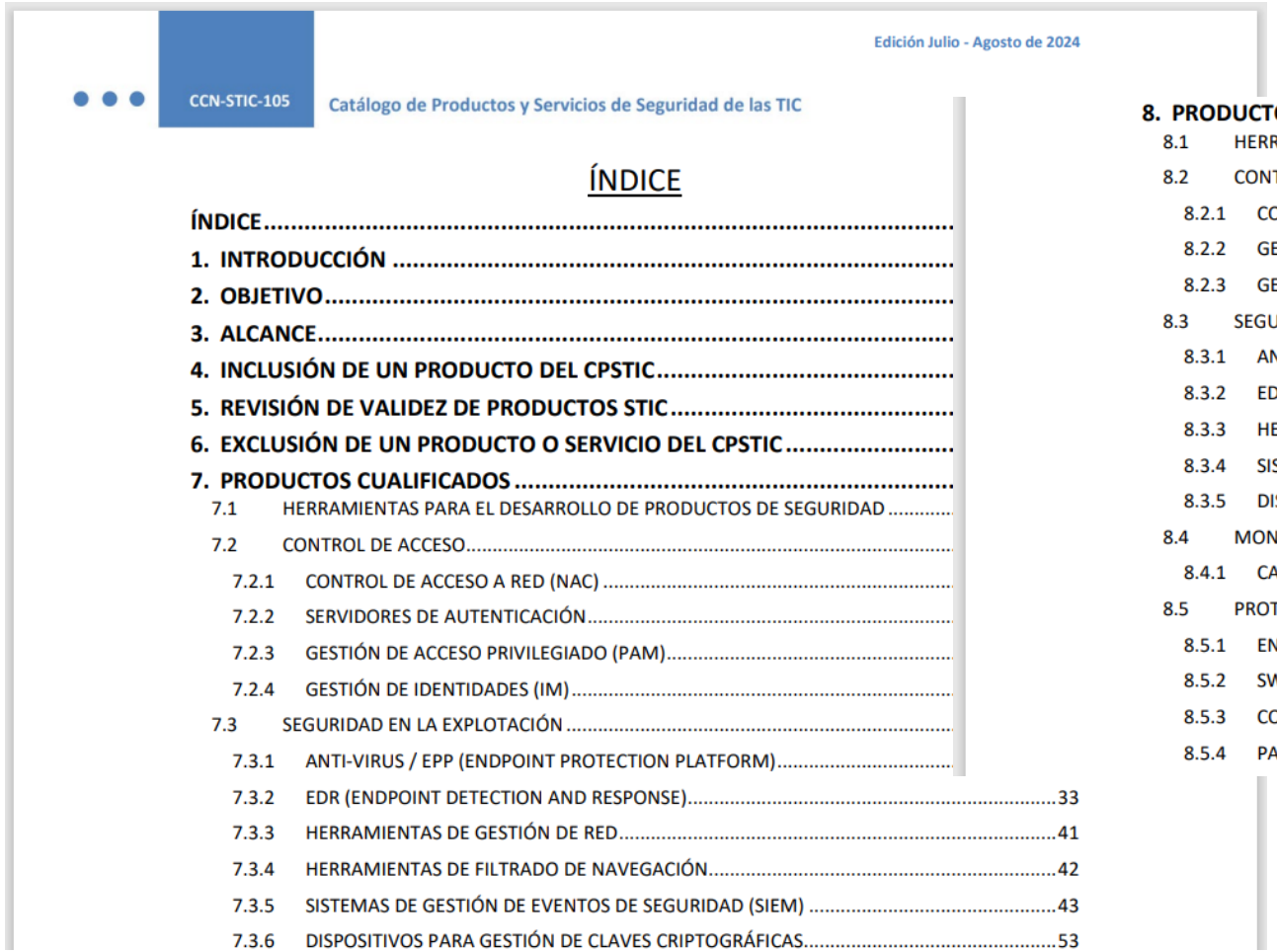
Req. fundamentales de seguridad

VI. ¿Cómo elegir un producto de catálogo?



https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

VI. ¿Cómo elegir un producto de catálogo?



Edición Julio - Agosto de 2024

CCN-STIC-105 Catálogo de Productos y Servicios de Seguridad de las TIC

ÍNDICE

VI. ¿Cómo elegir un producto de catálogo?

Chronicle SIEM	
Versión	N/A
Fabricante	Google
Familia	Sistemas de gestión de eventos de seguridad (SIEM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	16/02/2024
Revisión de Validez	30/09/2024

