Secure&IT by LKS Next

www.secureit.es

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría MEDIA RD 3/2010

FIRST Improving Security Together

CSIRT.es

Calidad Certificada ABS Quality Evaluations, Inc. Management System Certification ISO 9001:2015 Certificate Nº:57146

Seguridad Certificada ABS Quality Evaluations, Inc. Management System Certification ISO/IEC 27001:2013 Certificate Nº:48038

CYBERSECURITY MADE IN EUROPE

CIBERSEGURIDAD Y CUMPLIMIENTO

Francisco Valencia
Director General
Secure&IT
francisco.valencia@secureit.es
911 196 995

Secure & IT by LKS Next

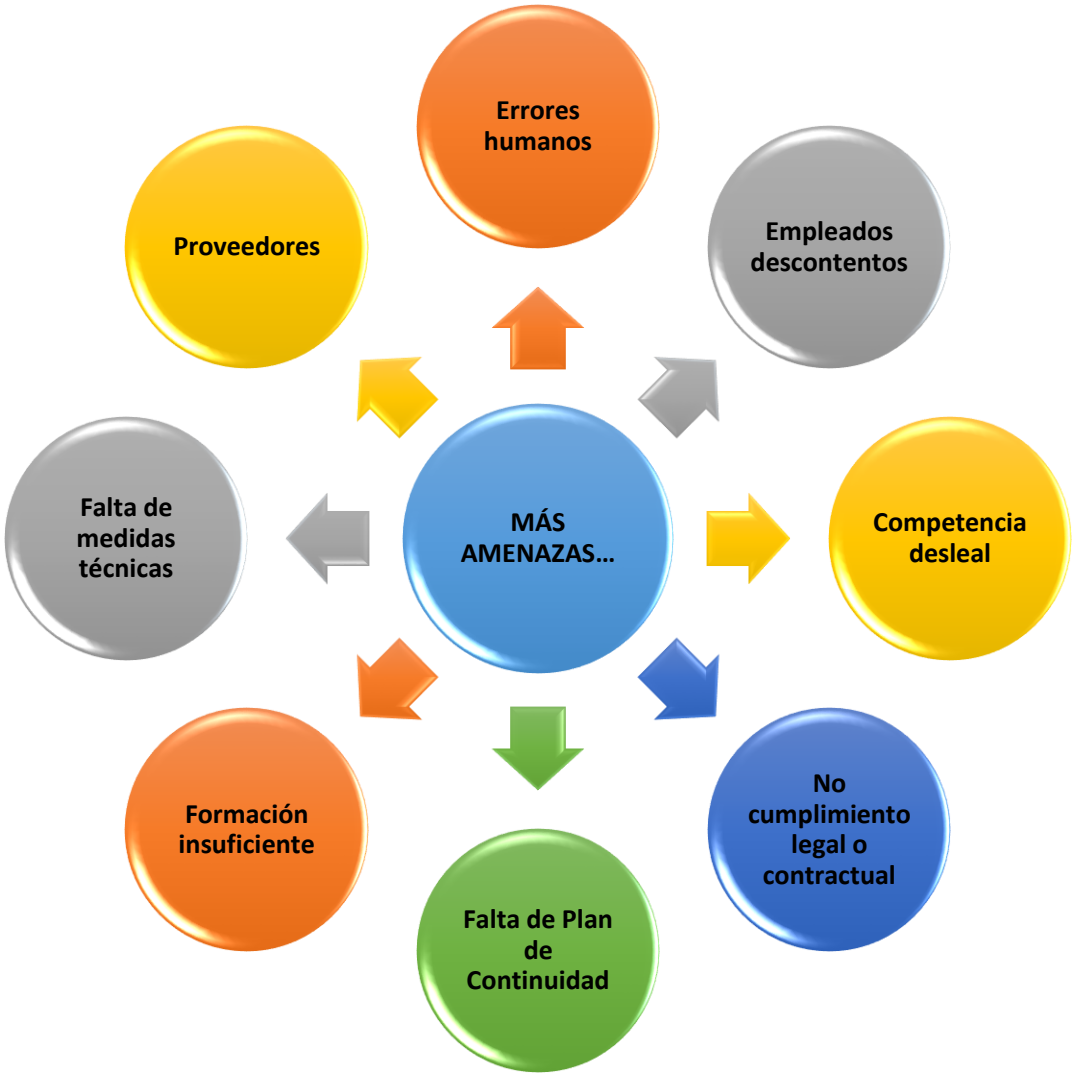
www.secureit.es

¿Falsa sensación de seguridad?

