Telefónica Empresas

WEBINAR

Ciber-resiliencia OT.

Desafíos y soluciones de la *transformación digital* de la Industria

Una iniciativa de: Telefónica Tech

En colaboración con: GOUERTIS Part of Telefónica Tech

Índice

01 Introducción y contexto

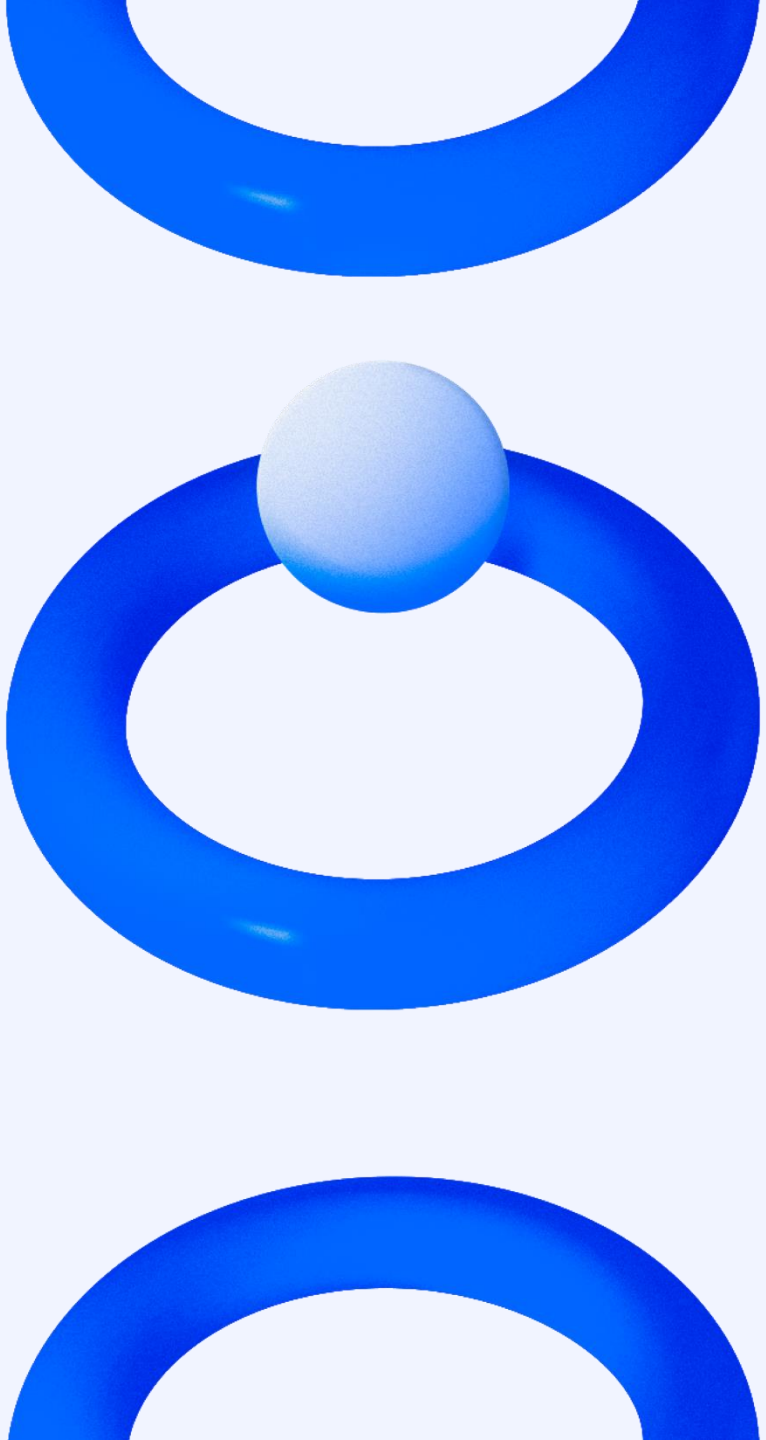
02 Automatización y Transformación Digital de Procesos Industriales

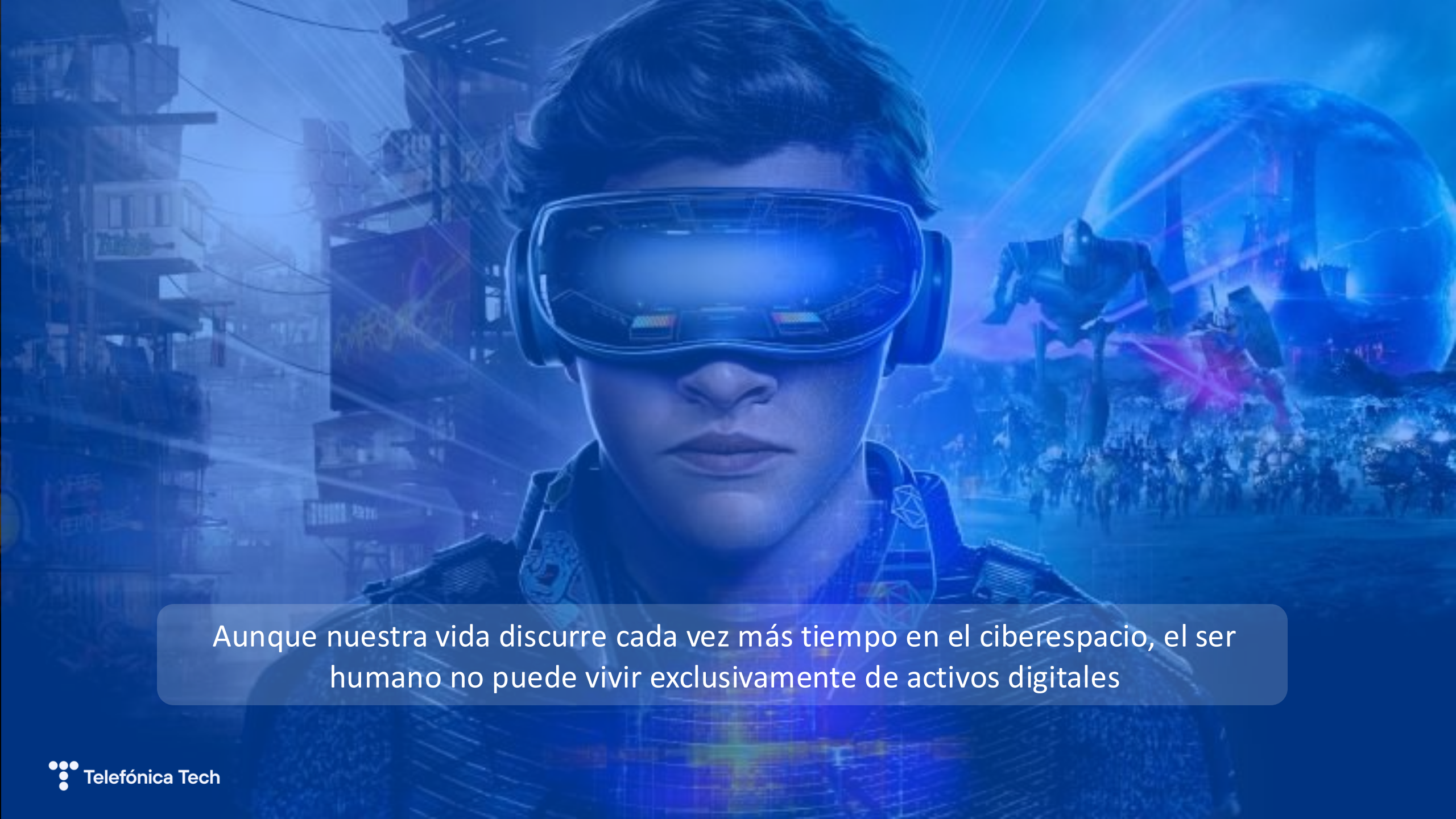
03 Modelo de Gobernanza y Gestión de la ciberseguridad en entornos OT

04 Soluciones de ciberseguridad para la Industria 4.0

05 Q&A

01. Introducción y contexto

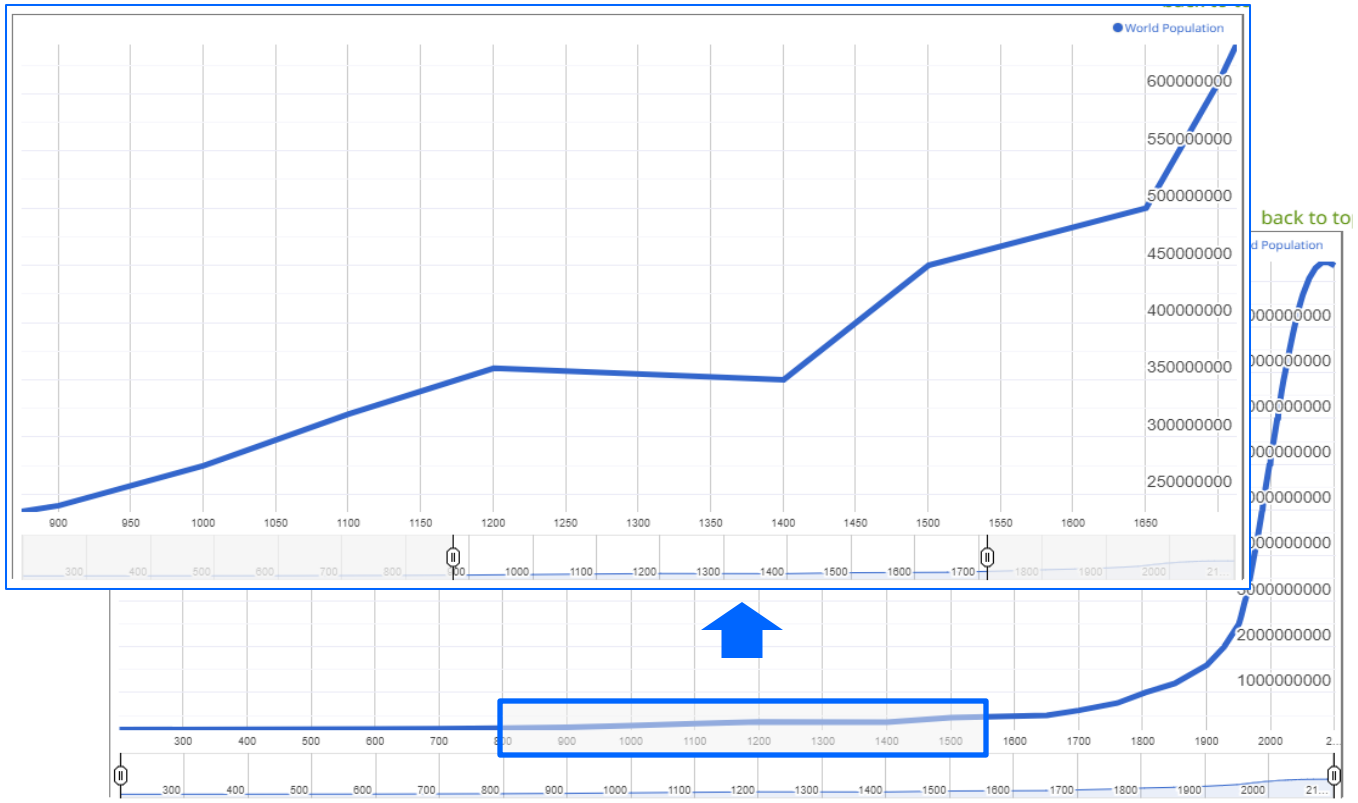




Aunque nuestra vida discurre cada vez más tiempo en el ciberespacio, el ser humano no puede vivir exclusivamente de activos digitales

Contexto Social - Económico

Y los recursos naturales están envueltos en una permanente sensación de escasez ante el imparable crecimiento de la población mundial …

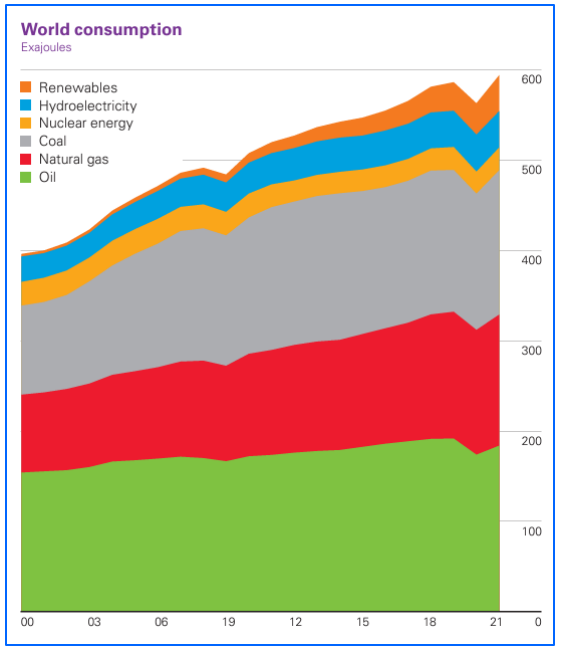


Fuente: https://www.worldometers.info/world-population/

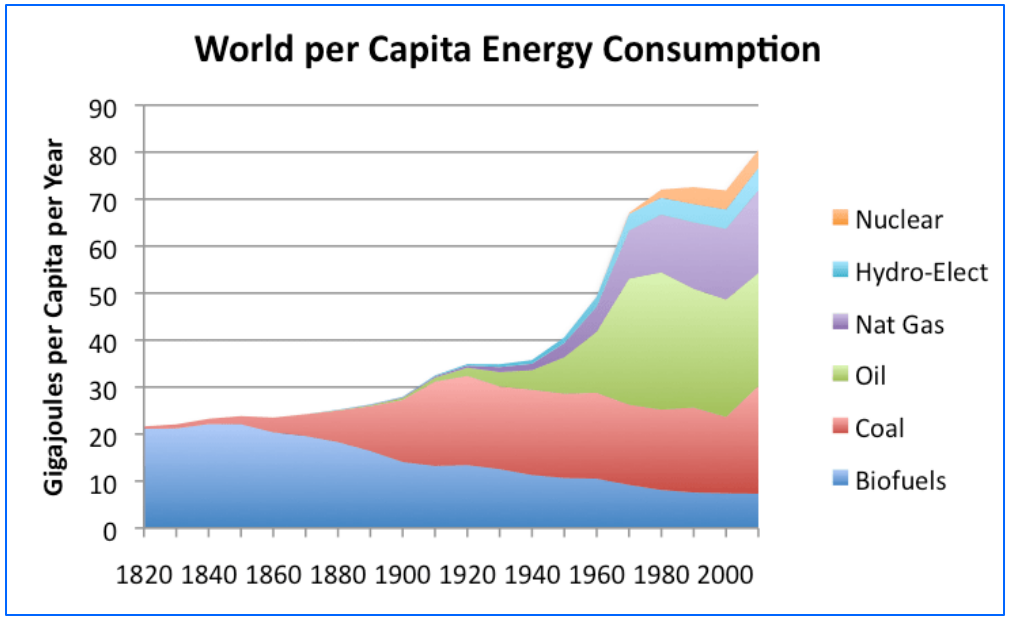
Contexto Social - Económico

debido a que la riqueza y la mejora de las condiciones de vida van inevitablemente ligadas a la disponibilidad de más energía y recursos por habitante (y a menor precio)

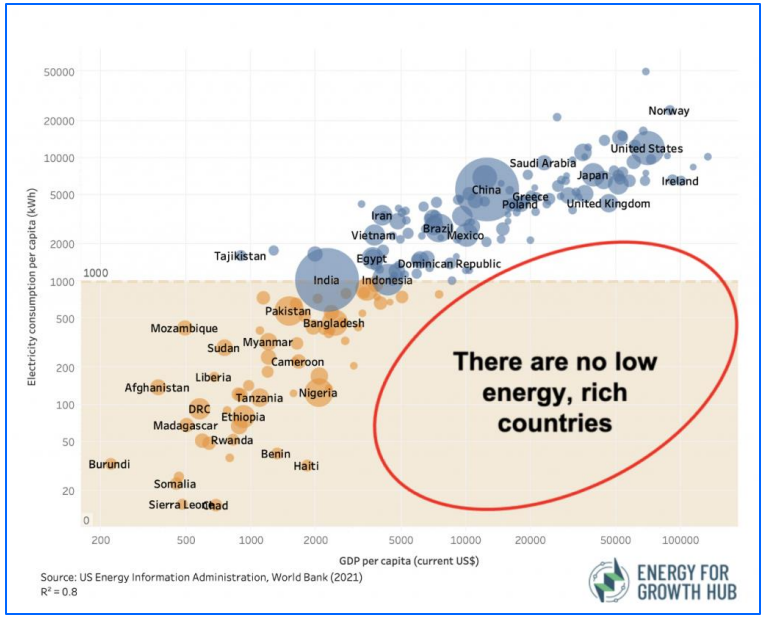
Caso concreto de la energía – auténtica savia del sistema económico



