Ciberseguridad en Manufactura, retos y mejores prácticas

Mary Carmen Vargas C.
Coordinadora Centro de Ciberseguridad Industrial CCI, Ecuador
Oficial de Seguridad de la Información de CELEC EP

Agenda

01 Ciberataques en entornos industriales /Amenazas en OT

02 Retos

03 Mejores Prácticas

04 Preguntas y Respuestas


Ciberataques en entornos industriales /Amenazas


CNN Exclusive
DHS Video
CNN

Cronología de los principales ataques a los ICS

2009

NIGHT DRAGON

Dirigido: Industria Petroquímica, gas y petróleo.

OB: espionaje y robo de información sensible.

Ataque: spear phising y vlnerabilidades en Windows

2010

STUXNET

Dirigido: Central nuclear Iraní

1ra arma de ciberguerra,

OB: retrasar el programa nuclear iraní.

Ataque: Malware infectó la Central nuclear Natanz, en Iran.

2011

DUQU

Dirigido: Sistemas SCADA de las empresas de Medio Oriente

OB: Obtener información SCADA

2012

FLAME

Dirigido: Empresa de petróleo y gas de Medio Oriente y Europa

OB: recabar información

VA: Spear Phising, USB.

Funcionalidades : activa Camara web y micrófonos

2013

DRAGON FLY

Dirigido a: Sector energía EEUU y Europa

Grupo de ciberespionaje,

OB:, espionaje industrial

Ataque: Spear PhisinG, Watering Holes.

2015

BLACKENERGY

Malware destructivo con un componente capaz de apagar sistemas críticos

Dirigido a: Planta energía eléctrica Ucrania
Grupo de ciberespionaje,

OB: sabotaje DoS

VA: correo malicioso

2017

TRITON

Dirigido a: Empresas industriales de Europa del Este

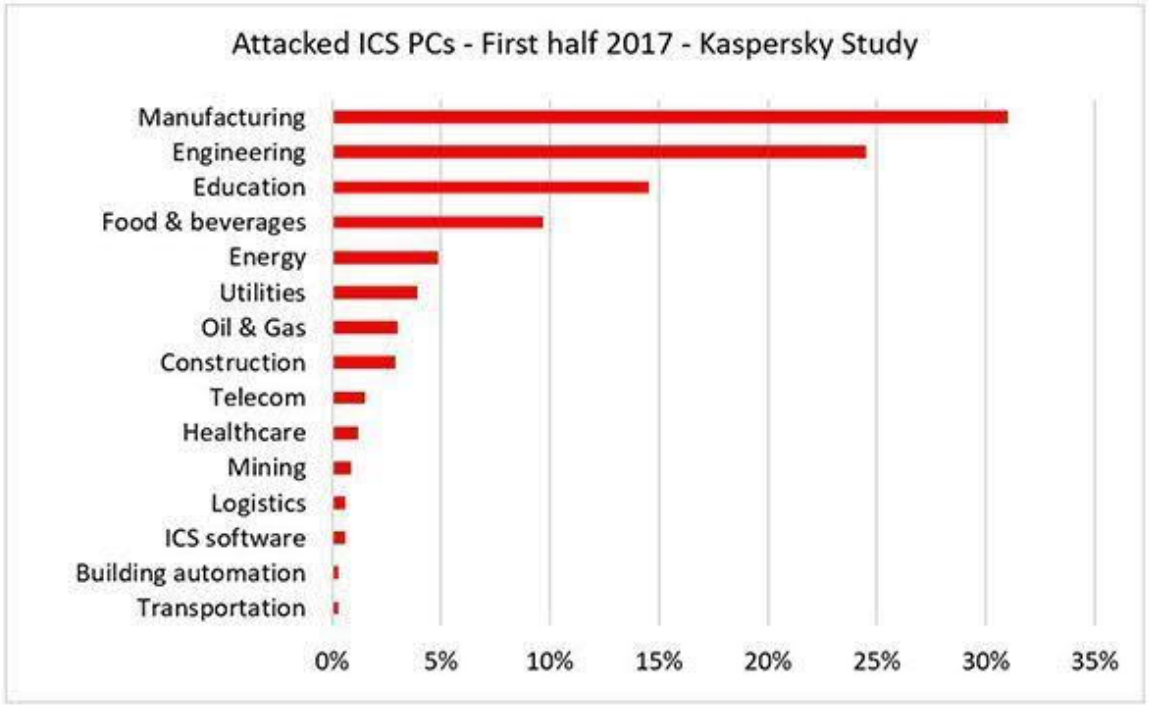
OB: Redes SCADA, cambio de la lógica programada

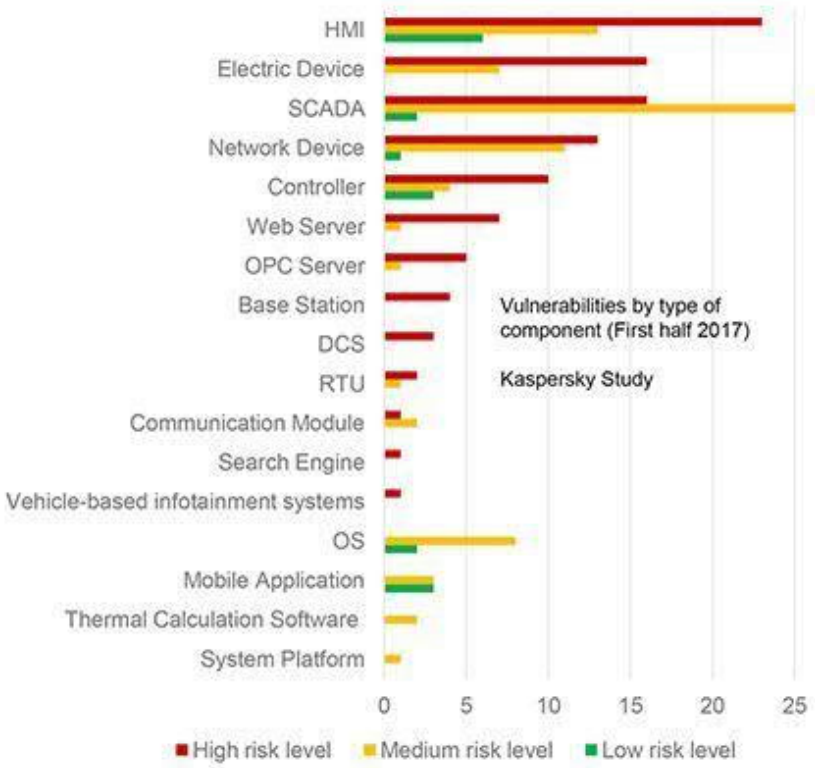
VA: USB

Ataque: Detener la producción y causar daños mayores a la instalaciones físicas..