Situación actual

- Movimientos sociales e inestabilidad política dan como resultado organizaciones de **hacktivismo**, **ciberdelincuencia**, **ciberterrorismo**, **ciberespionaje** y **ciberguerra**.
- Existen muchos intereses que tratan de desestabilizar el modelo económico occidental, con especial foco en las economías americana y europea
- El numero de ataques se ha incrementado en un **50% en 2020** con respecto a 2019, sumando más de **250.000 impactos graves en España**
- España es ya el **tercer país mas ciberatacado** del mundo, aunque es el séptimo en protección.
- La situación causada por COVID-19 ha provocado un fuerte incremento en algunas de estas amenazas
- Ataques con mayor crecimiento:
  - **Ataques OT/IoT** -> Automoción, Medicina, Industria, Smart Cities, Infraestructuras, etc…
  - **Ransomware** -> El trío Emotet / Trickbot / Tyuk ha crecido enormemente, causando gravísimos impactos en empresas de todos los tamaños y sectores.
  - **Fraude al CEO** -> Ha perdido impactos pero sigue siendo una gran amenaza, con pagos ilícitos que alcanzan millones de euros
  - **Robo de credenciales y phishing** -> Especialmente a sistemas de correo cloud y redes sociales. Empleados para posteriores ataques
  - **Ataques a dispositivos móviles** -> Desde aplicaciones malintencionadas hasta puntos de acceso WIFI inseguros
  - **Robo de información con chantaje** -> Afecta a empresas, particulares, menores..

Y la amenaza no son sólo los hackers…



La falta de valoración de activos y definición de procesos críticos de negocio dificulta la implantación de medidas técnicas y organizativas con éxito. Provoca inversiones vagamente justificadas y poco efectivas.

Los departamentos de Asesoría Jurídica de las empresas son expertos en normativa laboral, mercantil, fiscal, etc, pero rara vez son expertos en Derecho Tecnológico. Los Departamentos de TI tampoco manejan esta materia. Los incumplimientos y sanciones en protección de datos y otras normativas son habituales

La escasa formación y concienciación de los recursos humanos favorece la ingeniería social, deslealtad de empleados, robo de información para entregarlos a la competencia, etc.

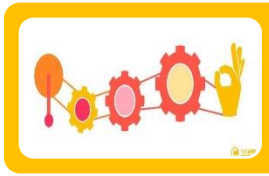
Impacto y Responsabilidad

ECONÓMICA

- **Pérdidas económicas inmediatas o indirectas. De difícil cuantificación**

REPUTACIONAL

- **Prestigio y Confianza del entorno se ven gravemente afectados**



OPERATIVA

- **Producción, logística, y otros procesos pueden verse afectados**

SOBRE LAS PERSONAS

- **Exposición de datos, pérdida de trabajo, salud…**

SOBRE EL CUMPLIMIENTO

- **Responsabilidad civil o penal por incumplimiento del deber de aplicar medidas preventivas – Código de Derecho de la Ciberseguridad**

SOBRE LA ESTRATEGIA

- **Imposibilidad de cumplir objetivos estratégicos. Incluso riesgo de continuidad de negocio.**