Fuente: BP Statistical Review of World Energy 2022 Edition



Fuente: https://ourfiniteworld.com/2012/03/12/world-energy-consumption-since-1820-in-charts/

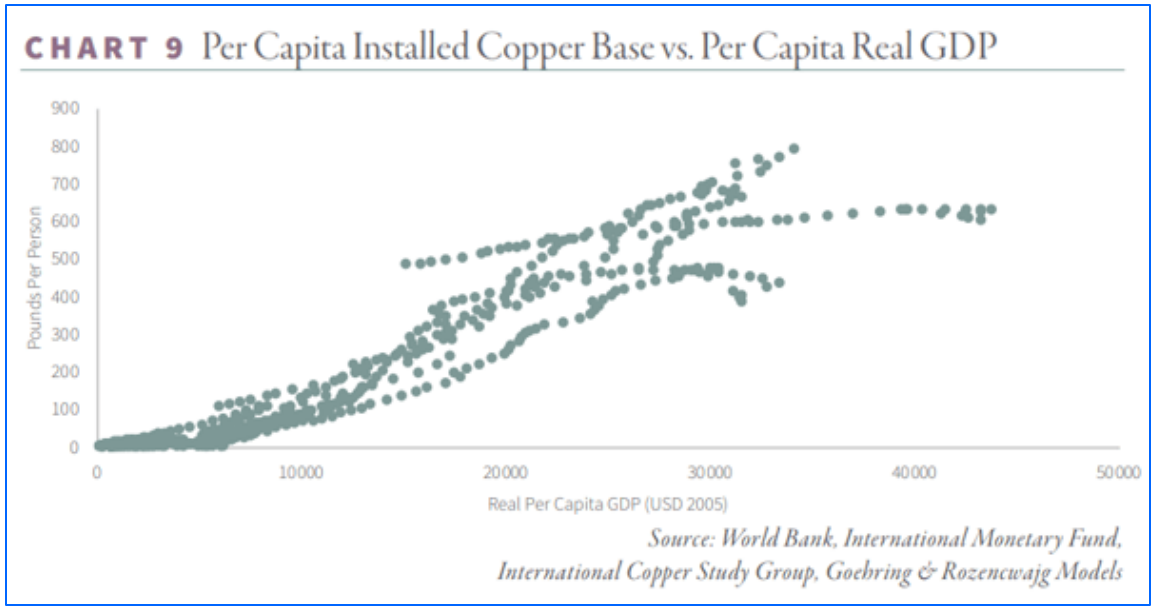


Fuente: https://energyforgrowth.org/article/how-does-energy-impact-economic-growth-an-overview-of-the-evidence/

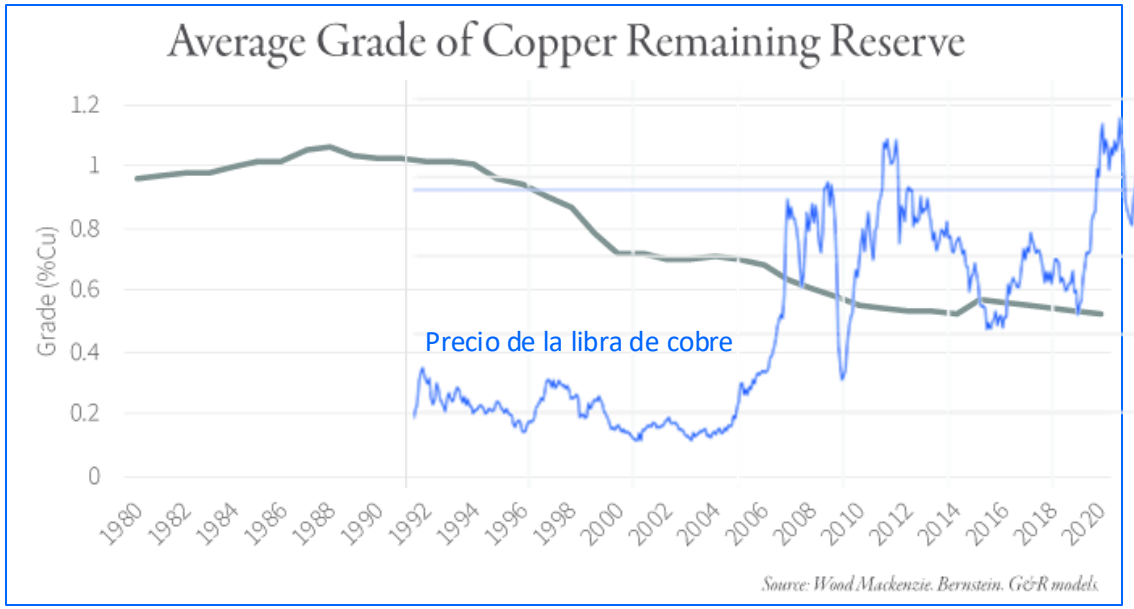
Contexto Social - Económico

debido a que la riqueza y la mejora de las condiciones de vida van inevitablemente ligadas a la disponibilidad de más energía y recursos por habitante (y a menor precio)

Caso concreto del cobre ("Dr Copper") – base de la electrificación de la Sociedad



Fuente: https://blog.gorozen.com/blog/how-the-electrification-of-india-may-impact-copper-prices

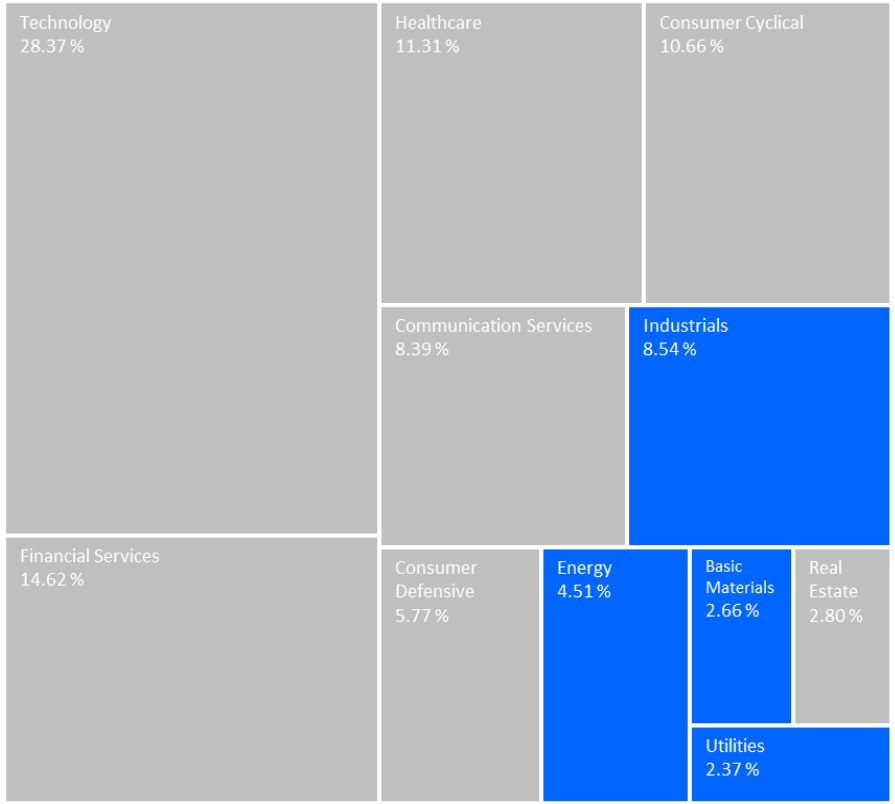


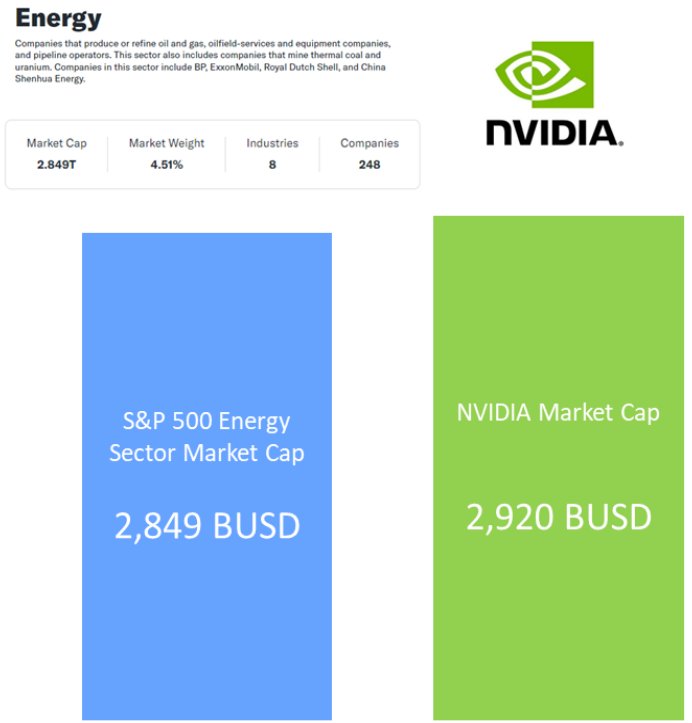
Fuente: https://blog.gorozen.com/blog/copper-depletion-decades-in-the-making

Fuente: https://tradingeconomics.com/commodity/copper

Contexto Social - Económico

Aunque parece que el mercado no está reconociendo la importancia de estos sectores (al menos en base a su apetito inversor) …

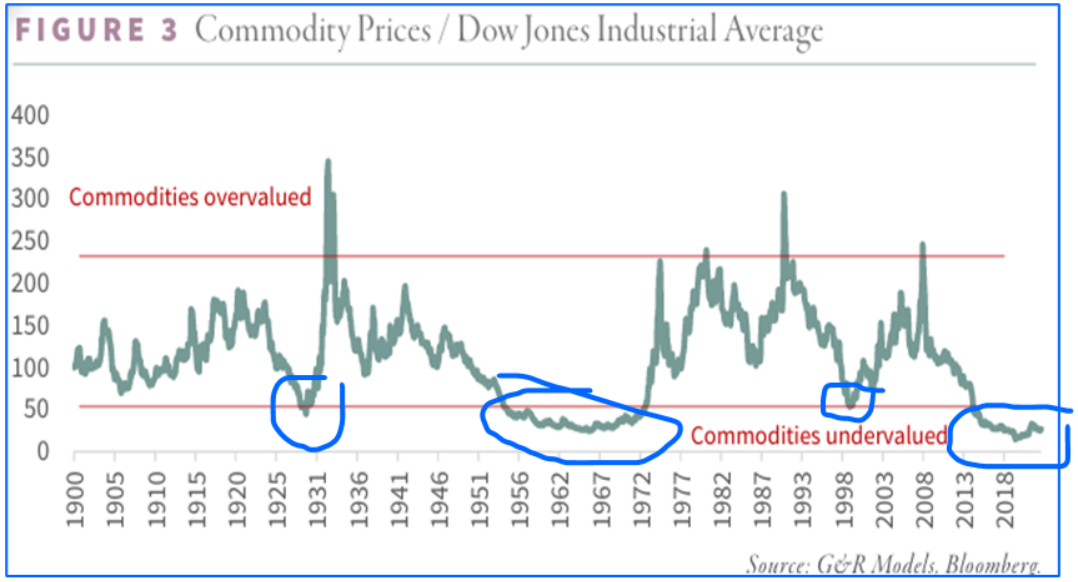




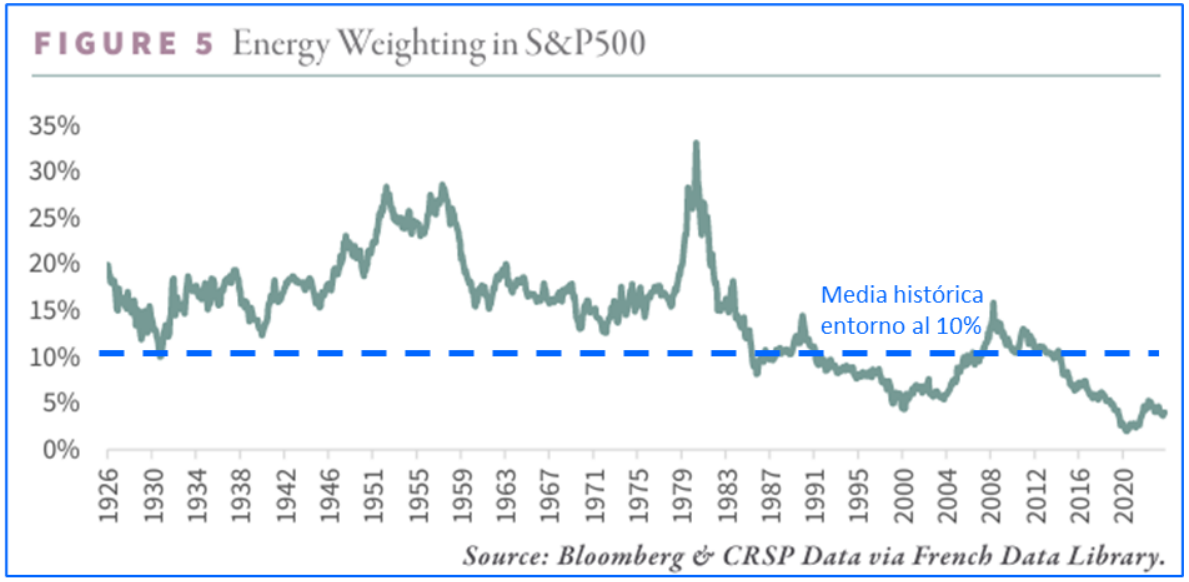
Source: Created by the autor with data from https://finance.yahoo.com/sectors/ - September 13th at Market close

Contexto Social - Económico

y, a pesar de que la inversión en los sectores energéticos y de materias primas es cíclico, parece que hemos llegado a un punto extremo.



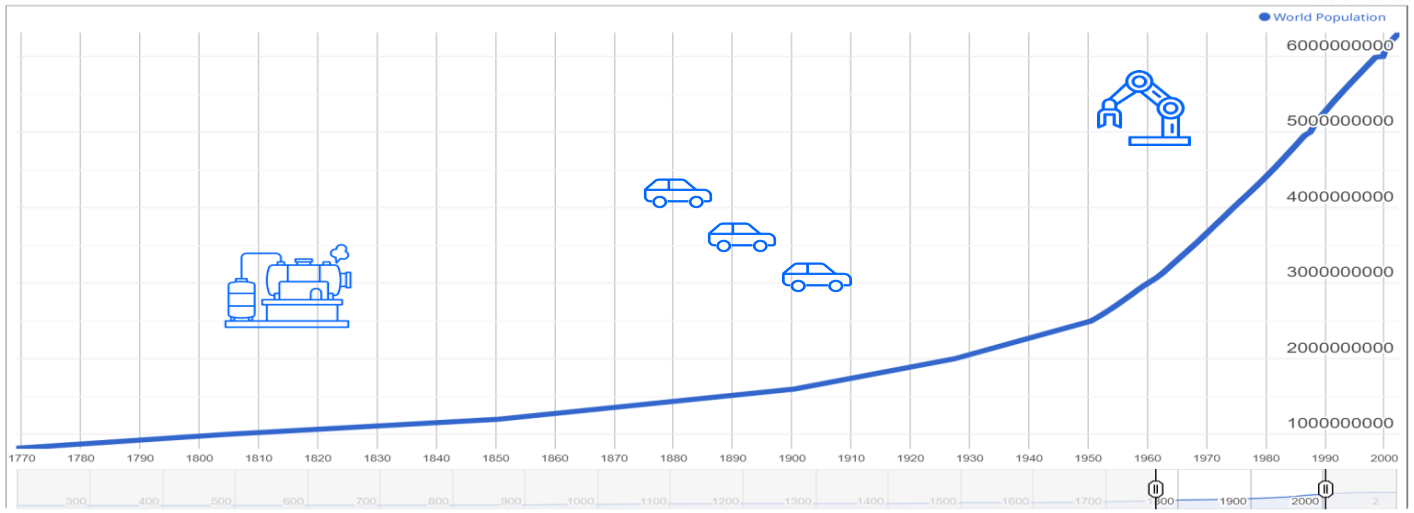
Source: Goehring and Roczenwajg Market Commentary 2023 Q2



Source: Goehring and Roczenwajg Market Commentary 2024 Q1

Contexto Social - Económico

¿Cómo ha conseguido el ser humano sobrevivir y mejorar progresivamente sus condiciones de vida? **Revoluciones Industriales**



1ª Revolución | 2ª Revolución | 3ª Revolución | ...