Descripción

Chronicle SIEM, una solución de gestión de eventos e información de seguridad (SIEM) nativa de la nube, permite a los clientes recopilar y analizar la telemetría de seguridad de toda su empresa para potenciar la detección, investigación y remediación de amenazas.
Como parte del servicio, Chronicle SIEM normaliza, correlaciona y enriquece los datos de seguridad para proporcionar análisis y contexto sobre actividades sospechosas.
Chronicle SIEM incluye Google Cloud Threat Intelligence, que es un servicio de inteligencia de amenazas agregado para clientes de Chronicle SIEM que aprovecha la inteligencia de amenazas de Google para resaltar amenazas en sus entornos de nube y on-premise.
Está respaldado por analistas de amenazas de Google que verifican los indicadores maliciosos en la telemetría de seguridad y revelan alertas contextualizadas a los clientes, lo que les permite dar una respuesta informada.

Observaciones

Procedimiento de Empleo Seguro pendiente de publicación

AWS Key Management Service (KMS)	
Versión	
Fabricante	AWS
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	30/09/2024

Descripción

AWS Key Management Service (KMS) facilita la creación y la administración de claves criptográficas y el control de su uso en una amplia gama de servicios de AWS y en sus aplicaciones. Utiliza módulos de seguridad de hardware que se han validado según FIPS 140-2 para proteger sus claves.
AWS KMS le proporciona un control centralizado sobre las claves criptográficas que se utilizan para proteger sus datos. El servicio está integrado con otros servicios de AWS, lo que facilita el cifrado de los datos que almacena en estos servicios y el control del acceso a las claves que los descifran. Los servicios integrados con KMS se pueden encontrar en https://aws.amazon.com/kms/

Observaciones

CCN-STIC-887A Guía de configuración segura AWS

VI. ¿Cómo elegir un producto de catálogo?

AWS Identity Access Management (IAM) + AWS STS	
Versión	
Fabricante	AWS
Familia	Gestión de identidades (IM)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/08/2022
Revisión de Validez	30/09/2024
Descripción	

AWS Identity and Access Management (IAM) permite controlar de forma segura el acceso a los servicios y recursos de AWS para sus usuarios, grupos y roles de AWS. Se pueden crear y administrar controles de acceso de grano fino con permisos, especificar quién puede acceder a qué servicios y recursos, y bajo qué condiciones.

Familia: **Gestión de Identidades (IM)**

Protección ante:

- Fuerza bruta
- Robo de credenciales
- …

VI. ¿Cómo elegir un producto de catálogo?

Falcon Sensor con Falcon Console Cloud	
Versión	7.05 (Falcon Sensor)
Fabricante	CrowdStrike
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2022
Revisión de Validez	30/04/2025

Descripción

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

Familia: **Anti-virus / EPP (Endpoint Protection Platform)**

Protección ante:

- Malware (troyanos, virus, …)
- Actividades maliciosas
- …

VI. ¿Cómo elegir un producto de catálogo?

Google KMS with EKM solution	
Versión	N/A
Fabricante	Google Cloud
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/05/2023
Revisión de Validez	30/04/2025
Descripción	

Google Cloud External Key Manager (EKM) es un servicio de Google Cloud que permite a los clientes generar y gestionar claves criptográficas de cifrado nativo de información en la nube a través de un tercero, protegidas a través de un Hardware criptográfico que está fuera de las infraestructuras de nube de Google. La protección de la información con claves generadas, protegidas y gestionadas fuera del proveedor de nube, habilita escenarios de soberanía del dato desde el momento en que la información almacenada en la nube de Google Cloud solo podrá ser descifrada por el gestor externo de la clave, que podrá ser:

- El propio usuario final mediante un módulo EKM instalado en sus propias infraestructuras.
- Un socio de confianza del usuario final que hospede y gestione dicho módulo EKM en sus infraestructuras.
- Uno de los socios locales de Google Cloud (sometidos exclusivamente a legislación Española) con la infraestructura ya preconfigurada y preparada para ofrecer este servicio desde la plataforma de Google Cloud, como "Control de Soberanía" (por ejemplo, SIA/Minsait/Indra para España, Thales para Francia o T-Systems para Alemania).