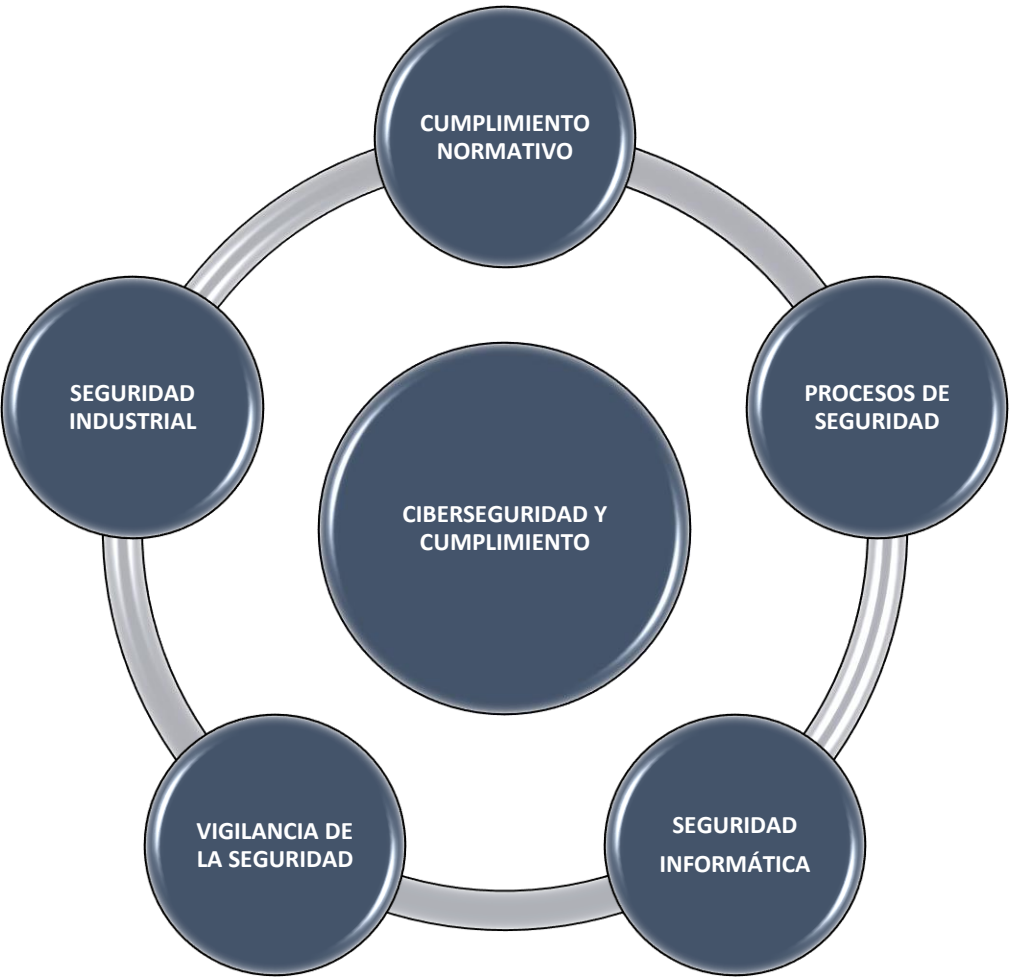
La empresa NO ES LA UNICA AFECTADA

Es **irresponsable y poco ético** no aplicar medidas cuando se pueden ver afectados, además:

& Proveedores
& Clientes
& Socios
& Empleados
& Candidatos
& Ciudadanos
& Usuarios
& Etc..

Por eso existe regulación sectorial, industrial, jurídica y de buenas practicas. Para ayudar a la empresa a ser **RESPONSABLE**

Los pilares de la Ciberseguridad



CUMPLIMIENTO NORMATIVO

Satisface la demanda que le es exigida a la organización.

- & Exigencias **Legales** (GDPR, C. Penal…)
- & Normas **Sectoriales** (PCI-DSS, ENS…)
- & **Estándares** (ISO 27001 / 20000 / 22301)
- & Medidas dispuestas por **Clientes**

PROCESOS CORPORATIVOS

Permite dotar al CEO de un "cuadro de mando" de la gestión de su seguridad.

- & Identificación y valoración de **Activos**
- & Análisis de **Riesgos**
- & Roles y **Responsabilidades**
- & **Medidas** aplicadas y sus **Resultados**

SEGURIDAD INFORMÁTICA

Protege las vulnerabilidades propias de los sistemas informáticos:

- & Sistemas anti **malware**
- & Protección contra **hackers**
- & **Criptografía**
- & **Ciberseguridad OT/IoT**

VIGILANCIA DE LA SEGURIDAD

Permite la rápida detección, respuesta y mitigación de impactos de seguridad

- & Aplica tanto a **IT** como a **procesos OT**
- & Reduce la incertidumbre. Existen **IRPs**
- & Control **gráfico**
- & Informes y **cuadros de mando**

Acerca de Secure&IT

MONDRAGON HUMANITY AT WORK — Finance Industry Retail Knowledge

Empresa 100% española creada en 2009 por Abogados expertos en Derecho de las TIC, Ingenieros y Expertos en Seguridad de la Información.

Misión: Ayudar a las empresas a disminuir los riesgos a que se exponen a causa de la gestión de su información.

Líderes en auditoría e implantación de modelos avanzados de gestión de la ciberseguridad y el cumplimiento normativo

Trofeos de la Seguridad TIC — Mejor Empresa de Seguridad TIC

Equipo altamente cualificado, gran parte de la inversión destinada a formación.