4ª Revolución Industrial - Sistemas Ciberfísicos

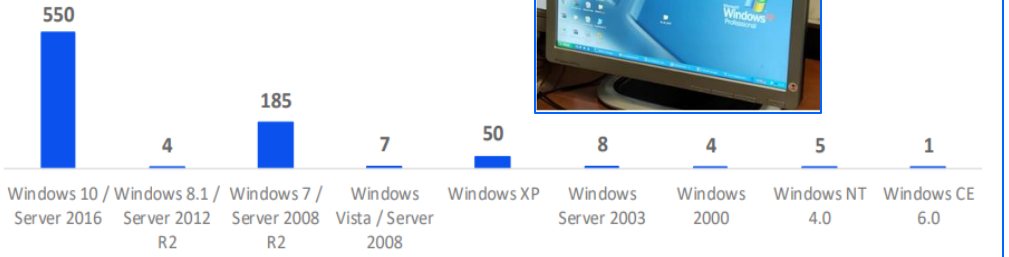
¿Cómo lo vamos a hacer a partir de ahora? Mediante los **sistemas ciberfísicos**

4ª Revolución

Sistemas ciber-físicos: fábricas y entornos inteligentes que toman decisiones de forma autónoma utilizando diferentes tecnologías que se apoyan en la conectividad

4ª Revolución Industrial - Sistemas Ciberfísicos

Pero la realidad de los sistemas ciberfísicos actuales resulta inquietante



Distribución de sistemas detectados en el entorno industrial

Many NHS computers are using outdated Windows software

GETTY IMAGES

HEALTH

Thousands of NHS computers 'still vulnerable to hackers'

Kat Lay, Health Editor

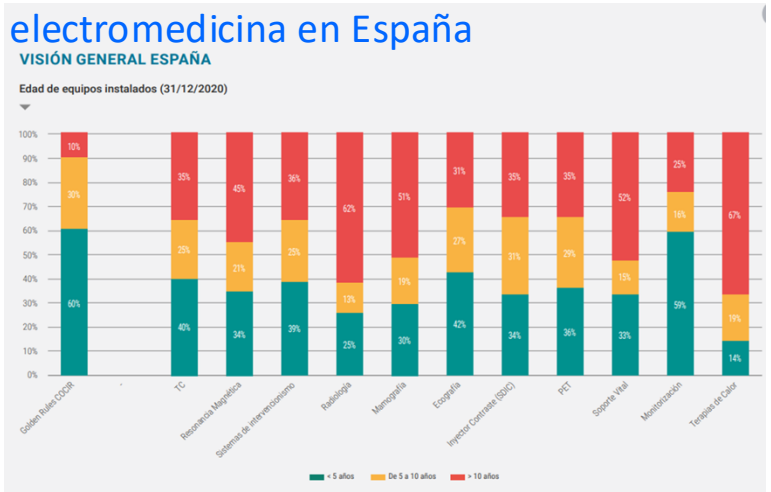
Wednesday August 30 2023, 12.01am BST, The Times

Almost 12,000 NHS computers may be vulnerable to cyberattacks because of outdated operating systems.

The figure, uncovered by the Labour Party in a parliamentary written question, follows a number of incidents in recent months where NHS services have been hit by hackers.

Fuente: https://www.thetimes.co.uk/article/thousands-of-nhs-computers-still-vulnerable-to-hackers-fvs2q90vz#:~:text=Will%20Quince%2C%20a%20health%20minister,hackers%20without%20updates%20being%20installed.

Edad media de los equipos de electromedicina en España



Fuente: https://www.redseguridad.com/especialidades-tic/ot-medica-un-elemento-clave-en-la-ciberseguridad-hospitalaria_20220211.html

4ª Revolución Industrial - Sistemas Ciberfísicos

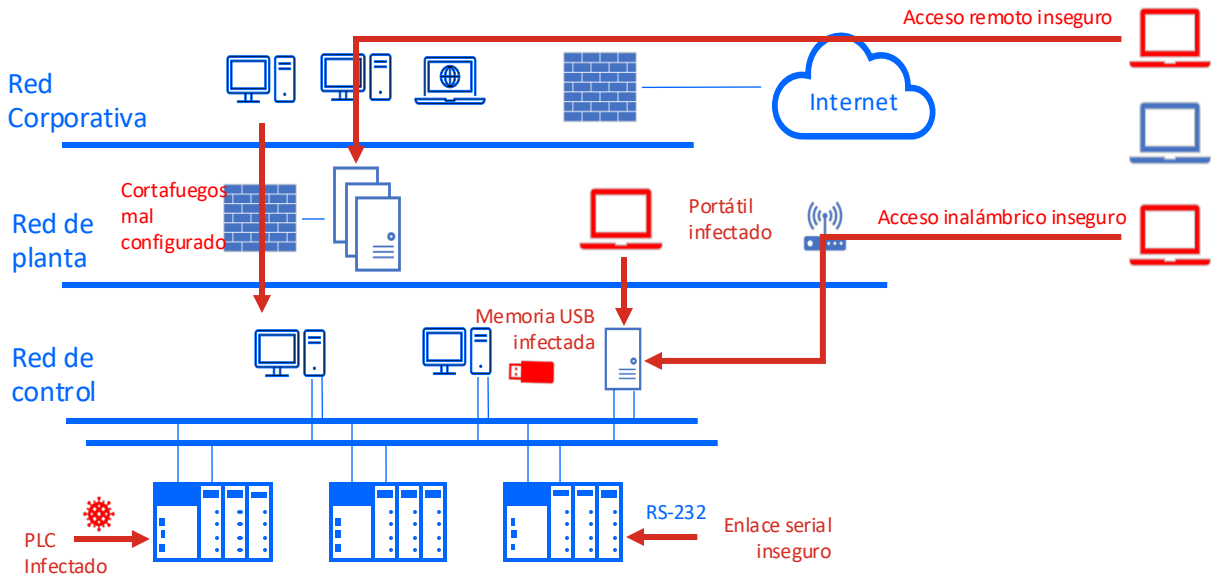
Lo que ha convertido a los **sectores** que más dependen de los **sistemas ciberfísicos** en principal objetivo de los cibercriminales

Share of attacks by industry 2019–2023

Industry	2023	2022	2021	2020	2019
Manufacturing	25.7%	24.8	23.2	17.7	8
Finance and insurance	18.2%	18.9	22.4	23	17
Professional, business and consumer services	15.4%	14.6	12.7	8.7	10
Energy	11.1%	10.7	8.2	11.1	6
Retail and wholesale	10.7%	8.7	7.3	10.2	16
Healthcare	6.3%	5.8	5.1	6.6	3
Government	4.3%	4.8	2.8	7.9	8
Transportation	4.3%	3.9	4	5.1	13
Education	2.8%	7.3	2.8	4	8
Media and telecommunications	1.2%	0.5	2.5	5.7	10

¿Por qué a los criminales les sale a cuenta centrarse en la Industria?

La Realidad de la Planta Industrial.



02. Automatización y Transformación Digital de Procesos Industriales

Revoluciones industriales

Del artesano a la fábrica del dato.

1ª REVOLUCIÓN INDUSTRIAL

Marcada por el paso de la producción artesanal al desarrollo de la maquinaria y la fabricación en mayor escala

2ª REVOLUCIÓN INDUSTRIAL

Marcada por la utilización de la energía eléctrica y la producción masiva en cadenas de montaje.

3ª REVOLUCIÓN INDUSTRIAL

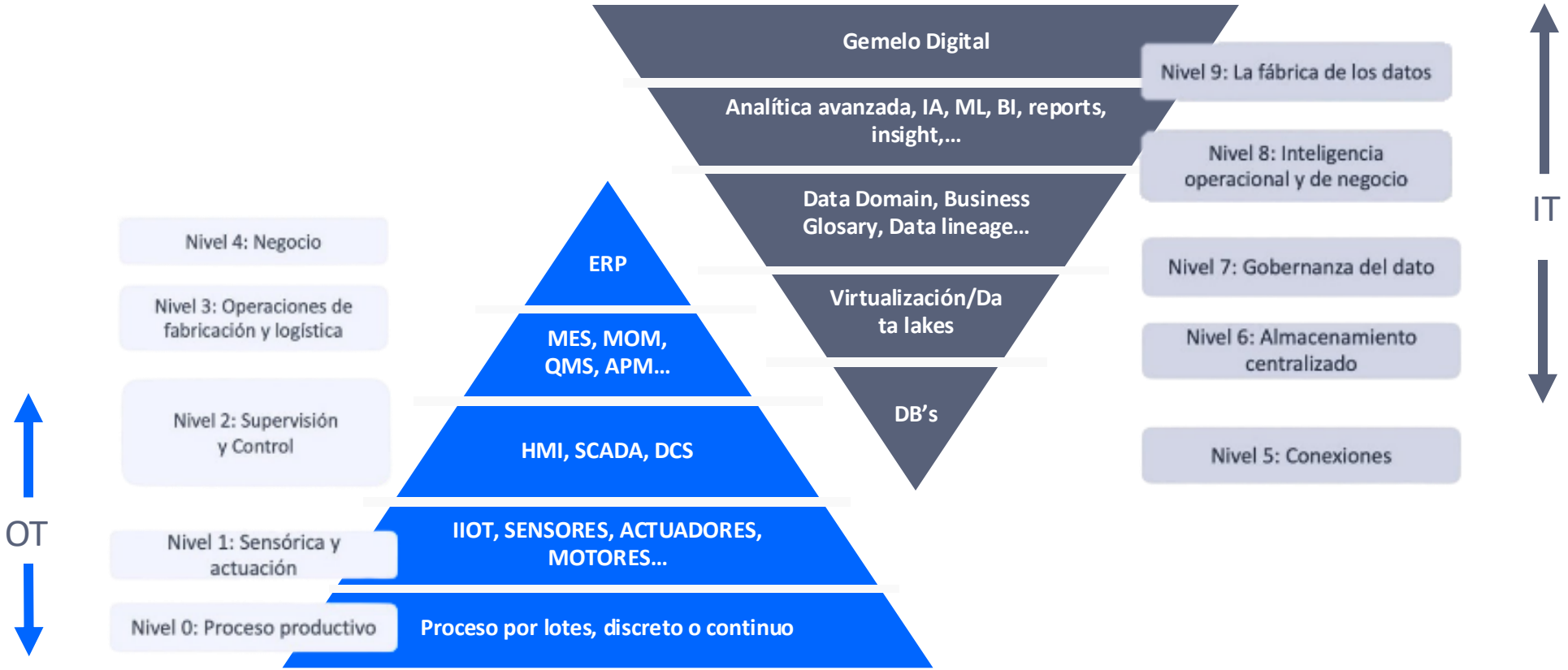
Marcada por la automatización de la fabricación y la informatización de las empresas industriales.

4ª REVOLUCIÓN INDUSTRIAL

Marcada por la conectividad, la captación y explotación de los datos de la planta

IT y OT

Esta visión global en la digitalización de planta, garantiza que se sigan los estándares industriales y se confluya en un **modelo que integre IT y OT** lo más optimizado posible.



Partner Integral

Una **Visión 360º de la Industria 4.0** en fábrica que nos permite abordar todo el proceso productivo de extremo a extremo.

SEGURIDAD
Cyber (IT/OT)
Seguridad física y perimetral

CLOUD COMPUTING
Almacenamiento y Computación Cloud

IOT
Conectividad de dispositivos, RFID, trabajador conectado, etc)

REDES IT/OT
(WIFI, 5G,LAN, etc))

PRODUCTO CONECTADO
(Postventa, inteligencia de cliente, distribución, etc)

BLOCK CHAIN

BIG DATA
(Predictivo, Machine Learning, Machine Visión, Digital Twin, etc)

SISTEMAS ERP

SISTEMAS MOM
(MES, SGA, APS, QMS, GMAO)

SISTEMAS DE CONTROL
(PLC, SCADA)

AUTOMATIZACIÓN
(AGV, Robótica, Sistemas de transporte, etc)

AUTOMATIZACIÓN Y TRANSFORMACIÓN DIGITAL DE PROCESOS INDUSTRIALES

Consultoría para la automatización y transformación digital

Ante proyecto

Diseño y cuantificación de proyectos de automatización industrial, incluyendo planos, listas de materiales, planificación, etc.

Use case Discovery

Detección de casos de uso en planta incluyendo el levantamiento de puntos de mejora en el proceso productivo y fichas de proyecto de aplicación tecnológica para la optimización de estos puntos.

Consultoría de digitalización

Estudio de los procesos de operativos de planta y detección de los puntos de mejora (AS-IS) así como elaboración de una hoja de ruta de transformación digital para abordar todos los puntos detectados (TO-BE).

AUTOMATIZACIÓN Y TRANSFORMACIÓN DIGITAL DE PROCESOS INDUSTRIALES

Automatización

Presentes en toda la cadena de valor

Ingeniería eléctrica

Programación de PLC’s y redes de comunicación

Instalaciones eléctricas

Integramos armarios eléctricos, pupitres de mando, montaje eléctrico y cableado de instalaciones.

Puesta en marcha y optimización

Garantizamos el inicio de la producción, soporte y posterior optimización durante toda la vida útil de los sistemas.

GOVERTIS
Part of Telefónica Tech

AUTOMATIZACIÓN Y TRANSFORMACIÓN DIGITAL DE PROCESOS INDUSTRIALES

Digitalización

Planificación Industrial (APS / MPS / MRP)

Implementación de sistemas de planificación avanzada para la secuenciación de OF's, planificación de demanda y aprovisionamientos, etc.

Gestión de la Producción / Planta (MES / UOC)

Implementación de sistemas de gestión de la producción como gestión de lotes, monitorización de productividades, gestión de la trazabilidad de producto, etc.

Gestión de la Logística (SGA)

Implementación de sistemas de gestión logística como control de inventario, automatización de órdenes de almacenamiento, trazabilidad de ubicaciones, etc.

Gestión del mantenimiento (GMAO / Predictivo)

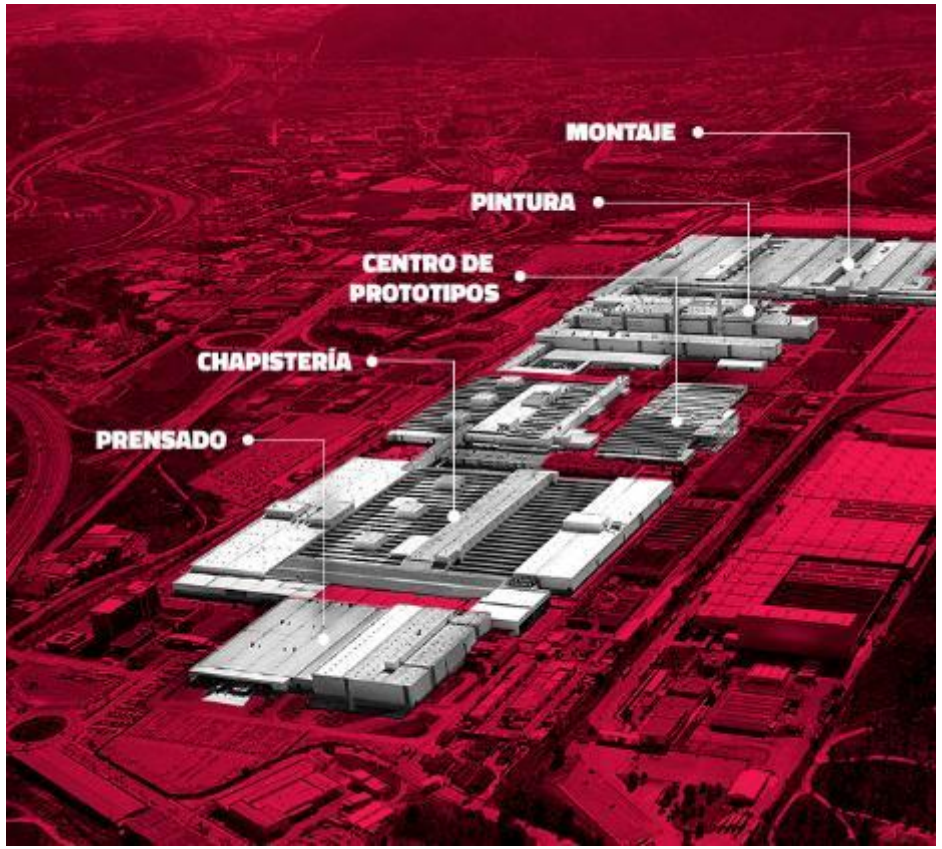
Implementación de sistemas de gestión del mantenimiento como control de calendarios de preventivos, gestión de recambios o predicción de averías.