El servicio EKM se presta desde múltiples regiones de Google Cloud, incluida la de España. Más información aquí: https://cloud.google.com/kms/docs/ekm?hl=es-419

Familia: **Dispositivos para gestión de claves criptográficas**

Protección ante:

- Robo de credenciales
- Acceso no autorizado de información crítica
- …

VI. ¿Cómo elegir un producto de catálogo?

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

Descripción

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

Familia: **Enrutadores**

Protección ante:

- Tráfico no autorizado
- Uso de protocolos no seguros
- …

VI. ¿Cómo elegir un producto de catálogo?

Sophos Firewall	
Versión	SFOS v20.0
Fabricante	Sophos
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	08/08/2024
Revisión de Validez	31/01/2025

Descripción

Sophos Firewall es una solución integral de seguridad de red que ofrece capacidades avanzadas de firewall, protección contra amenazas, filtrado web, control de aplicaciones y un sistema de prevención de intrusiones. El firewall admite alta disponibilidad y rendimiento mediante la agrupación en clústeres y el equilibrio de carga. También incluye controles de identidad de usuario, así como informes y análisis detallados. En resumen, combina múltiples funciones de seguridad en una solución fácil de gestionar, adecuada para redes de todos los tamaños.

Familia: **Firewall**

Protección ante:

- Amenazas externas
- Filtrado web
- Intrusiones
- …

VI. ¿Cómo elegir un producto de catálogo?

Procedimiento de Empleo Seguro (PES)

- Documento que detalla las **guías de uso y despliegue seguro** del producto/servicio que tiene entrada en Catálogo.
- Indispensable para que la certificación/cualificación tenga la **máxima duración** (solo 6 meses si no se presenta PES).
- **No es una guía completa.** Su objetivo es indicar las tareas concretas que se deben seguir para desplegar una configuración segura conforme a lo evaluado.
- Puede tener **referencias a otras guías de instalación y configuración** del producto/servicio.

VI. ¿Cómo elegir un producto de catálogo?

Procedimiento de Empleo Seguro (PES)

ÍNDICE

VI. ¿Cómo elegir un producto de catálogo?

Procedimiento de Empleo Seguro (PES)

ÍNDICE

VI. ¿Cómo elegir un producto de catálogo?

Procedimiento de Empleo Seguro (PES)

ÍNDICE

VI. ¿Cómo elegir un producto de catálogo?

Procedimiento de Empleo Seguro (PES)

ÍNDICE

VI. ¿Cómo elegir un producto de catálogo?

Procedimiento de Empleo Seguro (PES)

ÍNDICE

VI. ¿Cómo elegir un producto de catálogo?

Procedimiento de Empleo Seguro (PES)