Terroristmo->muerte

Estadísticas de ciber-ataques a PCs del entorno industrial





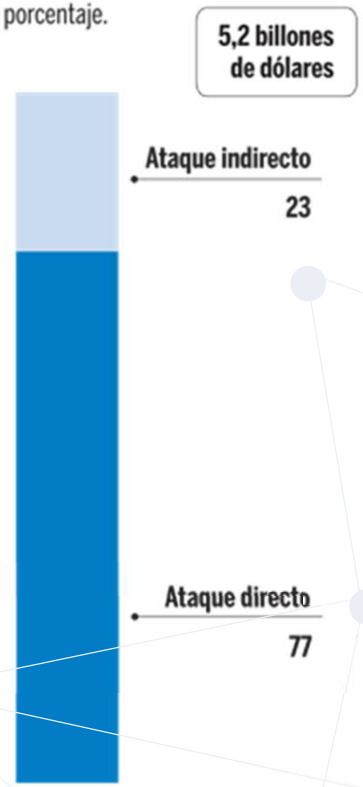
Fuente: Kaspersky

VALORACIÓN DEL RIESGO DE CIBERATAQUES POR INDUSTRIA

En miles de millones de dólares. Entre 2019 y 2023.

> Por tipo de ciberataque

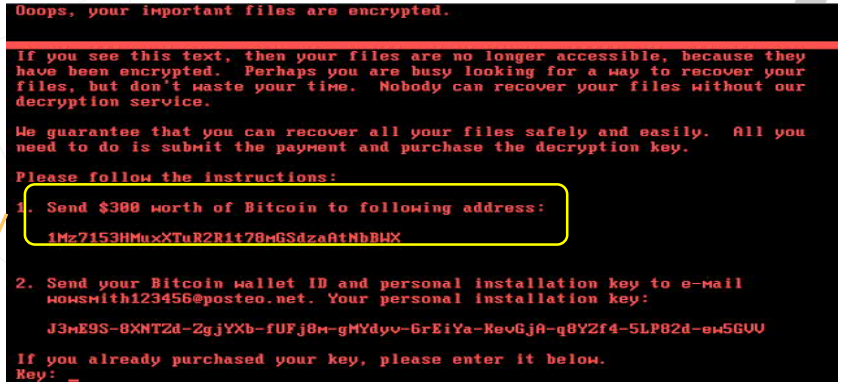
En porcentaje.