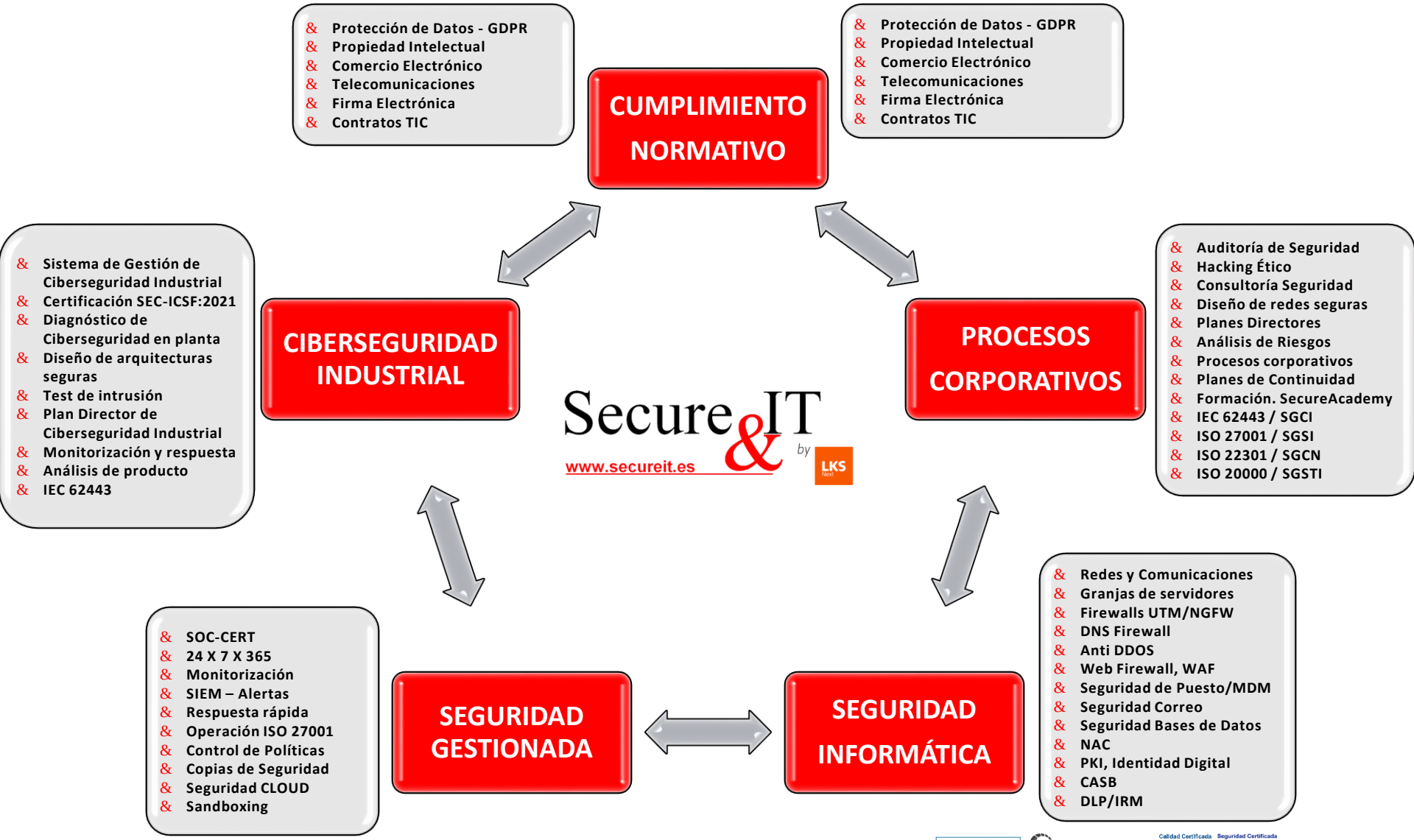
Seguridad 360º para la información de su empresa:

Procesos Corporativos
Seguridad Informática
Cumplimiento Normativo

Secure&View©. Dos centros de Seguridad SOC de control y supervisión 24x7x365 Madrid – Mondragón

ISO27001 / ISO9001 / CERT / ENS

Nuestros Servicios. Seguridad 360º



Certificaciones y reconocimientos

Referencias Ciberseguridad industrial

Secure&IT by LKS Next

www.secureit.es

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría MEDIA RD 3/2010

FIRST Improving Security Together

CSIRT.es

Calidad Certificada ABS Quality Evaluations, Inc. Management System Certification ISO 9001:2015 Certificate Nº:57146