ÍNDICE

VI. ¿Cómo elegir un producto de catálogo?

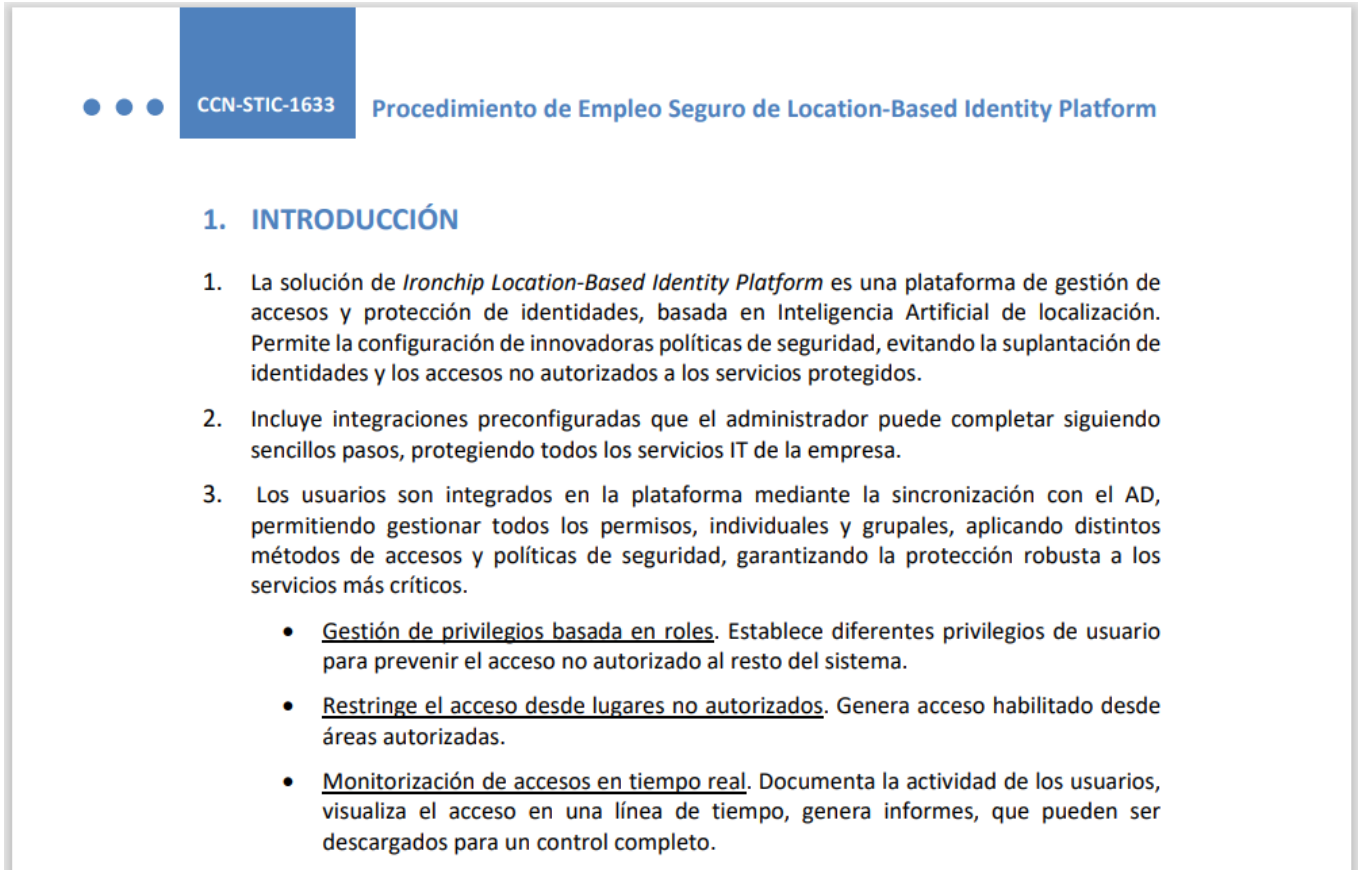
IRONCHIP Location-Based Identity Platform N/A

Listado: Cualificado
Fabricante: Ironchip Telco, S.L.
Categoría: Control de Acceso
Familia: Servidores de Autenticación
Tipo: Producto
Categoría ENS: Alta
Cualificado desde: 01/11/2023
Cualificado hasta: 30/04/2026

La solución de Ironchip Location-Based Identity Platform (LBAuth) represe
gestión de accesos y protección de identidades basada en inteligencia art
plataforma permite la configuración de políticas de seguridad innovadoras
suplantación de identidades y el acceso no autorizado a los servicios prot
Ironchip LBAuth incluye integraciones preconfiguradas que el administrad
sencillos, protegiendo de esta manera todos los servicios de tecnología d
usuarios son integrados dinámicamente en la plataforma, lo que posibilita
individuales como grupales, mediante la aplicación de diversos métodos
Esto asegura una protección sólida para los servicios más críticos de la o
de esta solución incluyen: - Gestión de privilegios basada en roles: Esta ca
diferentes niveles de privilegios de usuario, previniendo así el acceso no a
Restricción de acceso desde lugares no autorizados: La plataforma gener
desde áreas autorizadas, llevando la seguridad de la empresa al siguiente
personas autorizadas tengan acceso a los recursos protegidos. - Monitori
plataforma documenta la actividad de los usuarios, permitiendo a los administradores visualizar el acceso en una línea de tiempo. Además, ofrece la posibilidad de generar informes detallados que pueden ser descargados para un control completo del sistema.