Fuente: Accenture

Expansión

Los ataques directos generan grandes ganancias para los atacantes



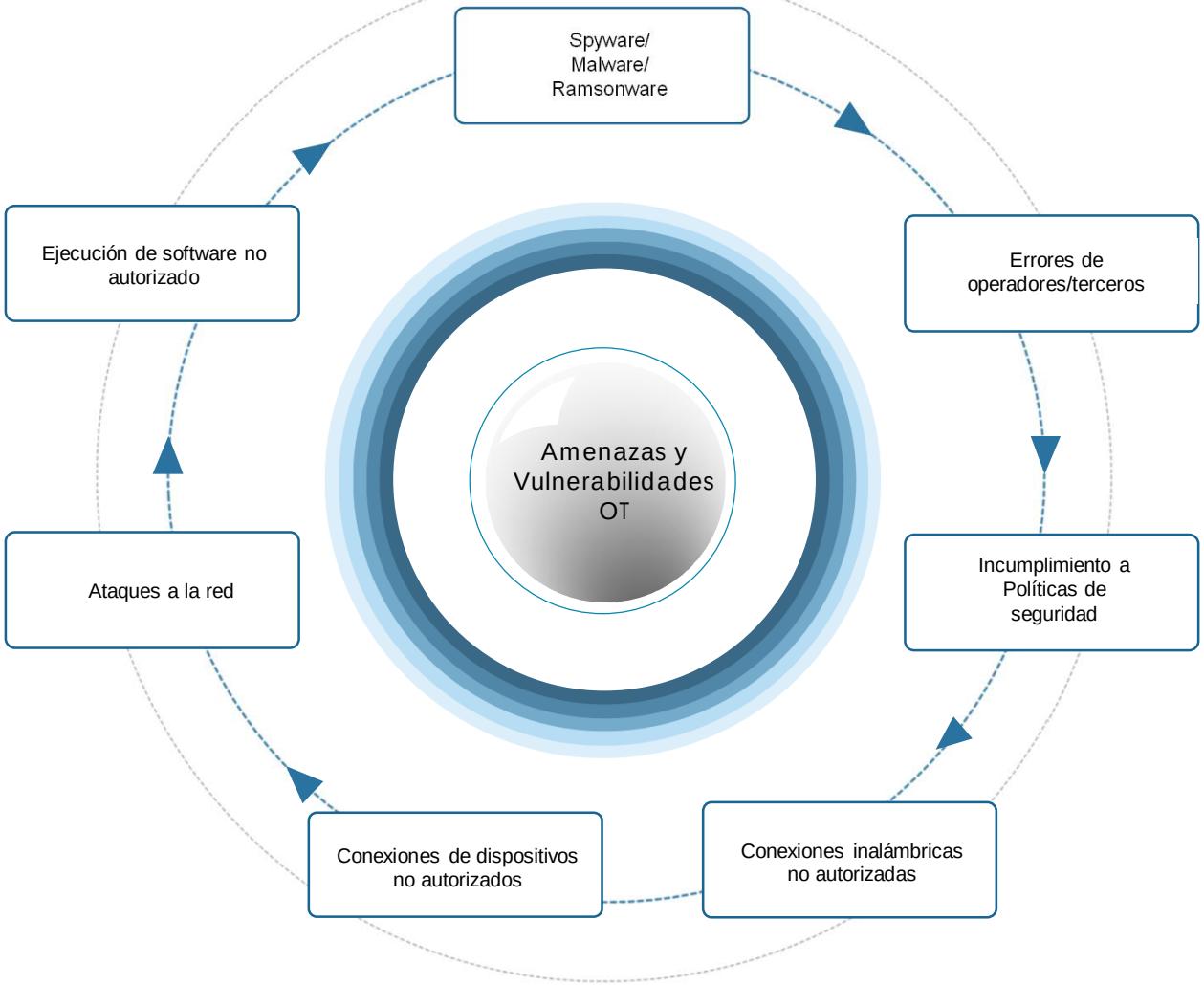
$300 X 317.18 X 365 = $34 M

average ransom | ransoms paid per day | days in a year

Ingreso bruto anual por ramsonware

www.cisco.com/go/asr2016

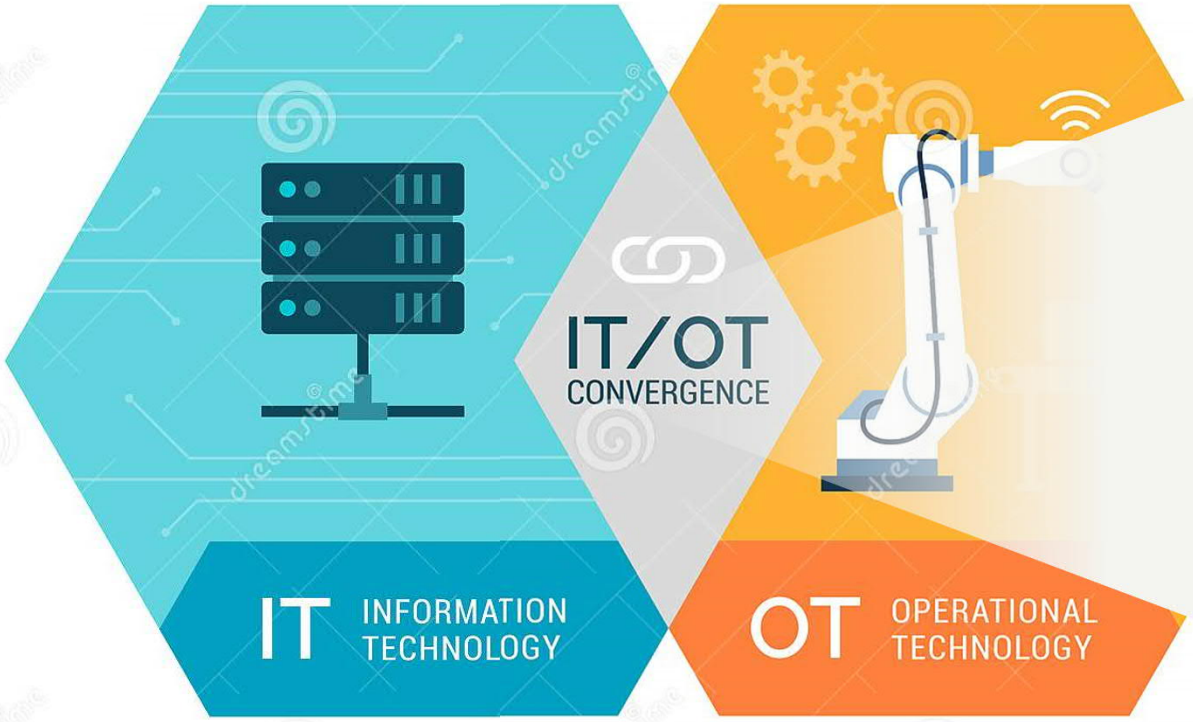
Amenazas y Vulnerabilidades



Las oportunidades de ataque se están expandiendo con rapidez.