Gestión de la Calidad (QMS)

Implementación de sistemas de gestión de la calidad como control de las muestras de laboratorio, gestión de SPC's, gestión de no conformidades, etc.

Caso de éxito

Gestión de la producción: Cliente del Sector Automoción



- Conexión directa a más de 1.200 PLC's de las líneas de fabricación
- Conexión con más de 1.500 robots en tiempo real
- Recolección de más de 3 M de registros cada hora
- Monitorización global de las instalaciones
- Imputación de micro-paros (TPM)
- Gestión de objetivos de producción en tiempo real
- Reportes automáticos periódicos con la información necesaria por departamento
- Monitorización de flujos de producción y detección de burbujas

+1,5%
Aumento de la Productividad (7.500 coches)

+25%
Disponibilidad Técnica

TECNOLOGÍAS:

SIEMENS

Germanedge

Caso de éxito

Automatización del montaje: Cliente del Sector Transporte

- Diseño y puesta en marcha de las celdas automáticas de montaje en línea de producción
- Migración y programación de PLC’s de control
- Implementación de SCADA para control de seguridades de toda la nave
- Integración de los AGV’s con el proceso productivo
- Implementación del sistema MES para la ejecución de la producción
- Implementación de un planificador avanzado para la secuenciación de OF’s y control de materiales y fechas de entrega

-70%
Reducción de errores humanos

Reducción del tiempo de fabricación

Mejora de la eficiencia de planta

TECNOLOGÍAS:

SIEMENS Objective From Aptean

Caso de éxito

Digital: Cliente del Sector Metalúrgico

- Captación de todos los datos de proceso procedentes de las diferentes fuentes de planta.
- Creación de un Dashboard unificado que permita visualizar qué está ocurriendo en tiempo real y tomar las decisiones adecuadas.
- Diseño de un gemelo digital basado en los datos de planta donde el usuario puede simular la producción a un mes vista y realizar modificaciones ficticias para ver cómo estas afectan a la producción total del mes.

Reducción de las replanificaciones De producción

Aumento de Productividad global

TECNOLOGÍAS:

Germanedge

Objective
From Aptean

Caso de éxito

Trazabilidad de producto: Cliente del Sector Metalúrgico

- Digitalización de todos los movimientos de material en planta mediante tablets.
- Creación de un motor logístico que orquesta las tareas de ubicación y crea tareas automáticamente a los operarios de almacén y de producción.
- Conocimiento en tiempo real de dónde están todas las referencias en fábrica, quién las ha movido, cuándo, para qué orden de fabricación. Etc.
- Eliminación del criterio del operario para la ubicación de materiales.
- Coordinación con carretillas auto-tripuladas para los movimientos recurrentes.

-30%
Tiempo muerto de búsqueda

+100%
Trazabilidad de +producto

TECNOLOGÍAS:

Objective
From Aplean

Caso de éxito

Predicción de la Demanda: Cliente del Sector Alimentario

- Predicción de la demanda mediante analítica del dato a corto, medio y largo plazo (5 años).
- Simulación de escenarios de demanda vs escenarios productivos.
- Optimización del margen de negocio con la modificación de precios frente a los escenarios de demanda.
- Optimización de las líneas de producción basadas en una estimación más certera de la demanda.
- Reducción de segundas calidades y stock de producto.

80%
Índice de acierto de predicción

P/D%
Margen global Negocio

TECNOLOGÍAS:

Germanedge

03. Modelo de Gobernanza y Gestión de la ciberseguridad en entornos OT

Principios de Gobernanza en Seguridad OT

El Gobierno de la Seguridad OT asegura una alineación estratégica entre las operaciones industriales, la continuidad de negocio y la seguridad.

Modelo de Gobierno de la Seguridad OT

Principios de Gobernanza en Seguridad OT

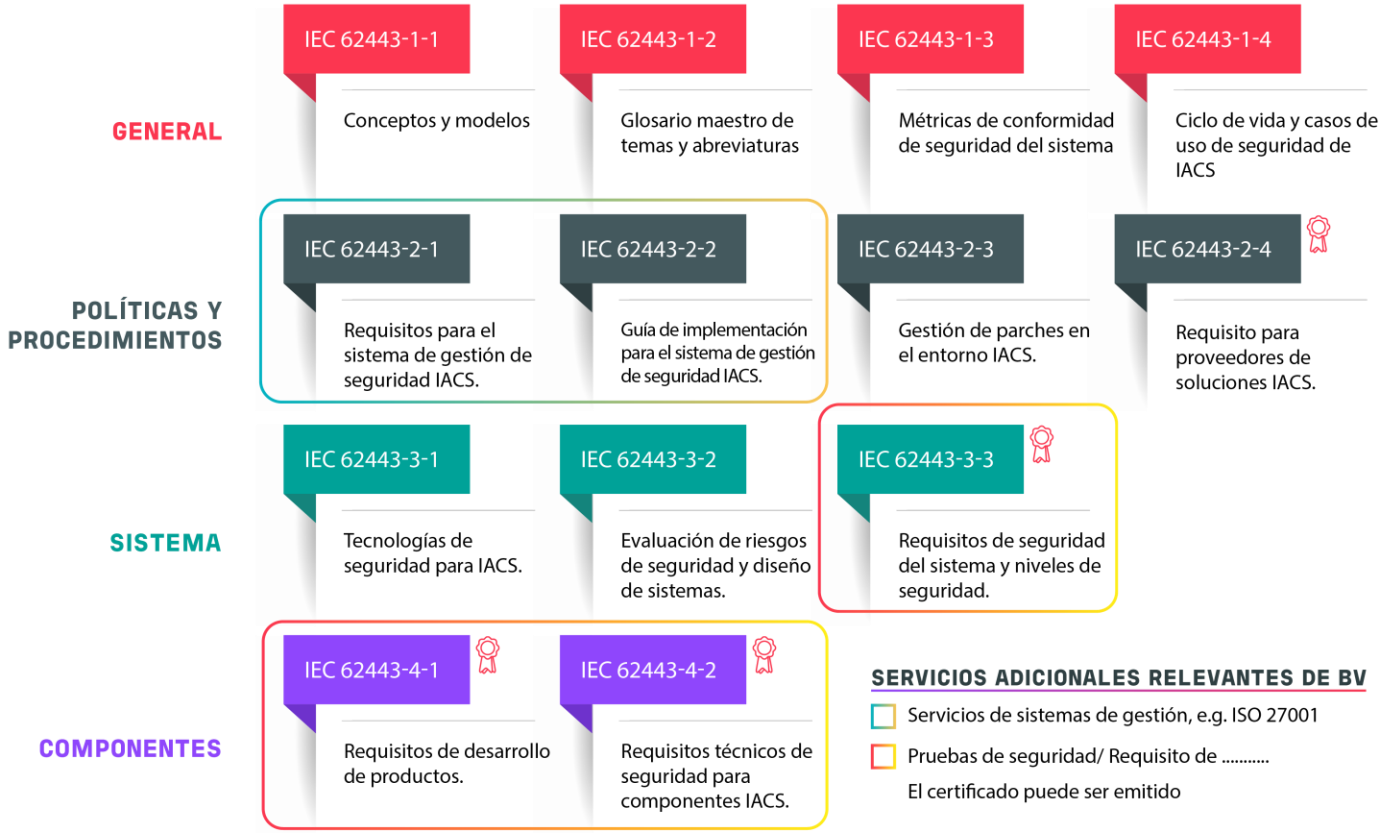
El Gobierno de la Seguridad OT asegura una alineación estratégica entre las operaciones industriales, la continuidad de negocio y la seguridad.

Modelo de Gobierno de la Seguridad OT

Estándares y normativas clave

Los estándares proporcionan un marco de referencia para gestión y el gobierno de la seguridad industrial

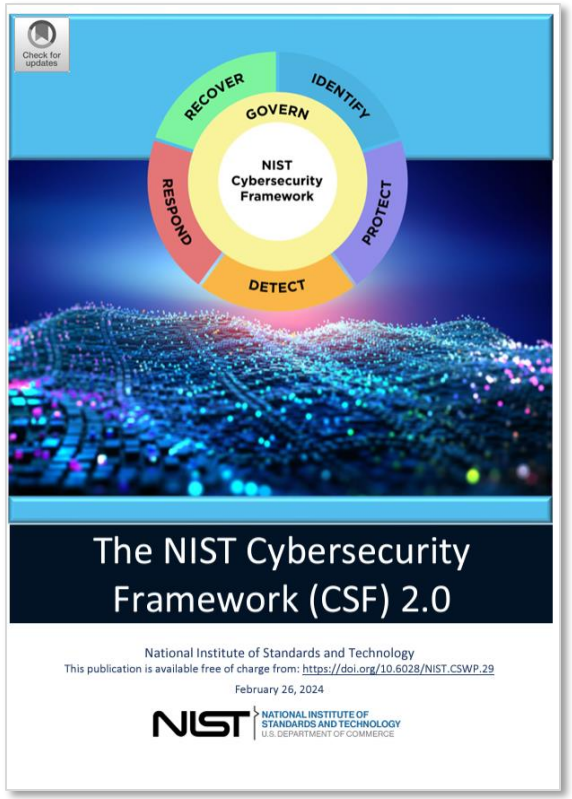
ISA/IEC 62443



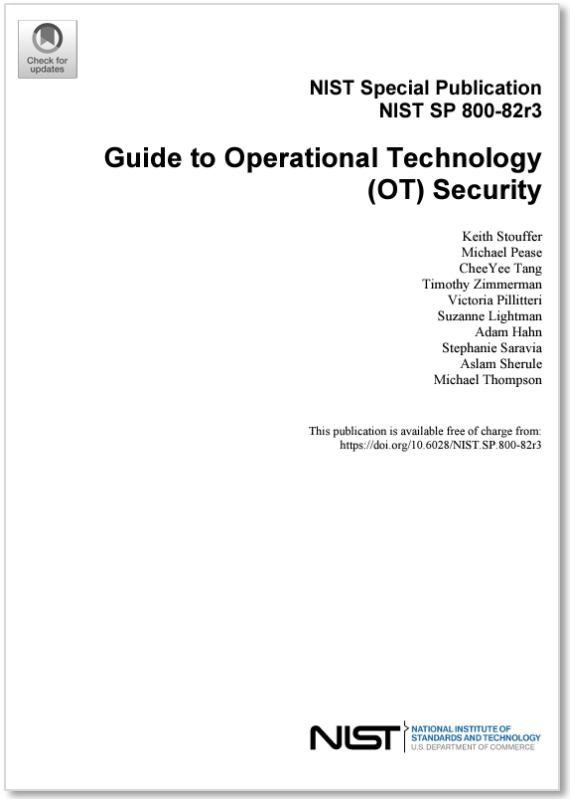
Estándares y normativas clave

Los estándares proporcionan un marco de referencia para gestión y el gobierno de la seguridad industrial

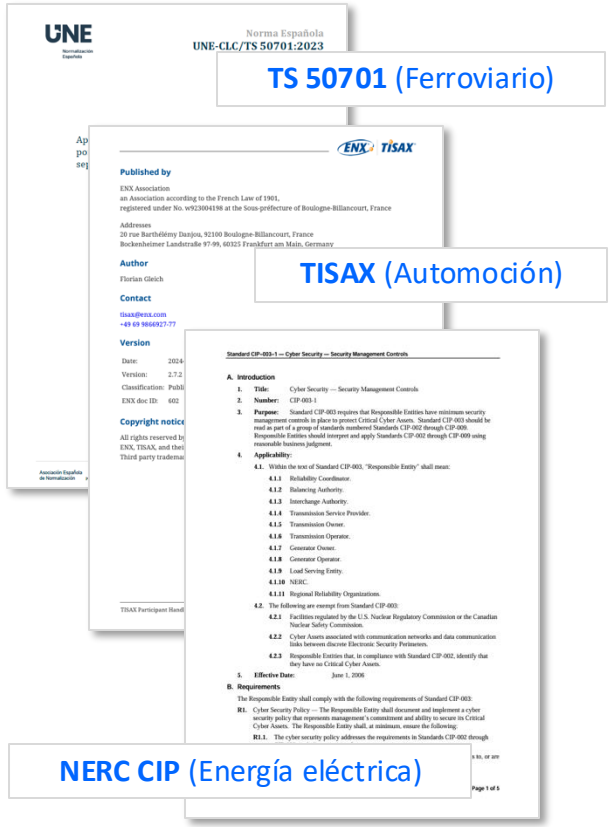
ISA/IEC 62443



NIST CSF 2.0



NIST SP 800-82r3



Regulación y cumplimiento normativo

La regulación nacional e internacional establece obligaciones en materia de seguridad en sistemas OT

- Protección de Infraestructuras Críticas
- Directiva europea NIS2

Sectores de alta criticidad:

- Energía
- Transporte
- Banca
- Infraestructura de los mercados financieros
- Sector Sanitario
- Agua potable
- Aguas residuales
- Infraestructura digital
- Gestión de servicios de TIC (B2B)
- Entidades de la Administración pública
- Espacio

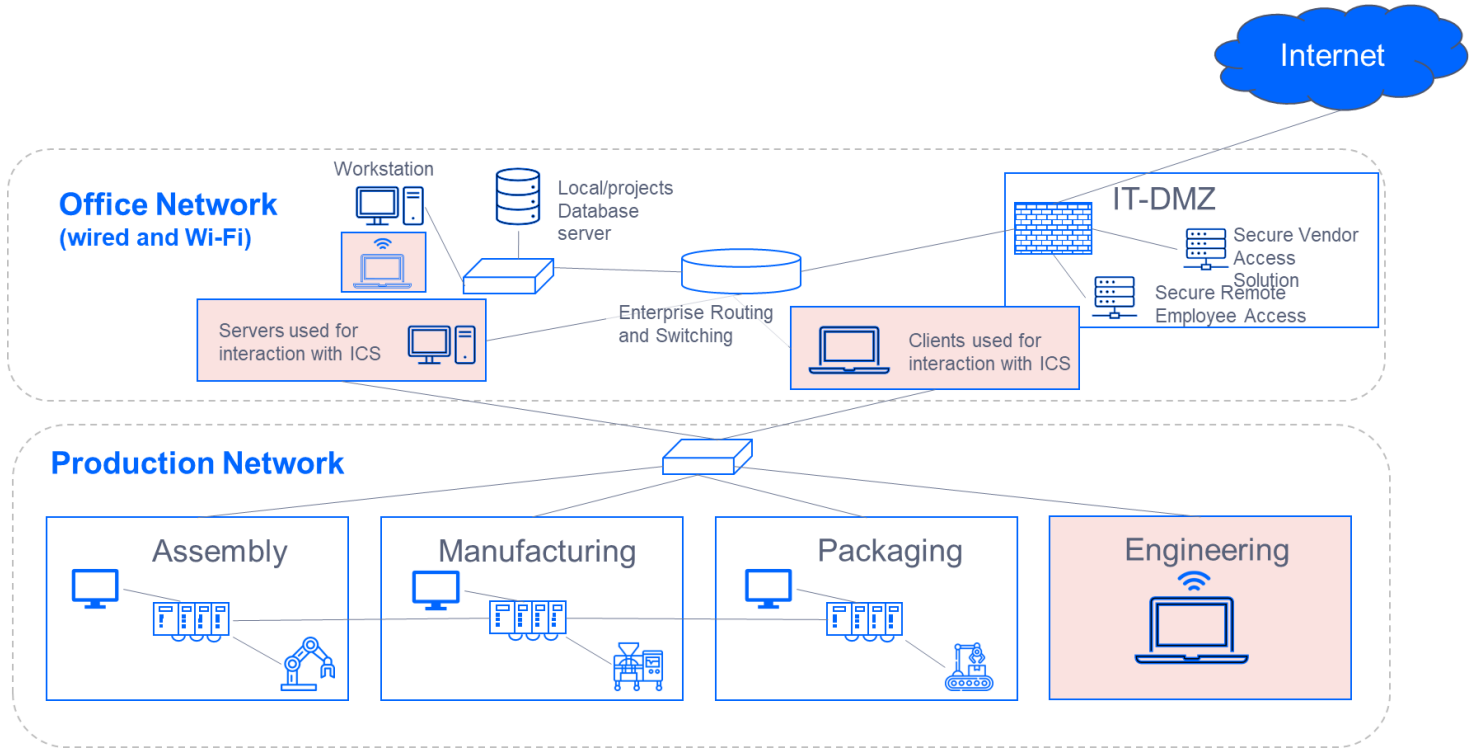
Otros sectores críticos:

- Servicios postales y de mensajería
- Gestión de residuos
- Fabricación, producción y distribución de sustancias y mezclas químicas
- Producción, transformación y distribución de alimentos
- Fabricación (productos sanitarios; productos informáticos, electrónicos y ópticos; material eléctrico; maquinaria…)
- Proveedores de servicios digitales
- Investigación

Evaluación y gestión de riesgos en sistemas industriales

Proceso de evaluación de riesgos

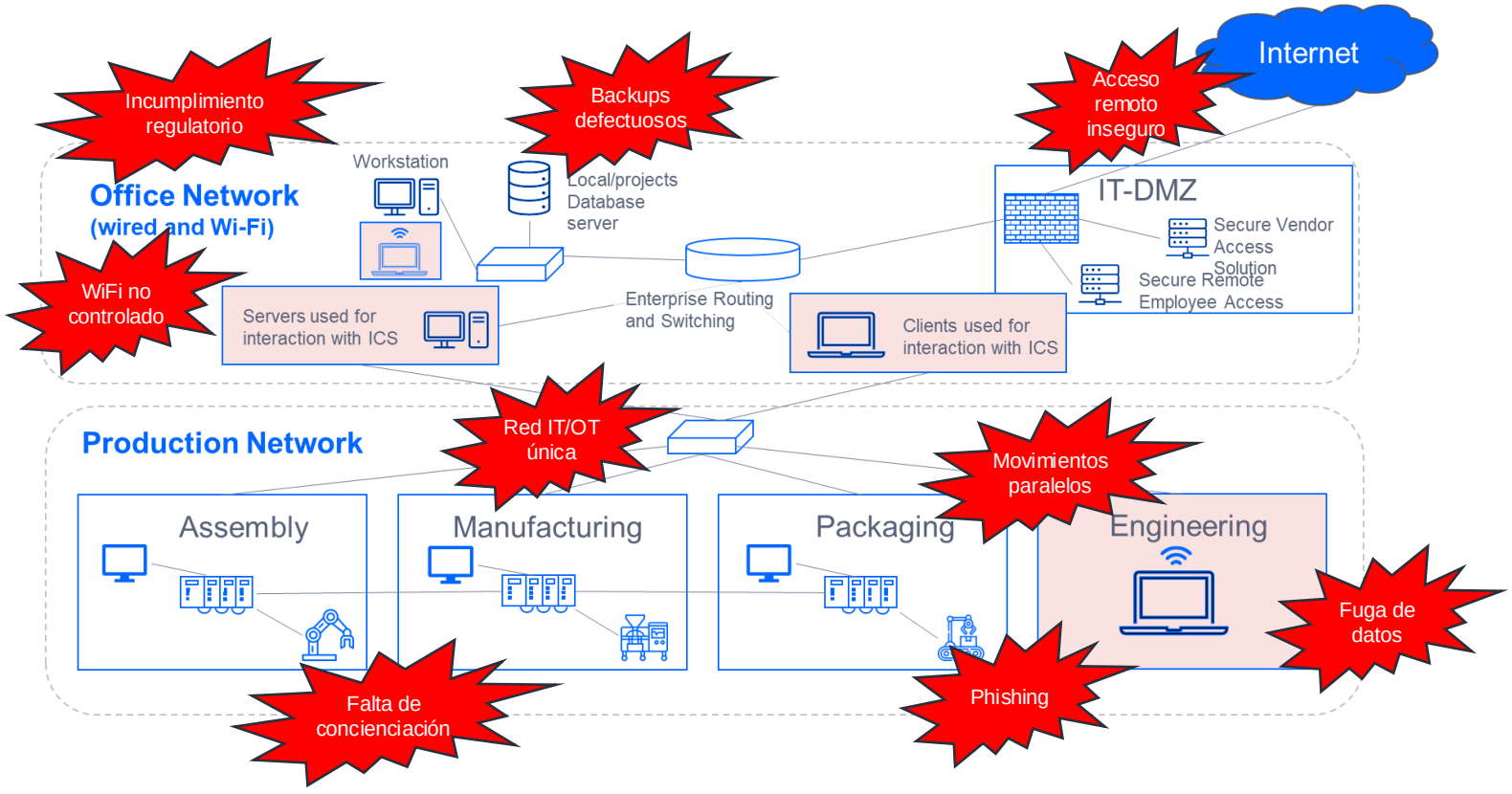
- Definir el alcance (SuC)
- Evaluación inicial de riesgos
- Modelo de Zonas y Conductos
- Evaluación detallada de riesgos
- Criterios de impacto y niveles de seguridad
- Plan de tratamiento de riesgos



Evaluación y gestión de riesgos en sistemas industriales

Proceso de evaluación de riesgos

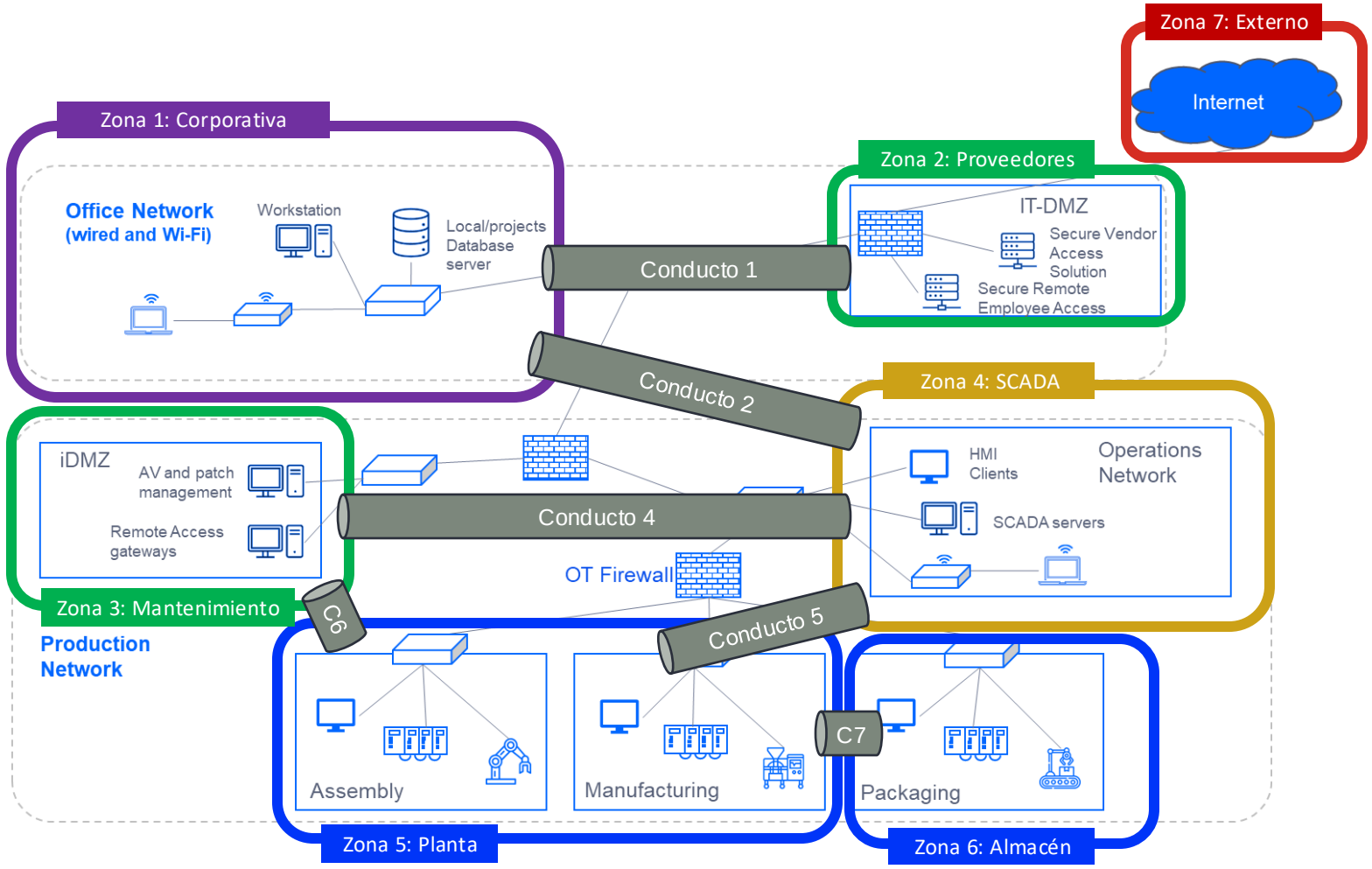
- Definir el alcance (SuC)
- Evaluación inicial de riesgos
- Modelo de Zonas y Conductos
- Evaluación detallada de riesgos
- Criterios de impacto y niveles de seguridad
- Plan de tratamiento de riesgos



Evaluación y gestión de riesgos en sistemas industriales

Proceso de evaluación de riesgos

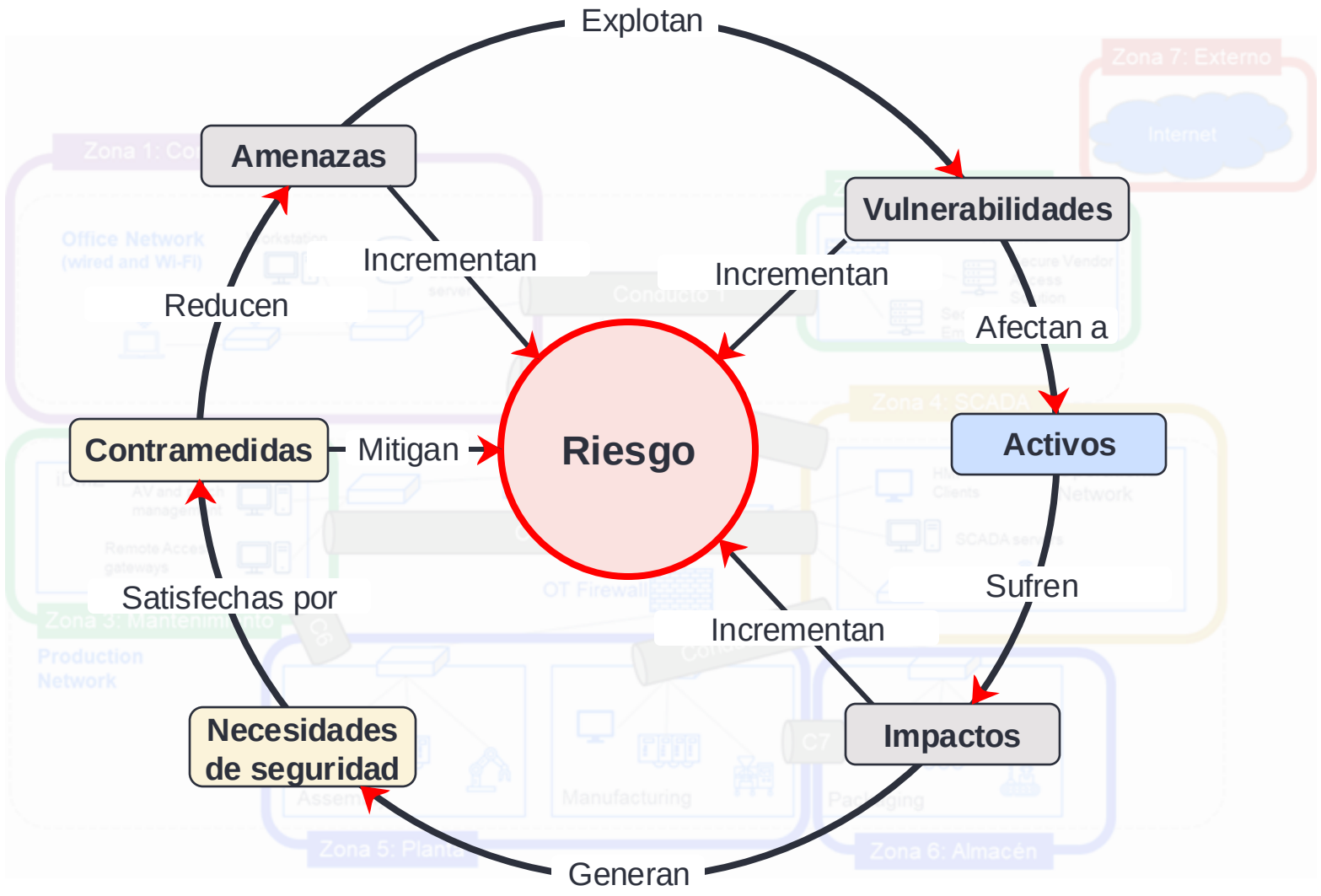
- Definir el alcance (SuC)
- Evaluación inicial de riesgos
- Modelo de Zonas y Conductos
- Evaluación detallada de riesgos
- Criterios de impacto y niveles de seguridad
- Plan de tratamiento de riesgos



Evaluación y gestión de riesgos en sistemas industriales

Proceso de evaluación de riesgos

- Definir el alcance (SuC)
- Evaluación inicial de riesgos
- Modelo de Zonas y Conductos
- Evaluación detallada de riesgos
- Criterios de impacto y niveles de seguridad
- Plan de tratamiento de riesgos



Evaluación y gestión de riesgos en sistemas industriales

Proceso de evaluación de riesgos

- Definir el alcance (SuC)
- Evaluación inicial de riesgos
- Modelo de Zonas y Conductos
- Evaluación detallada de riesgos
- Criterios de impacto y niveles de seguridad
- Plan de tratamiento de riesgos