CCN-STIC-1633 Procedimiento de Empleo Seguro Location-Based Identity Platform IRONCHIP

VI. ¿Cómo elegir un producto de catálogo?

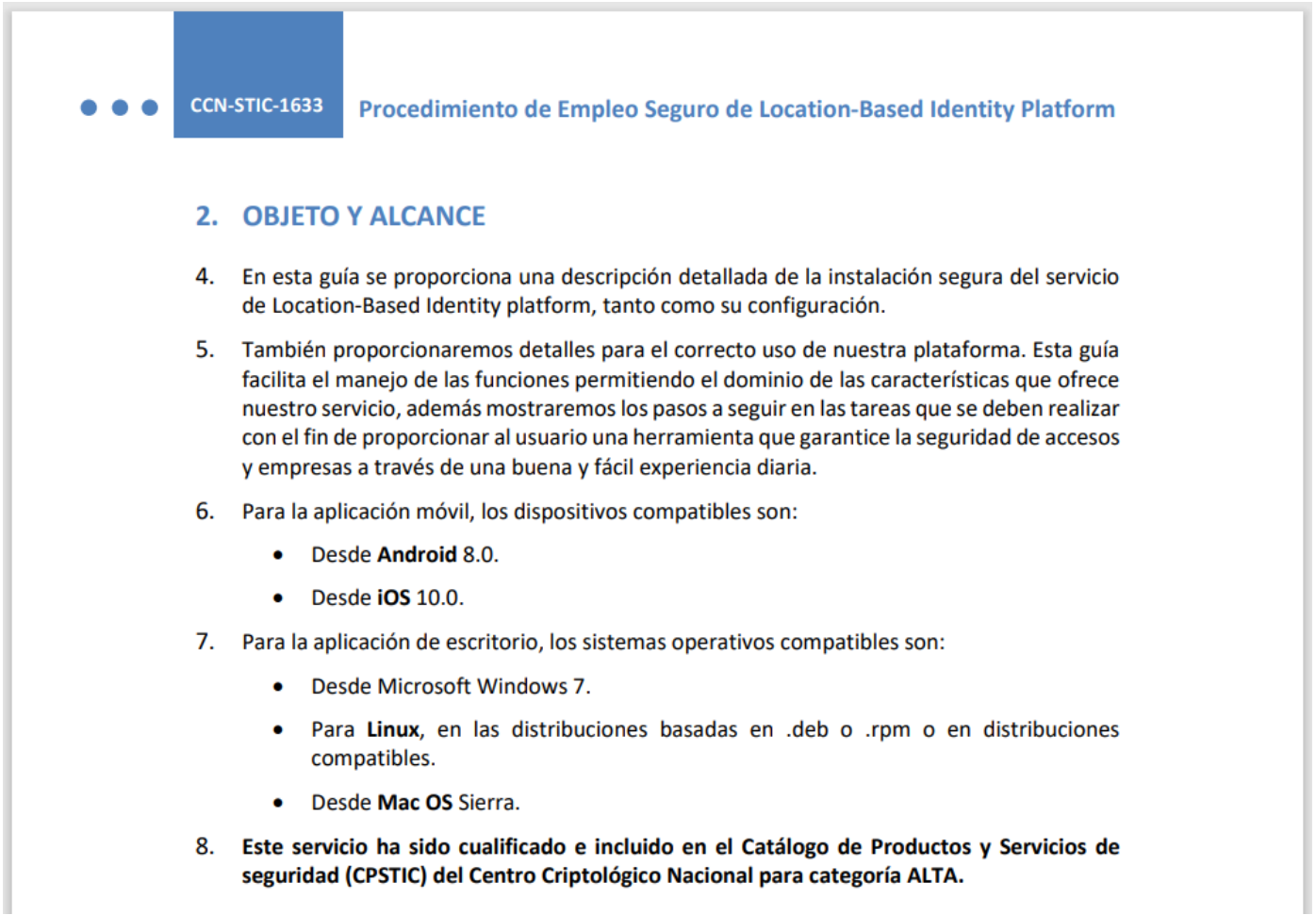


CCN-STIC-1633 Procedimiento de Empleo Seguro de Location-Based Identity Platform

1. INTRODUCCIÓN

1. La solución de *Ironchip Location-Based Identity Platform* es una plataforma de gestión de accesos y protección de identidades, basada en Inteligencia Artificial de localización. Permite la configuración de innovadoras políticas de seguridad, evitando la suplantación de identidades y los accesos no autorizados a los servicios protegidos.
2. Incluye integraciones preconfiguradas que el administrador puede completar siguiendo sencillos pasos, protegiendo todos los servicios IT de la empresa.
3. Los usuarios son integrados en la plataforma mediante la sincronización con el AD, permitiendo gestionar todos los permisos, individuales y grupales, aplicando distintos métodos de accesos y políticas de seguridad, garantizando la protección robusta a los servicios más críticos.
    - Gestión de privilegios basada en roles. Establece diferentes privilegios de usuario para prevenir el acceso no autorizado al resto del sistema.
    - Restringe el acceso desde lugares no autorizados. Genera acceso habilitado desde áreas autorizadas.
    - Monitorización de accesos en tiempo real. Documenta la actividad de los usuarios, visualiza el acceso en una línea de tiempo, genera informes, que pueden ser descargados para un control completo.

