

Categorías y familias del CPSTIC



¿Cómo están organizados los productos y servicios en el catálogo?

Terminología CPSTIC

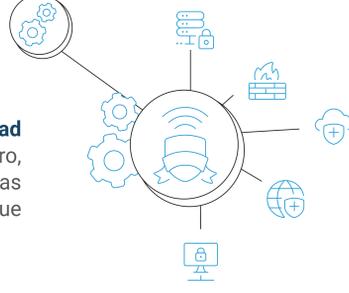


Categoría

Clasificación de acuerdo a las **medidas de seguridad que aporta** (p.ej.: control de acceso, protección de las comunicaciones, etc.). Se basarán en las categorías que componen el marco operacional [op.XXX] y de medidas de protección [mp.XXX] recogidas en el Anexo II del ENS, siempre y cuando estas resulten aplicables a productos. Cada categoría está compuesta de un conjunto de familias.

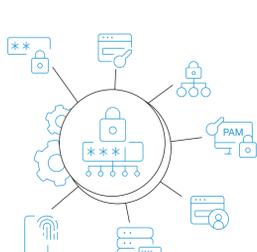
Familia

Clasificación de producto de acuerdo a su **funcionalidad principal** (p.ej.: cortafuegos, herramienta de borrado seguro, etc.). Un producto o servicio podría ser incluido en una o varias familias de acuerdo a las funcionalidades de seguridad que suministre.



CUALIFICADOS

Control de acceso



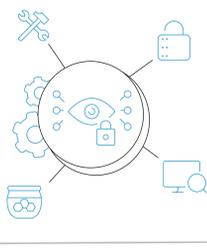
- o Control de acceso a red (NAC)
- o Dispositivos biométricos
- o Herramientas multifactor
- o Gestión de identidades (IM)
- o Dispositivos single sign-on
- o Servidores de autenticación
- o Gestión de acceso privilegiado (PAM)

Seguridad en la explotación

- o Antivirus | Endpoint Protection Platform (EPP)
- o Filtrado de navegación
- o Endpoint Detection and Response (EDR)
- o Sistemas de gestión de eventos de seguridad
- o Herramientas de gestión de red
- o Dispositivos para gestión de claves criptográficas
- o Actualización de sistemas
- o Herramientas de gestión de dispositivos (UEM)



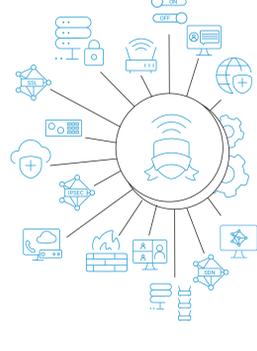
Monitorización de la seguridad



- o IDS, IPS y AntiDDoS
- o Captura, monitorización y análisis de tráfico
- o Sistemas HoneyPot | HoneyNet
- o Herramientas de sandbox

Protección de las comunicaciones

- o Enrutadores
- o Cortafuegos
- o Pasarelas seguras de intercambio de datos
- o Herramientas de voz por IP (VoIP)
- o Dispositivos de red inalámbricos
- o Switches
- o Proxies
- o Diodos de datos
- o Cifradores IP
- o Web Application firewall (WAF)
- o Redes privadas virtuales: IPSEC
- o Redes privadas virtuales: SSL
- o Redes definidas por software (SDN)
- o Herramientas de videoconferencia
- o Herramientas de mensajería instantánea (IM)



Protección de la información y soportes de información



- o Cifrado y compartición segura de información
- o Herramientas para firma electrónica
- o Sistemas de prevención de fugas de datos
- o Almacenamiento cifrado de datos
- o Herramientas de Borrado Seguro
- o Hardware Security Module (HSM)

Protección de equipos y Servicios

- o Dispositivos móviles
- o Protección de correo electrónico
- o Sistemas operativos
- o Copias de seguridad
- o Plataformas confiables
- o Infraestructura de escritorio virtual (VDI)
- o Balanceadores de carga
- o Hiperconvergencia
- o Virtualización
- o CASB
- o Herramientas de videoidentificación
- o Conmutadores KVM



Herramientas para el desarrollo de productos de seguridad



Seguridad OT



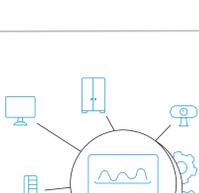
APROBADOS

Protección en entornos tácticos

- o Plataformas y dispositivos tácticos confiables
- o Soluciones para protección de las comunicaciones tácticas



Tempest



- o Armarios apantallados
- o Periféricos
- o Monitores
- o CPU
- o Impresoras

CONFORMIDAD Y GOBERNANZA

Gobernanza y planificación de la seguridad



Normativa de seguridad y conformidad



Notificación y gestión de ciberincidentes



Formación y concienciación en ciberseguridad



Análisis y Gestión de Riesgos



Intercambio de ciberinteligencia