Zona 7: Externo

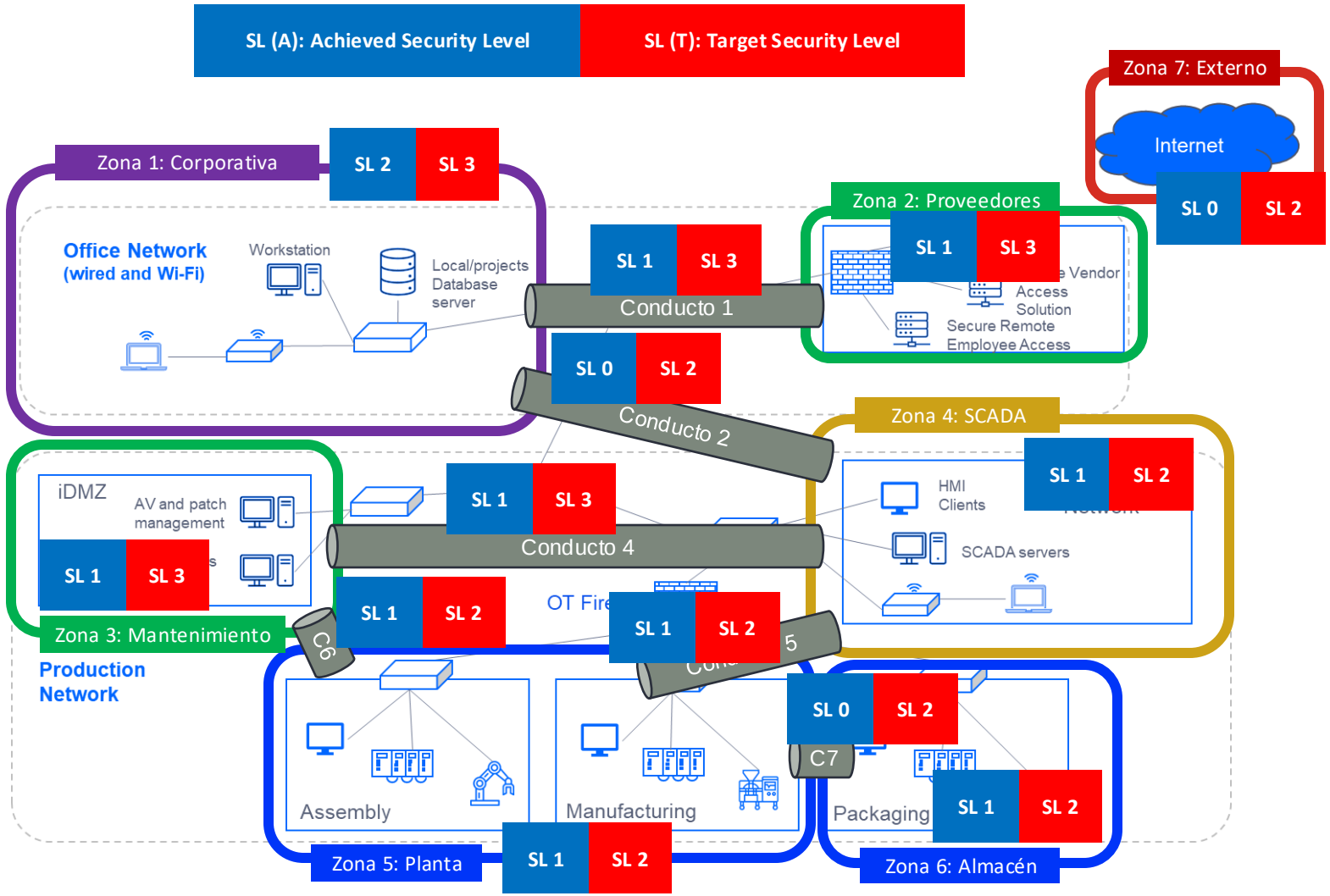
MATRIZ DE IMPACTO

		Continuidad de las operaciones	Seguridad de la información de los Sistemas de Control			Seguridad operacional	
Impacto	Valor	Interrupción de las operaciones	Coste	Legal	Confianza / Reputación	Personas	Medioambiente
Muy Alto	5	> 5 días	> 6 M €	Delito muy grave	Daños irreparables a la imagen	Múltiples fallecimientos	Incidente catastrófico. Delito muy grave
Alto	4	> 2 días	> 3 M €	Delito grave	Daño a la imagen de marca	Heridas con secuelas graves o muerte de una persona	Delito grave
Moderado	3	≤ 2 días	> 1,5 M €	Delito menor	Pérdida de confianza de clientes	Heridas mayores	Delito menor
Bajo	2	< 8 horas	> 300K €	Investigación o Inspección	Pérdida de reputación interna o local con pérdida de ingresos	Heridas menores con hospitalización	Investigación o Inspección
Insignificante	1	< 2 horas	≤ 300K €	N/A	Pérdida de reputación interna o local sin pérdida de ingresos	Heridas leves	Daño local reparable

Evaluación y gestión de riesgos en sistemas industriales

Proceso de evaluación de riesgos

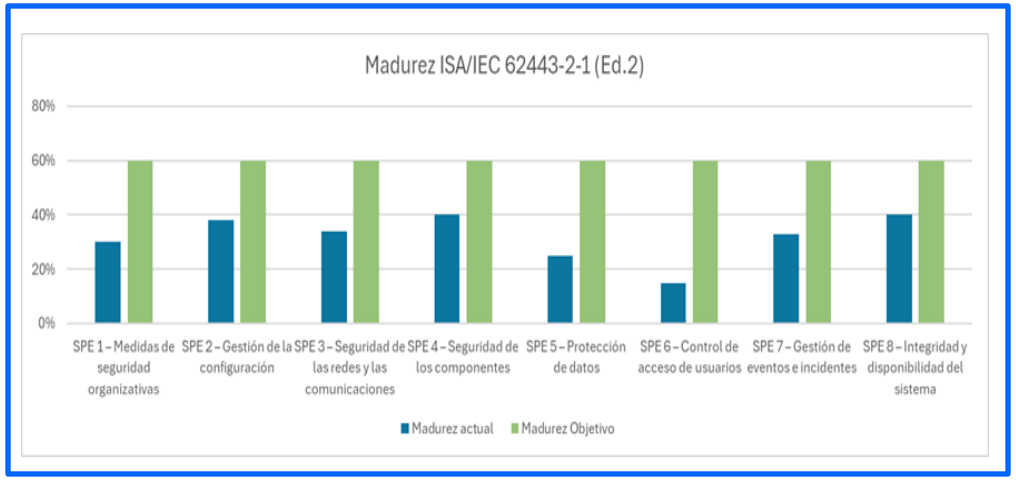
- Definir el alcance (SuC)
- Evaluación inicial de riesgos
- Modelo de Zonas y Conductos
- Evaluación detallada de riesgos
- Criterios de impacto y niveles de seguridad
- Plan de tratamiento de riesgos

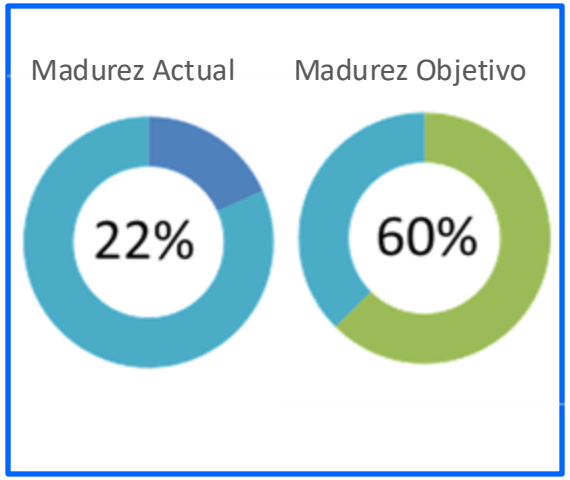


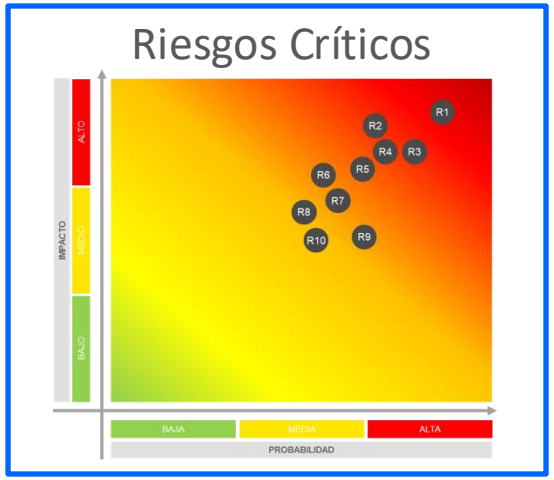
Evaluación y gestión de riesgos en sistemas industriales

Proceso de evaluación de riesgos

- Definir el alcance (SuC)
- Evaluación inicial de riesgos
- Modelo de Zonas y Conductos
- Evaluación detallada de riesgos
- Criterios de impacto y niveles de seguridad
- Plan de tratamiento de riesgos



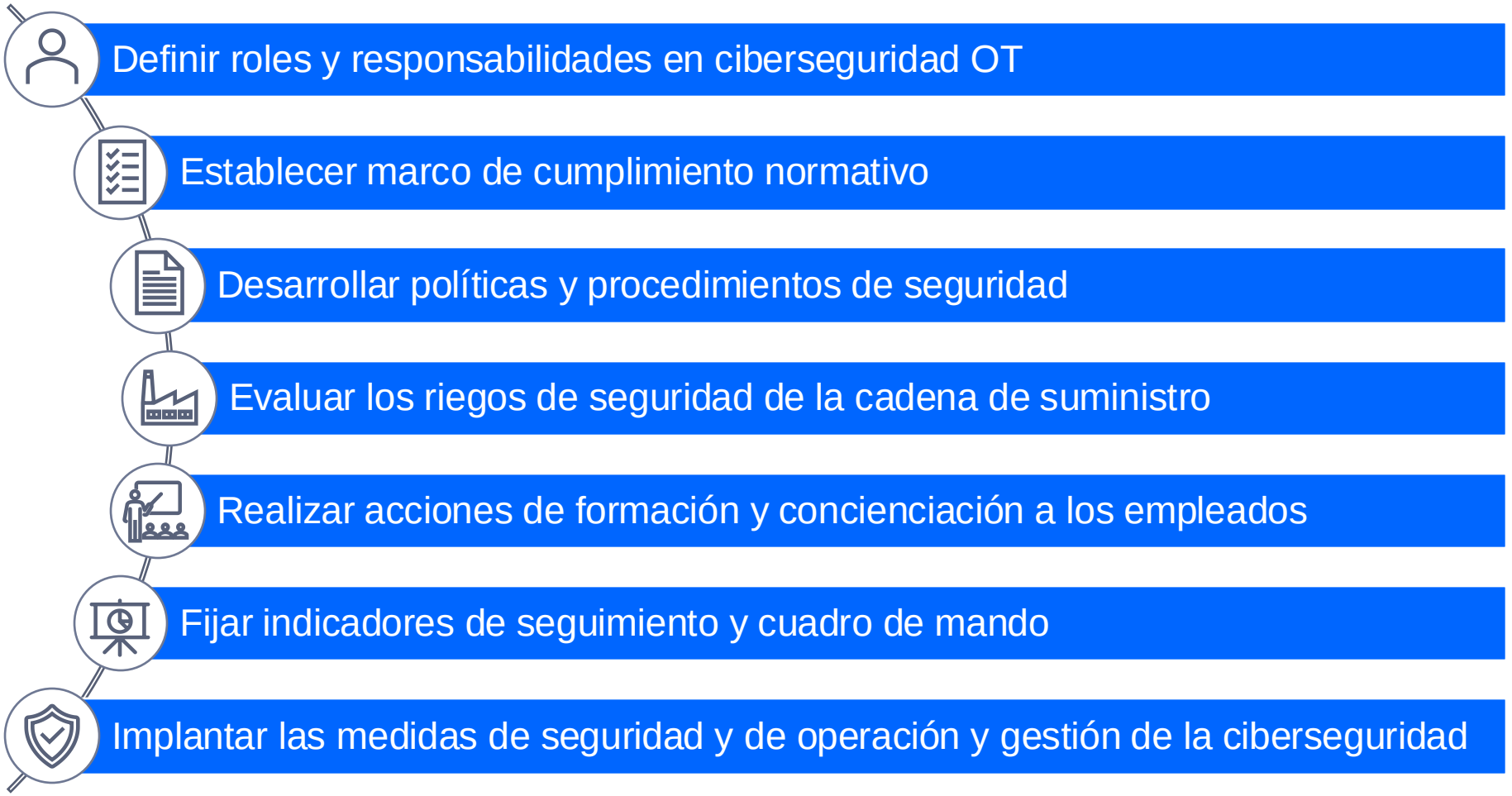




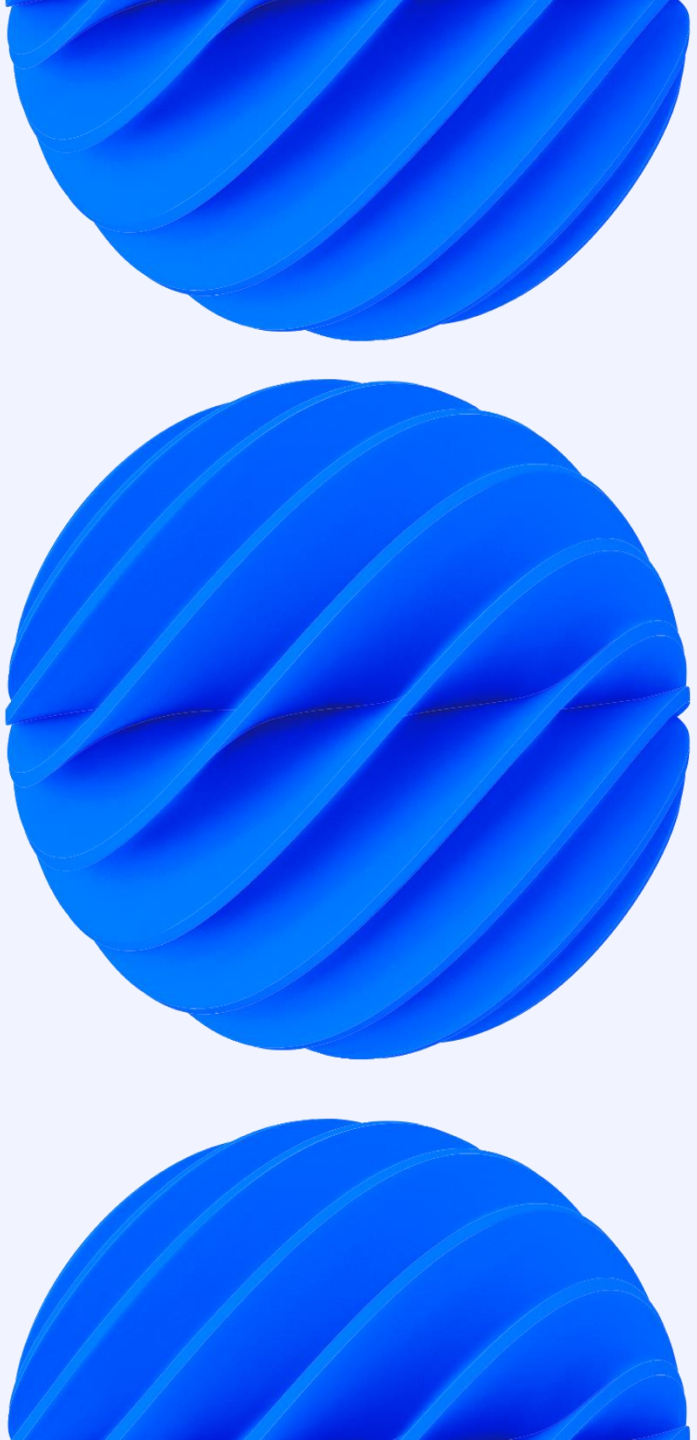
Proyecto	AÑO 1 1T	AÑO 1 2T	AÑO 1 3T	AÑO 1 4T	AÑO 2 1T	AÑO 2 2T	AÑO 2 3T	AÑO 2 4T
Política de seguridad y normativa de uso de los sistemas OT								
Bloqueo de los puertos USB								
Protección de los accesos remotos de proveedores OT								
Evaluación de riegos de terceros								
Plan de concienciación al personal en ciberseguridad (anti-phishing)								
Herramienta de monitorización de la red								
Elaborar los planes de recuperación ante desastres (DRP)								
Auditoría de seguimiento IEC 62443								
Cifrado de servidores y equipos portátiles								
Implantar MFA para sistemas críticos y accesos remotos								
Establecer un sistema de respuesta a incidentes (y contrato DFIR)								