VI. ¿Cómo elegir un producto de catálogo?



CCN-STIC-1633 Procedimiento de Empleo Seguro de Location-Based Identity Platform

2. OBJETO Y ALCANCE

4. En esta guía se proporciona una descripción detallada de la instalación segura del servicio de Location-Based Identity platform, tanto como su configuración.
5. También proporcionaremos detalles para el correcto uso de nuestra plataforma. Esta guía facilita el manejo de las funciones permitiendo el dominio de las características que ofrece nuestro servicio, además mostraremos los pasos a seguir en las tareas que se deben realizar con el fin de proporcionar al usuario una herramienta que garantice la seguridad de accesos y empresas a través de una buena y fácil experiencia diaria.
6. Para la aplicación móvil, los dispositivos compatibles son:
   - Desde **Android** 8.0.
   - Desde **iOS** 10.0.
7. Para la aplicación de escritorio, los sistemas operativos compatibles son:
   - Desde Microsoft Windows 7.
   - Para **Linux**, en las distribuciones basadas en .deb o .rpm o en distribuciones compatibles.
   - Desde **Mac OS** Sierra.
8. **Este servicio ha sido cualificado e incluido en el Catálogo de Productos y Servicios de seguridad (CPSTIC) del Centro Criptológico Nacional para categoría ALTA.**

VI. ¿Cómo elegir un producto de catálogo?

6.1 MODO DE OPERACIÓN SEGURO

52. El diseño del producto se ha concebido con un enfoque centrado en la seguridad. Se han implementado medidas y protocolos específicos para garantizar un desempeño seguro en todas las posibles configuraciones del producto. Los valores por defecto han sido cuidadosamente seleccionados y configurados de manera que, en la mayoría de los casos, sean apropiados para un uso seguro y eficiente.

53. El producto no cuenta con distintos modos de operación. La configuración inicial del producto es segura por defecto.

6.2 AUTENTICACIÓN

6.2.1 AUTENTICACIÓN DEL SERVICIO

54. Los accesos a la herramienta de administración están protegidos por defecto mediante el propio producto quedando excluido cualquier mecanismo de autenticación no seguro.

55. Se ha restringido el acceso a la herramienta de administración únicamente a usuarios con privilegios de administrador. Esta limitación asegura que solo aquellos con los niveles adecuados de autorización puedan llevar a cabo funciones administrativas, proporcionando una capa de control adicional y mitigando posibles amenazas internas.

6.2.2 AUTENTICACIÓN DE APLICACIONES

VII. Conclusiones

EN RESUMEN…

- Los productos del CPSTIC ofrecen unas garantías de seguridad superiores por haber superado con éxito un proceso de evaluación/certificación.
- Elevan el nivel de seguridad ofrecido por un Sistema TIC.

PERO…

- Los productos no son infalibles ni están libres de vulnerabilidades.
- La seguridad de los productos es solo una parte de la seguridad de un sistema.
- Se ofrecen garantías técnicas sobre el producto. No sobre el fabricante.

VII. Conclusiones

PRÁCTICAS RECOMENDADAS…

- Autenticación Multifactor (MFA)
- Cifrado de datos
- Actualización y parches constantes
- Capacitación del personal
- Monitorización continua
- Segmentación de redes
- Políticas de respaldo regulares

Protección como inversión

VII. Conclusiones

El CPSTIC tiene como objetivo **CUBRIR LAS NECESIDADES** transmitidas por las Administraciones Públicas

Si quieres adquirir un producto / servicio de seguridad y **NO** está en el CPSTIC

PÍDESELO AL FABRICANTE / PROVEEDOR

cpstic.ccn@cni.es

Contacto

jtsec: Beyond IT Security

Granada & Madrid – Spain

hello@jtsec.es

@jtsecES

www.jtsec.es

"Any fool can make something complicated. It takes a genius to make it simple."
Woody Guthrie