R E T O S

Convergencia IT/OT



Fuente: Dreamstime.com

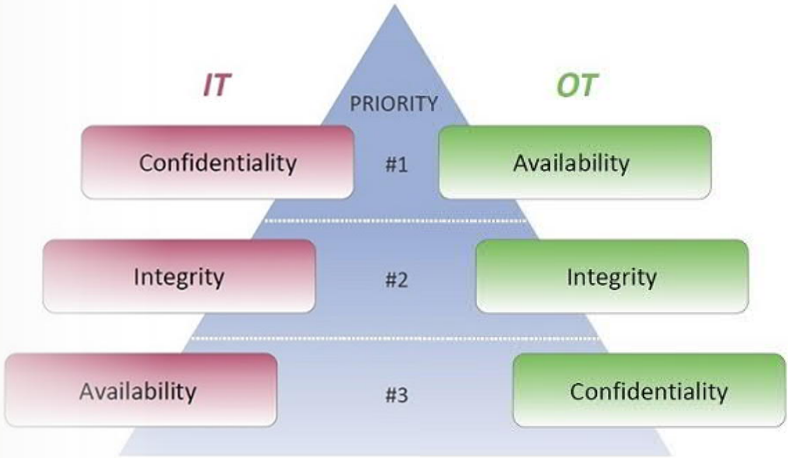
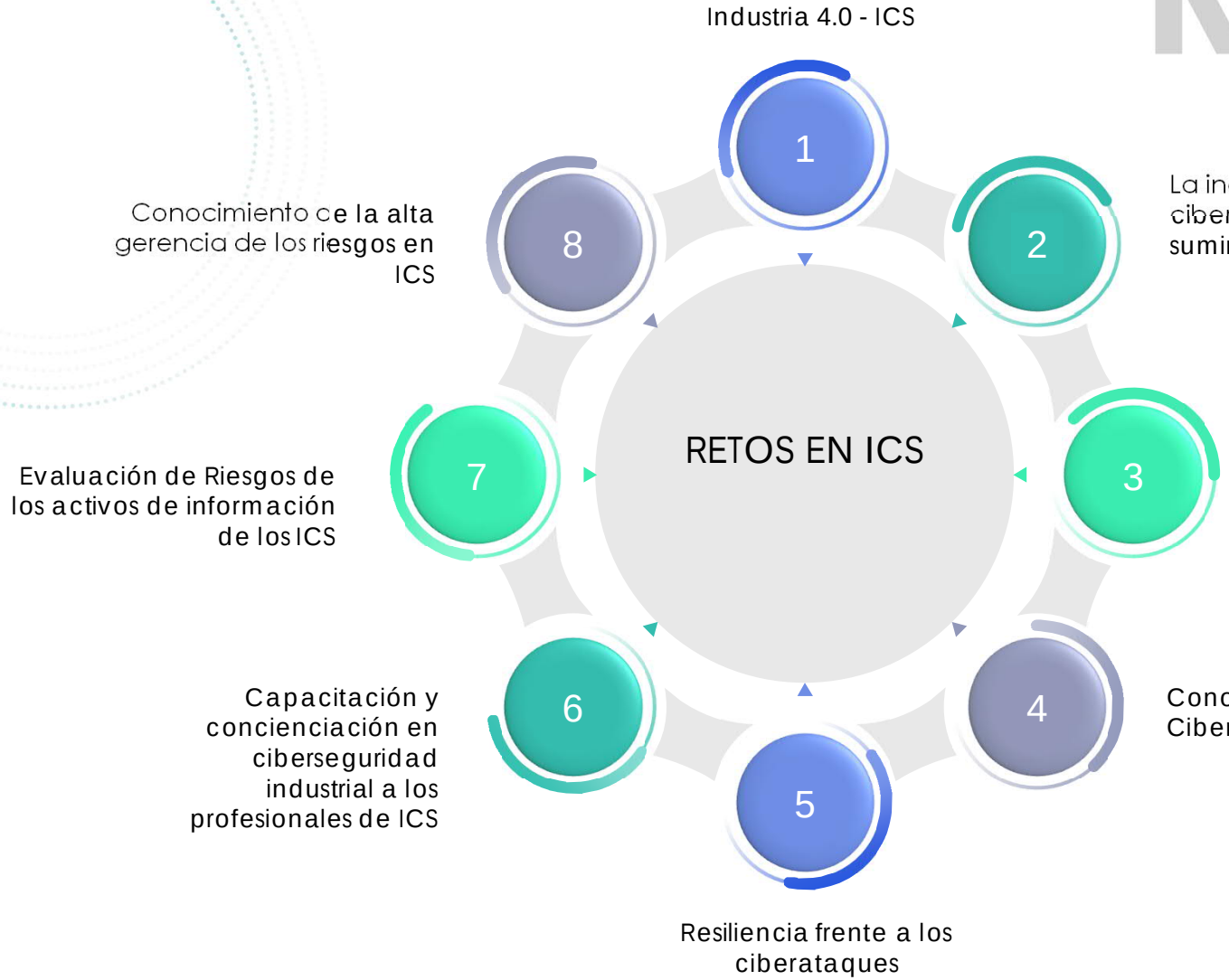


Figure 1. CIA Triad

Retos en ICS


RETOS EN ICS
1
Industria 4.0 - ICS
2
La incorporación de la ciberseguridad en la cadena de suministro.
3
La incorporación de ciberseguridad en las etapas del Ciclo de Vida de un Proyecto de Automatización Industrial
4
Conocer el estado actual de Ciberseguridad en los ICS
5
Resiliencia frente a los ciberataques
6
Capacitación y concienciación en ciberseguridad industrial a los profesionales de ICS
7
Evaluación de Riesgos de los activos de información de los ICS
8
Conocimiento de la alta gerencia de los riesgos en ICS

MEJORES PRÁCTICAS

Content Here

You can simply impress your audience and add a unique zing.