Modelo de Gobernanza de la ciberseguridad en entornos OT

Puntos clave



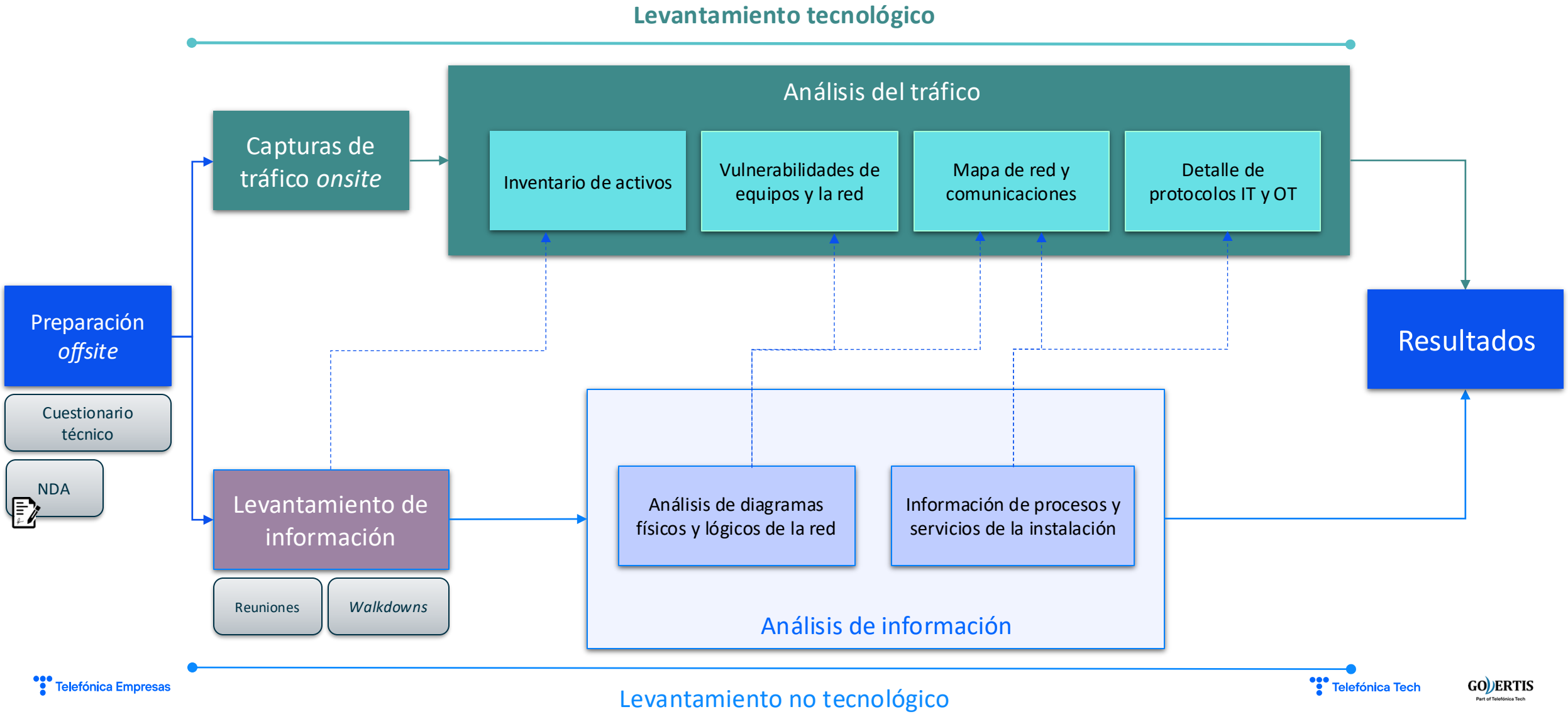
04. Soluciones de ciberseguridad para la Industria 4.0



Reto 1: Conocer cuáles son mis activos críticos, a qué riesgos están expuestos y cómo mitigarlos

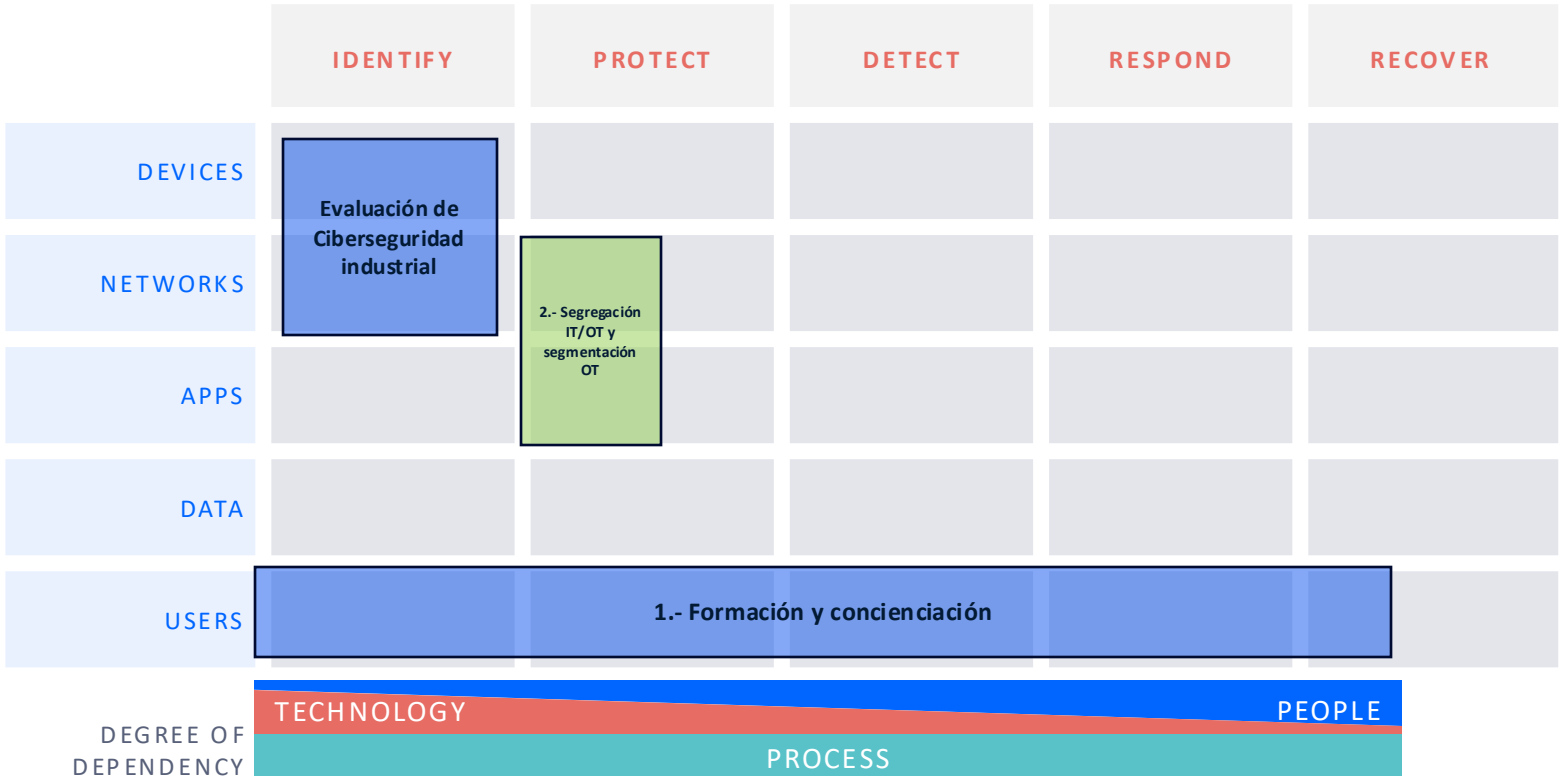
Source: https://www.goagilix.com/industrial-network-design-best-practices/

Propuesta de solución para el reto 1: Evaluaciones de Ciberseguridad Industrial



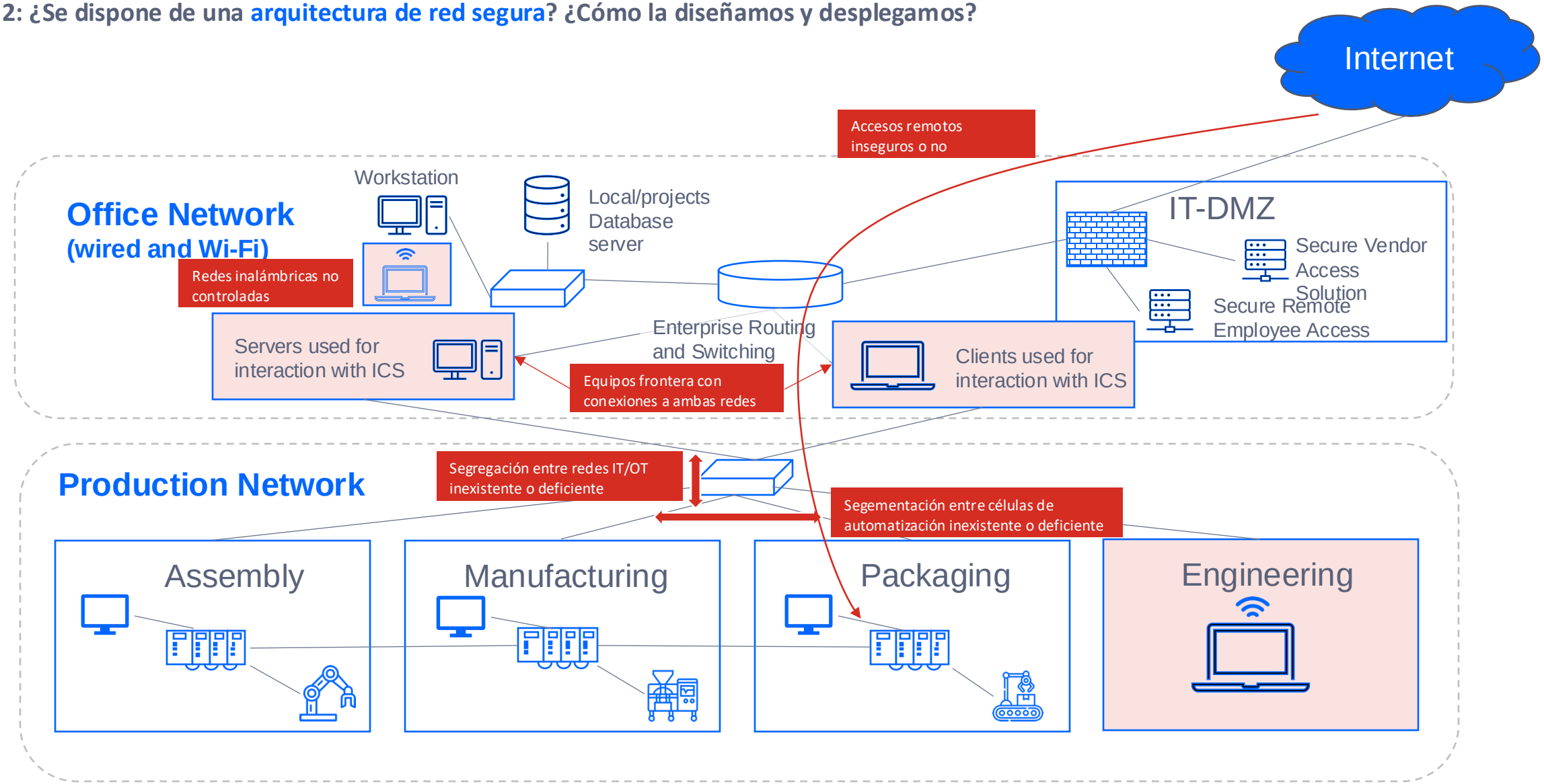
¿Cómo empezamos a poner orden a esta situación?

Matriz de ciberdefensa como marco de referencia para identificar y planificar la construcción de las contramedidas

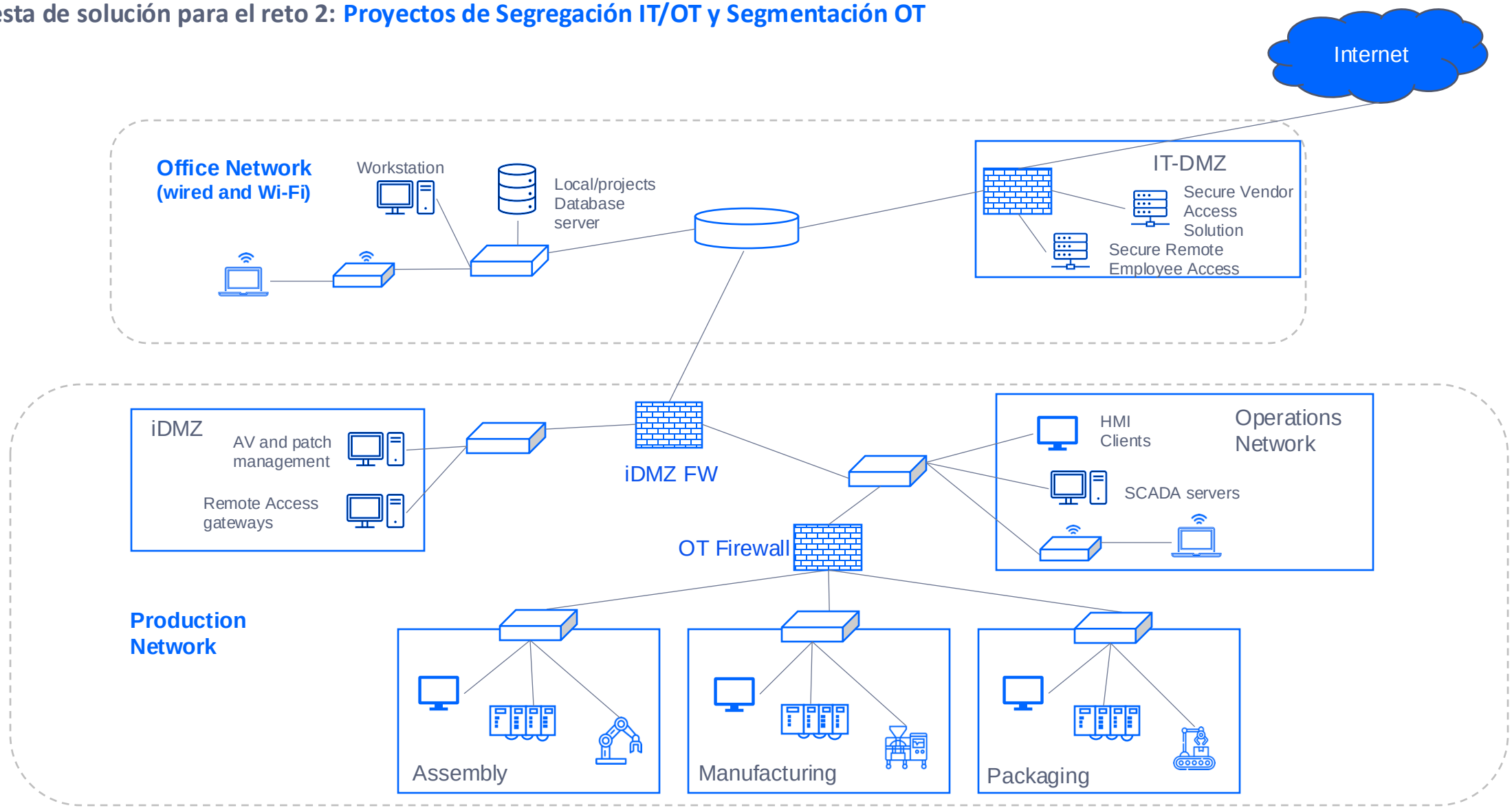


Source: @SOUNILYU | cyberdefensematrix.com

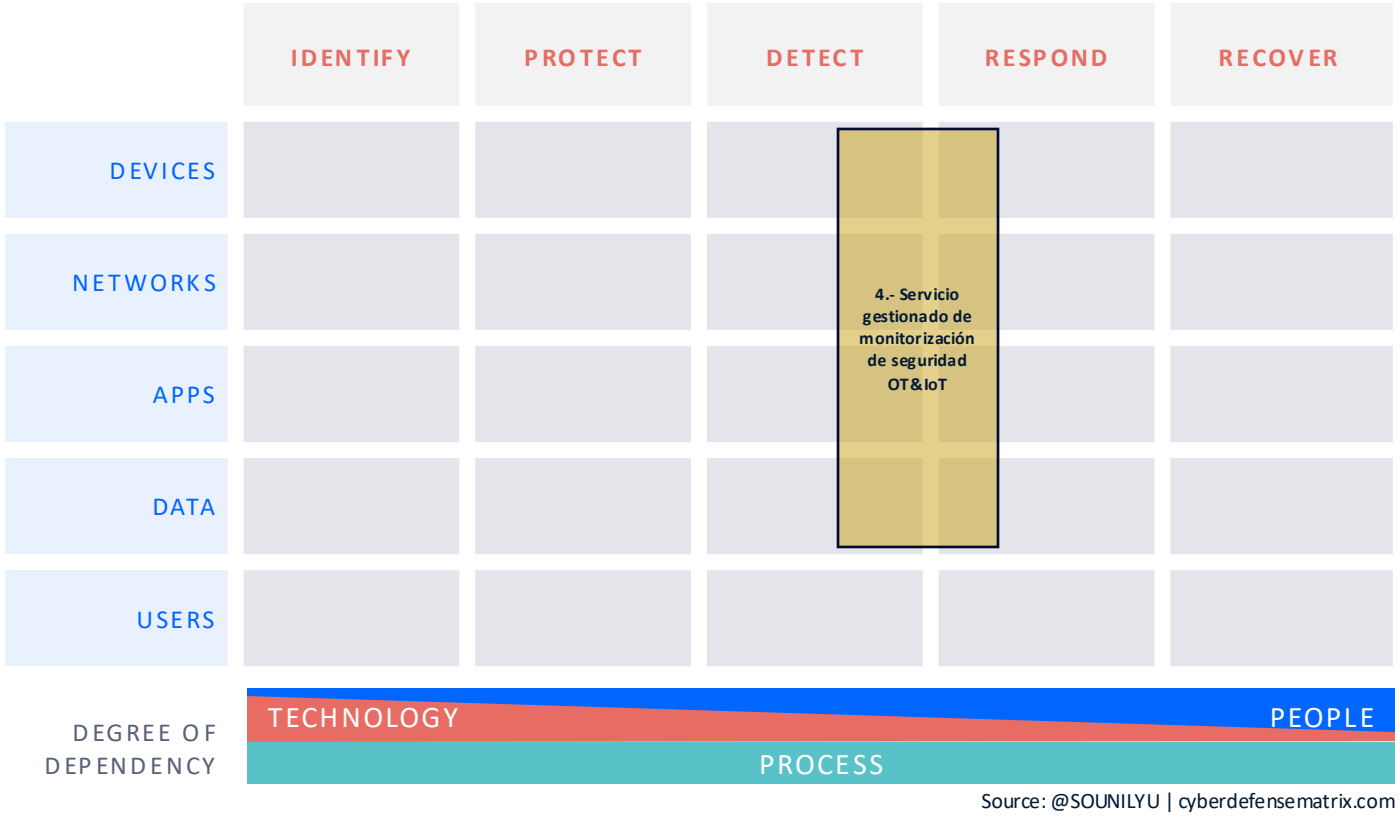
Reto 2: ¿Se dispone de una arquitectura de red segura? ¿Cómo la diseñamos y desplegamos?