Mejores Prácticas en ICS

Plan Táctico

ARQUITECTURA

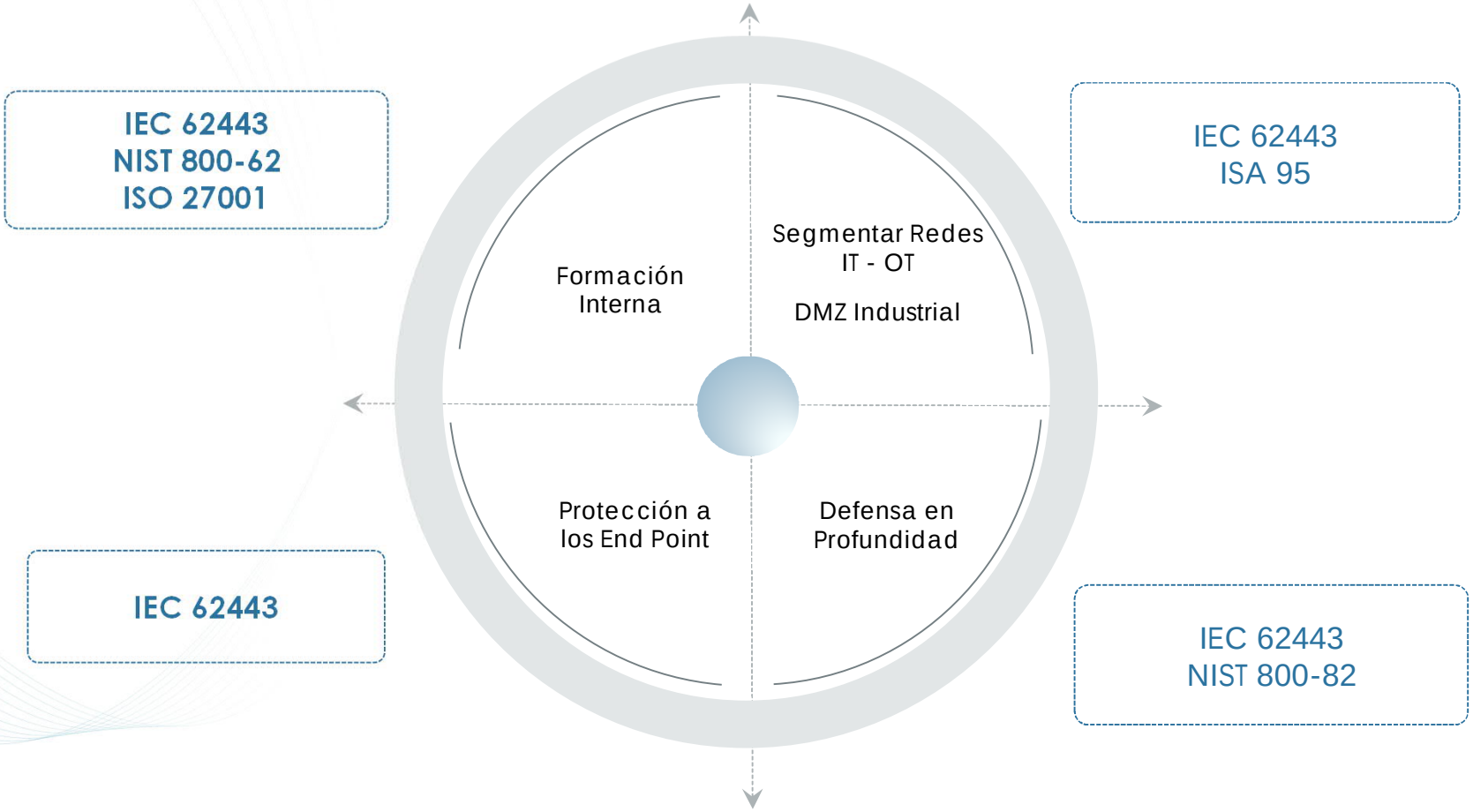
ESTÁNDARES

MECANISMOS

ADMINISTRACIÓN SEGURIDAD

END TO END

Mejores Prácticas en ICS



Segmentación de redes

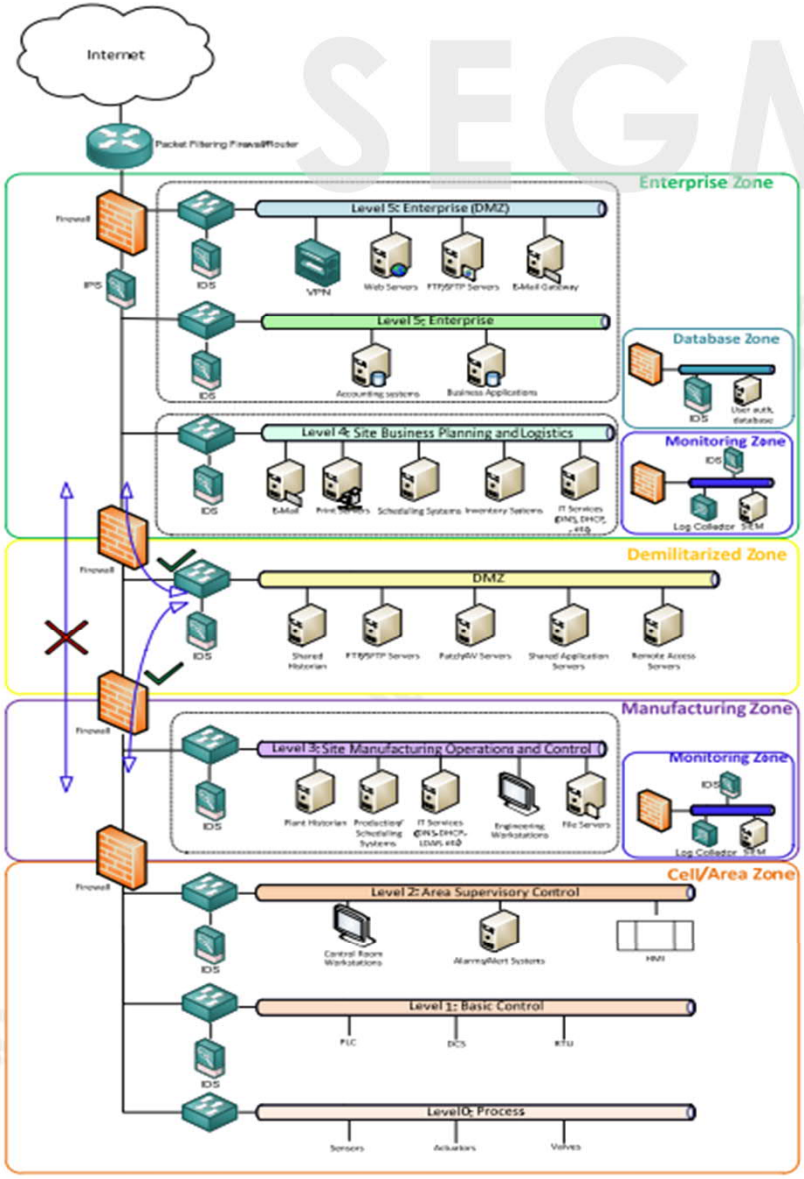


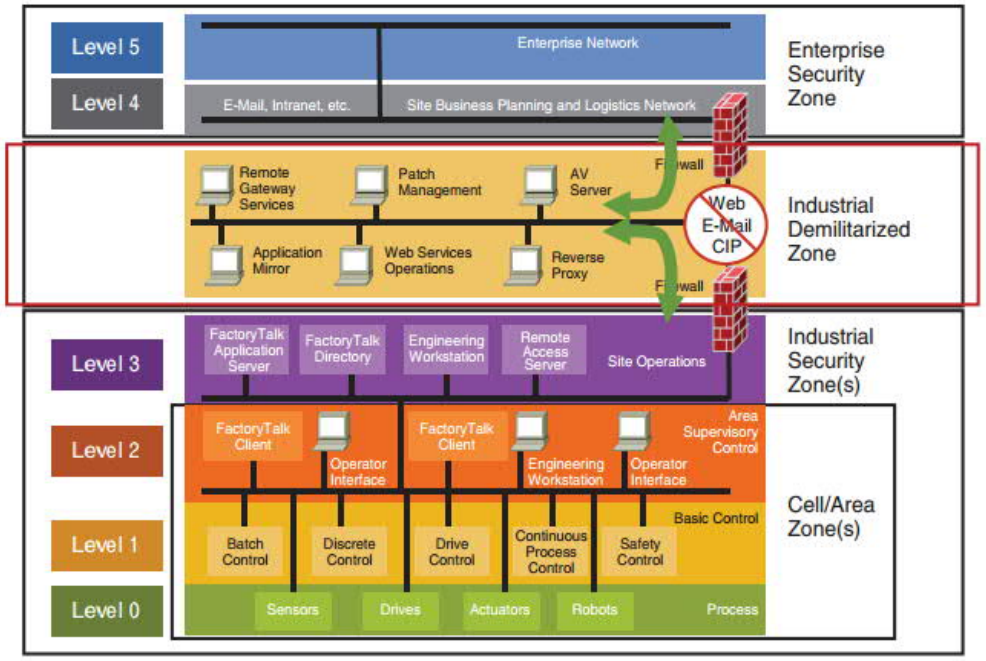
Figure 2 – Modified Purdue Model for Control Hierarchy architecture (NIST special publicat

Por qué segmentar:

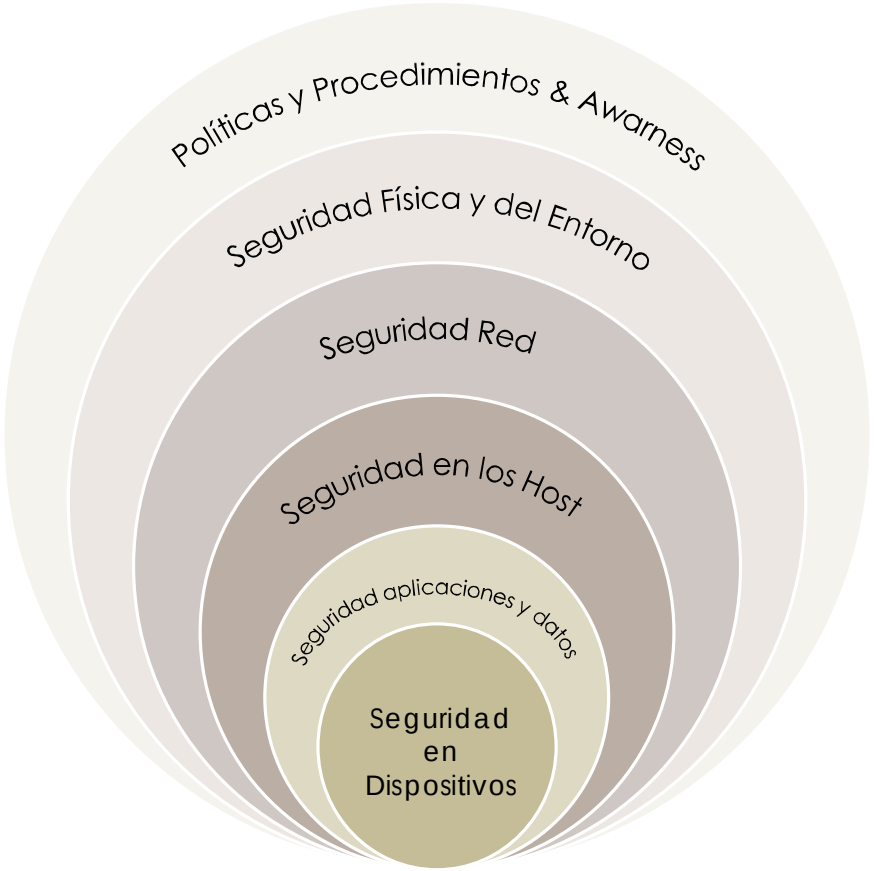
- Reduce los dominios de falla o alcance de un ataque.
- El tratamiento de las redes IT es diferente de OT (CIA / AIC)
- Brindar soporte para acceso remoto.
- Permite integrar ciertas soluciones de IT, que deben acceder a información de OT.
- Analítica de datos, Big data, Data Science: para mantenimiento predictivo.

DMZ Industrial

COMPONENTE PRINCIPAL:
FIREWALL

Define zonas	Inspección de paquetes	IPS/IDS	Gestión de acceso remoto	Mínimo Privilegio
		Active Directory Services	Patch Managment	Terminal Services
		Terminal Services	Network Time Protocol – NTP	Web Proxy Server
		Identitiy Services	SFTP seguro o FTP sobre SSL	File Transfer Server Gateway
		Anti.Virus Server	EDR	Authentication Authorization
		Aplicaciones acceso data	Soluciones para gestionar Servicios OT	Aplicaciones de monitoreo

Defensa en profundidad



IEC 6244-3 / NIST 800 - 82

POLITICAS Y PROCEDIMIENTOS & AWARNESS

Reglas y lineamientos, procedimiento que definan el enfoque de la organización para la protección de las redes industriales, con base en requerimientos de manufactura. Políticas: respaldos, accesos, password, plan de concienciación.

SEGURIDAD FISICA Y DEL ENTORNO

Objetivo: evitar que un posible atacante disponga de acceso físico a los equipos e infraestructuras de red industrial. Limitar el acceso a los data centers de los ICS. Control de ingreso, CCTV, Bloqueo de USB físicamente. Tener cuidado con las llaves de los con troladores y tableros de control.

SEGURIDAD RED

Las medidas en esta capa se centran en el aseguramiento de los accesos remotos a la red. Firewall, iDMZ, Mínimos privilegios. Políticas de password, ACL, NTP, LOGs,, encripción: SSH, HTTPs, SNMP v3, Deshabilitar Servicios innecesarios, device hardening, AAA, Sincronización de Tiempo NTP

SEGURIDAD EN LOS HOST

La seguridad en servidores como clientes, deshabilitado las actualizaciones automáticas manejo de actualizaciones validadas, políticas password, eliminar cuentas de usuarios invitados, respaldos, restringir acceso físico, bloquear USB, antivirus, EDR

SEGURIDAD APLICACIONES Y DATOS

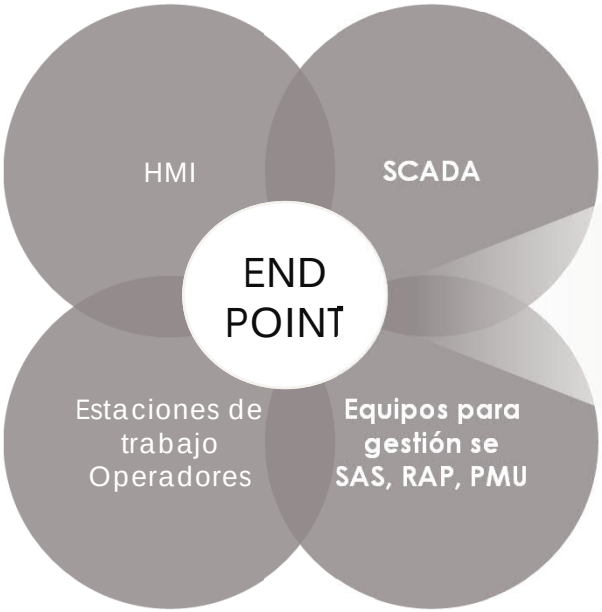
Control de acceso mediante la implantación de mecanismos de autenticación y autorización. Implementar soluciones para administración de red, Contar con una solución de AssetCenter

La autenticación y autorización, así como el cifrado, constituyen las tecnologías más empl eadas para proteger los datos.

SEGURIDAD DISPOSITIVOS

Manejar las recomendaciones de los fabricantes-Firmware, políticas de password, .

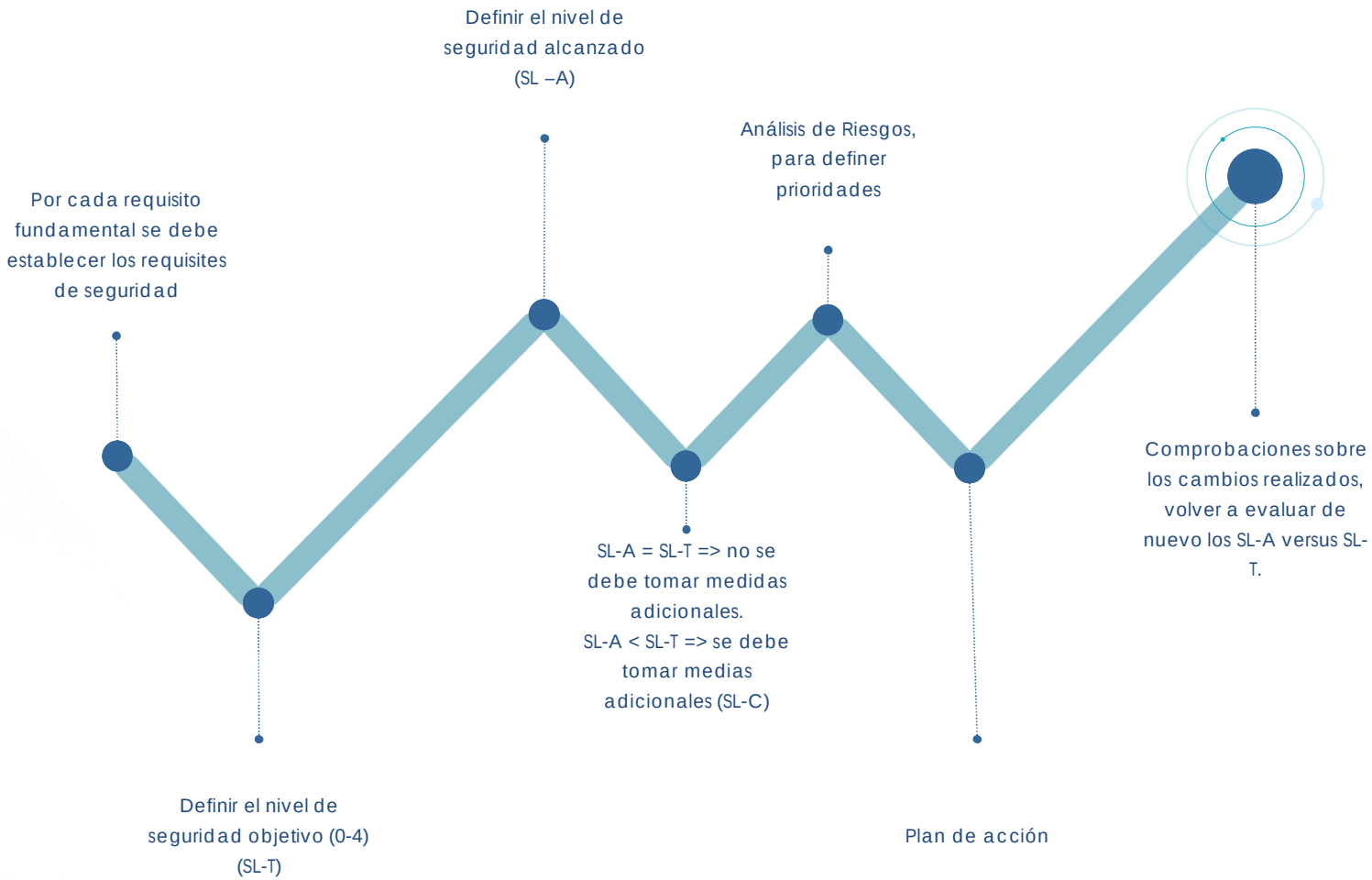
7 requisitos fundamentales de la IEC 62443 para End Points