Propuesta de solución para el reto 2: **Proyectos de Segregación IT/OT y Segmentación OT**

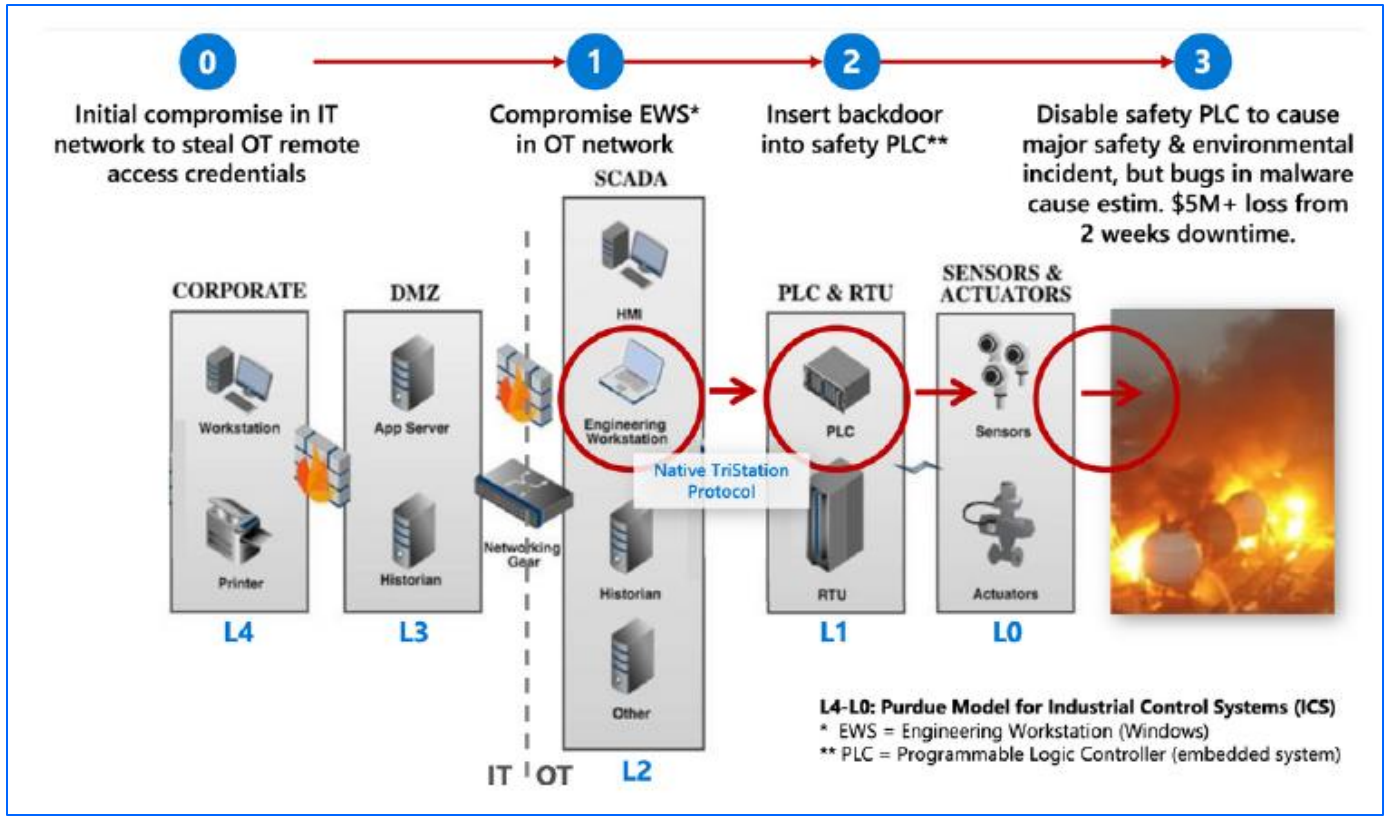


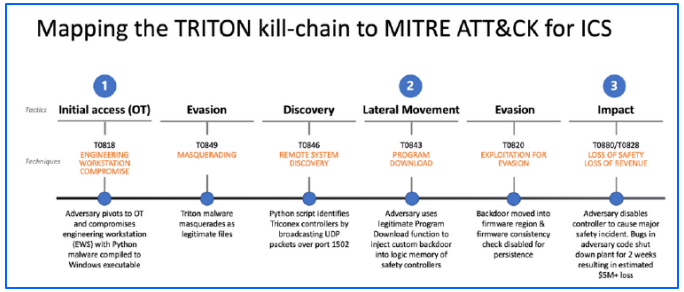
Propuesta de solución para el reto 2:



Source: @SOUNILYU | cyberdefensematrix.com

Reto 3: ¿Como mejoramos nuestras capacidades de **detección de incidentes en OT** y proporcionamos **visibilidad** continua de los activos?





Source: Microsoft blog - TRITON and MITRE ATTACK for ICS

Propuesta de solución para el reto 3: Servicio OT&IoT Security Monitoring

TCCT ofrece el servicio líder para la **seguridad y visibilidad de OT e IoT**. Se entrega como un **servicio gestionado** que aprovecha nuestras capacidades de iMSSP y está impulsado por la mejor tecnología de monitorización de su clase.

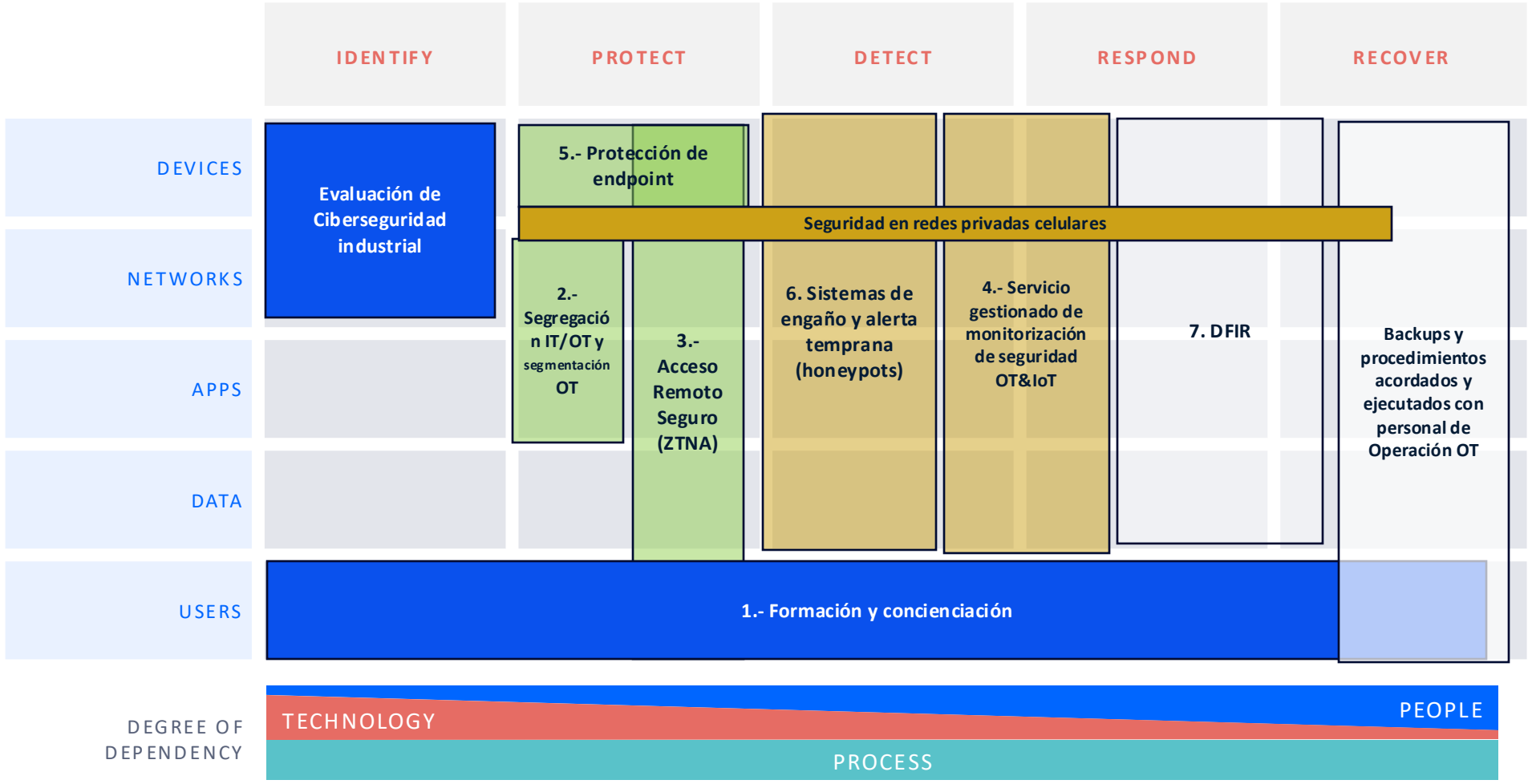
Funcionalidades clave

Visibilidad de lo qué hay en la red y cómo se comporta
Seguridad y visibilidad integrales en redes industriales e IoT

Detección de ataques, anomalías y malas prácticas específicas de industria
Notificación detallada de amenazas conocidas y desconocidas

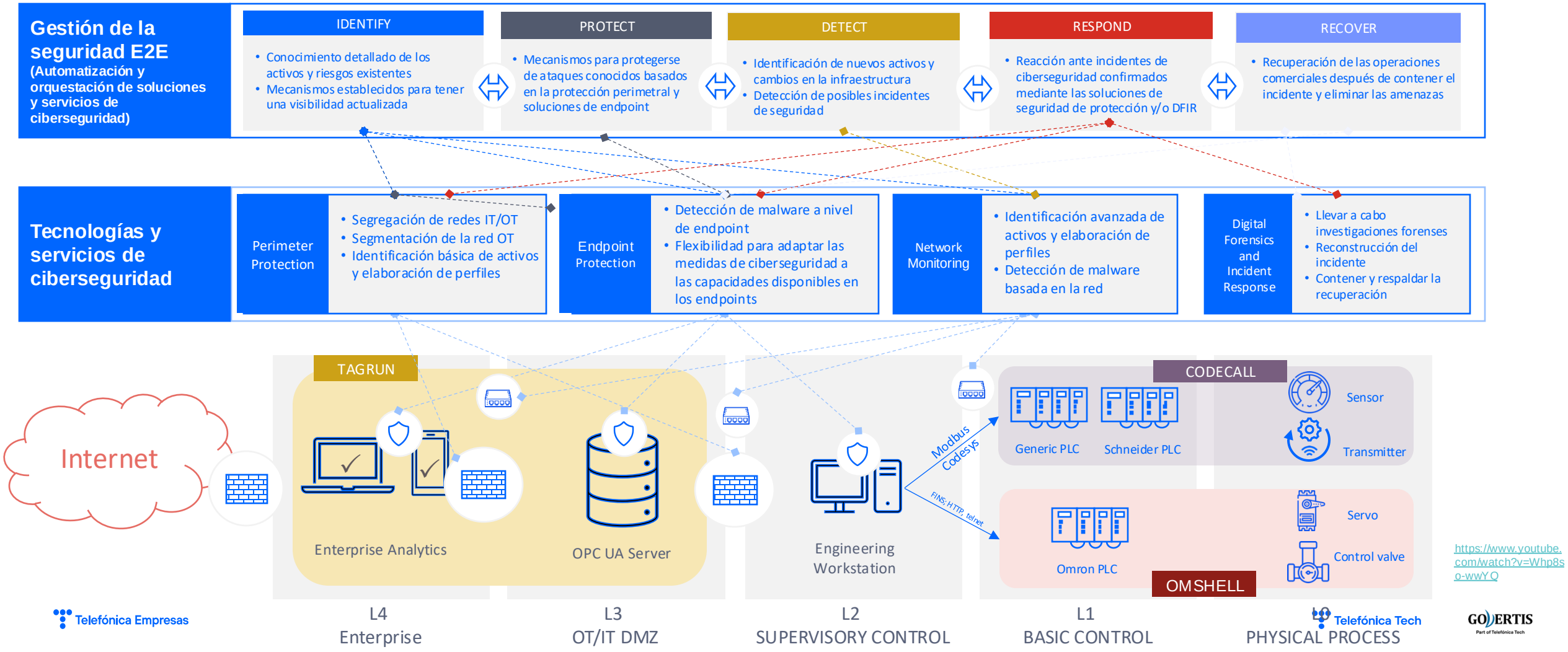
Servicio gestionado por un equipo especializado
Tecnología gestionada por equipo de ciberseguridad industrial con notificaciones en tiempo real ante incidentes e informes periódicos enriquecidos

RESUMEN: Mapa de contramedidas (soluciones) de ciberseguridad para entornos industriales.



Source: @SOUNILYU | cyberdefensematrix.com

Mission Critical SOC: para aumentar significativamente la resiliencia de los sistemas ciberfísicos es vital coordinar las diferentes contramedidas para que el conjunto actúe como un sistema con visión y capacidad E2E



https://www.youtube.com/watch?v=Whp8so-wwYQ

Los **sistemas ciberfísicos** son esenciales para asegurar y mejorar nuestro nivel de vida, pero su criticidad y bajo nivel de ciberseguridad los está convirtiendo en principal víctima de los cibercriminales

Por ello es fundamental empezar a tomar medidas, empezando por **conocer los activos y los riesgos** a los que están expuestos e implantando las contramedidas básicas adaptadas a estos entornos

Para incrementar la resiliencia de los entornos más expuestos resulta esencial implementar el concepto de "**Mission Critical SOC**", basado en coordinar las funciones de ciberseguridad básicas para mantener un conocimiento actualizado del entorno y de la postura de seguridad así como poder reaccionar satisfactoriamente

Telefónica Tech

04

Q&A con los asistentes

¿CÓMO CONTACTAR CON NOSOTROS?

Código QR:

O

Contacta con tu comercial de Telefónica

Una iniciativa de: Telefónica Tech

En colaboración con: GOODERTIS
Part of Telefónica Tech