END POINTs

REQUISITOS DE SEGURIDAD

IEC62443 PARA END POINTs



Aplicación de la IEC 62443 para End Points - ejemplo

SRs y REs	SL-1	SL-2	SL-3	SL-4
FR 3 - INTEGRIDAD DEL SISTEMA (SI)				
SR 3.1 - Integridad en las comunicaciones	✓	✓	✓	✓
RE (1) Usar criptografía para proteger la integridad			✓	✓
SR 3.2 - Protección contra código malicioso	✓	✓	✓	✓
RE (1) Protección contra código malicioso en los puntos de entrada y salida		✓	✓	✓
RE (2) Gestión centralizada para protección contra código malicioso			✓	✓
SR 3.3 - Verificación de funcionalidades de seguridad	✓	✓	✓	✓
RE (1) Mecanismos automáticos para verificar funcionalidades de seguridad			✓	✓
RE (2) Verificaciones de funcionalidades de seguridad durante la operación normal				✓
SR 3.4 - Integridad del software e información		✓	✓	✓
RE (1) Notificaciones automáticas sobre violaciones de integridad			✓	✓
SR 3.5 - Validación de entradas	✓	✓	✓	✓
SR 3.6 - Salidas Determinísticas	✓	✓	✓	✓
SR 3.7 - Manejo de errores		✓	✓	✓
SR 3.8 - Integridad de sesiones		✓	✓	✓
RE (1) Invalidar IDs de sesión una vez que la sesión fue terminada			✓	✓
RE (2) Generación de IDs únicos de sesión			✓	✓
RE (3) Aleatoriedad de IDs de sesión				✓

Fuente: Centro de Ciberseguridad Industrial

FR 3 – INTEGRIDAD DEL SISTEMA (SI)

Requisito de Seguridad: SR 3.2 Protección contra Código Malicioso

Nivel de Seguridad Objetivo: 4

Nivel de Seguridad Alcanzado: 2

Nivel de Seguridad de capacidad:2

Evaluación de Riesgos: Riesgo Crítico

Plan de Acción: Implementación de solución antimalware

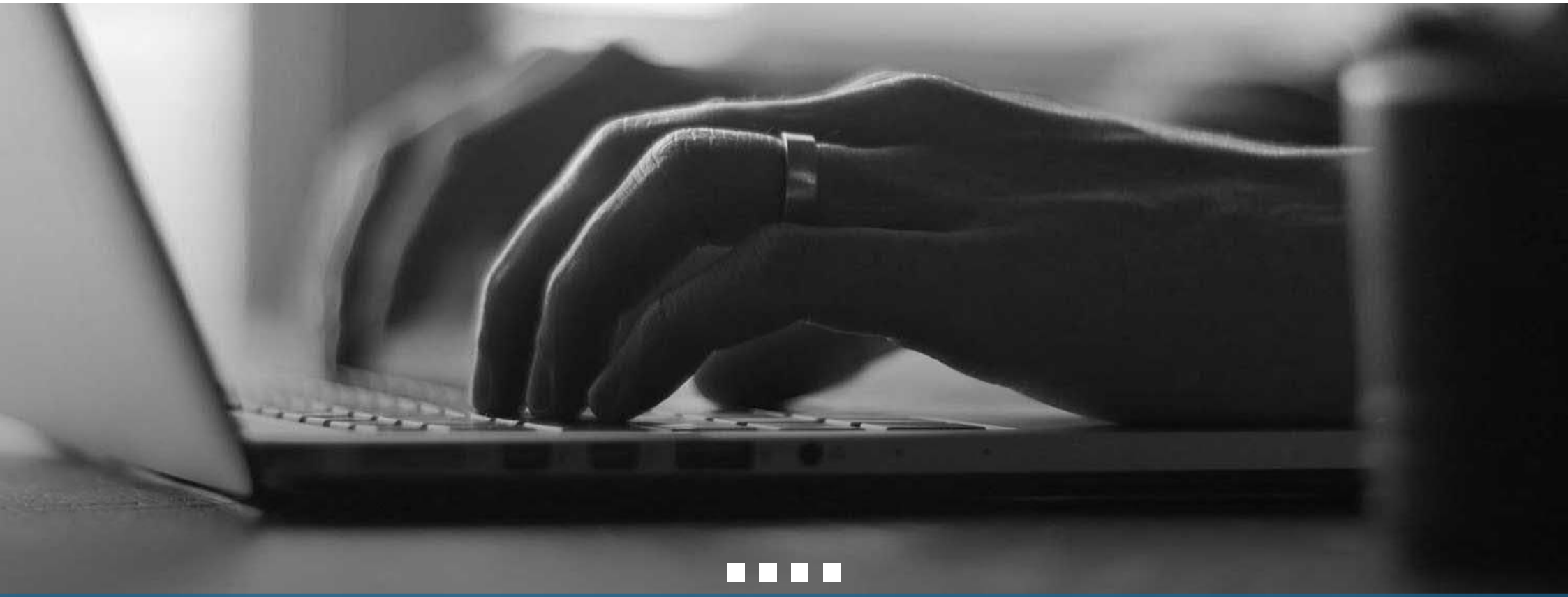
Comprobaciones y reevaluación

Capacidades y Soluciones que apoyan la protección de Endpoints

Formación y conciención personal

Fuente: Centro de Ciberseguridad-CCI

Preguntas y Respuestas



THANK YOU

Ciberseguridad en Manufactura, retos y mejores prácticas

Mary Carmen Vargas

mcvc75@gmail.com

mary-vargas-a187a597