Seguridad Certificada ABS Quality Evaluations, Inc. Management System Certification ISO/IEC 27001:2013 Certificate Nº:48038

CYBERSECURITY MADE IN EUROPE

RETOS DE LA CIBERSEGURIDAD EN ENTORNOS INDUSTRALES

Francisco Valencia
Director General
Secure&IT
francisco.valencia@secureit.es
911 196 995

Ciberseguridad amenaza permanente

La ciberseguridad es actualmente, sin dudas, una de las principales preocupaciones en nuestras empresas. Las amenazas son palpables y, sin importar si su materialización se produce de forma intencional o involuntaria, el impacto en la disponibilidad de los **sistemas de producción industrial** puede ser muy elevado, ocasionando tiempos de inactividad que pueden poner en peligro en propio negocio.

Ciberseguridad Industrial

Que implica

La ciberseguridad industrial pretende proteger:

LA INFORMACIÓN	EL PROCESO INDUSTRIAL	LA INTEGRIDAD FÍSICA DE LAS PERSONAS E INSTALACIONES
Que existe, se transmite y se procesa en las infraestructuras industriales	Y los elementos que lo componen: PLCs, HMIs, SCADAs, red, PCs,…	La seguridad desde la perspectiva de la seguridad funcional
SECURITY		SAFETY

Proceso de mejora continua

El flujo de la ciberseguridad en OT

Identificar	Proteger	Monitorizar	Responder	Recuperar
los elementos del proceso industrial y riesgos asociados	para limitar o contener el impacto de un incidente	para identificar la ocurrencia de eventos no legítimos	respuesta planificada ante un evento	la operación normal después de un incidente y lecciones aprendidas
Proceso, actividad y activos ligados	**Protección específica de acuerdo al proceso industrial**	**Anomalías y eventos de seguridad**	**Disminuir el impacto en la actividad del negocio**	**Restauración de la actividad productiva habitual**

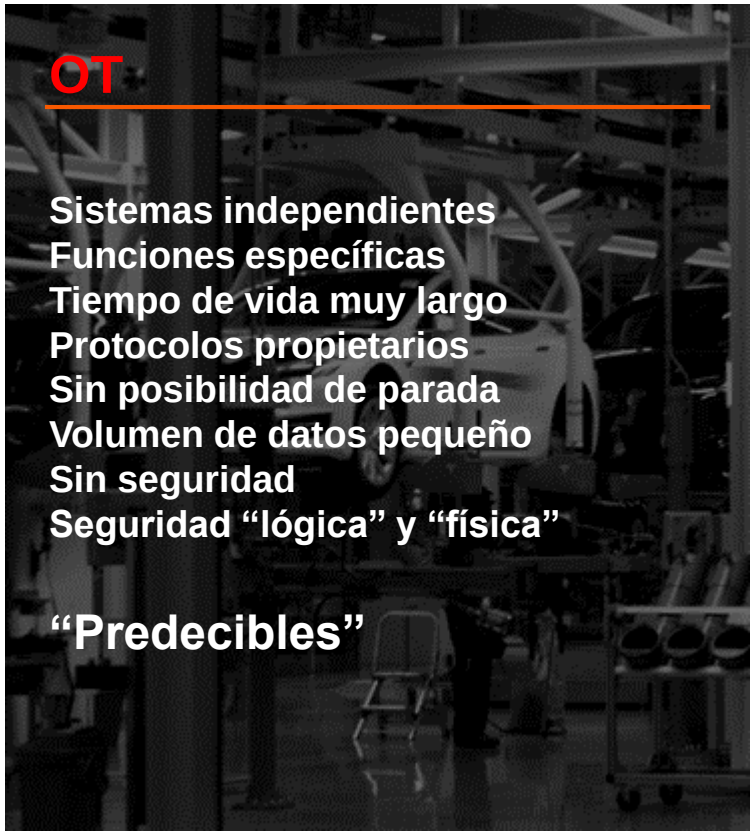
Indeterminismo Vs Determinismo

Distinta naturaleza, distintos objetivos

IT

Diseñados para la conectividad
Multitud de servicios
Actualizaciones frecuentes
Uso de estándares
Ventanas de parada programables
Alto volumen de datos
Seguridad por diseño
Seguridad “lógica”

“Impredecibles”

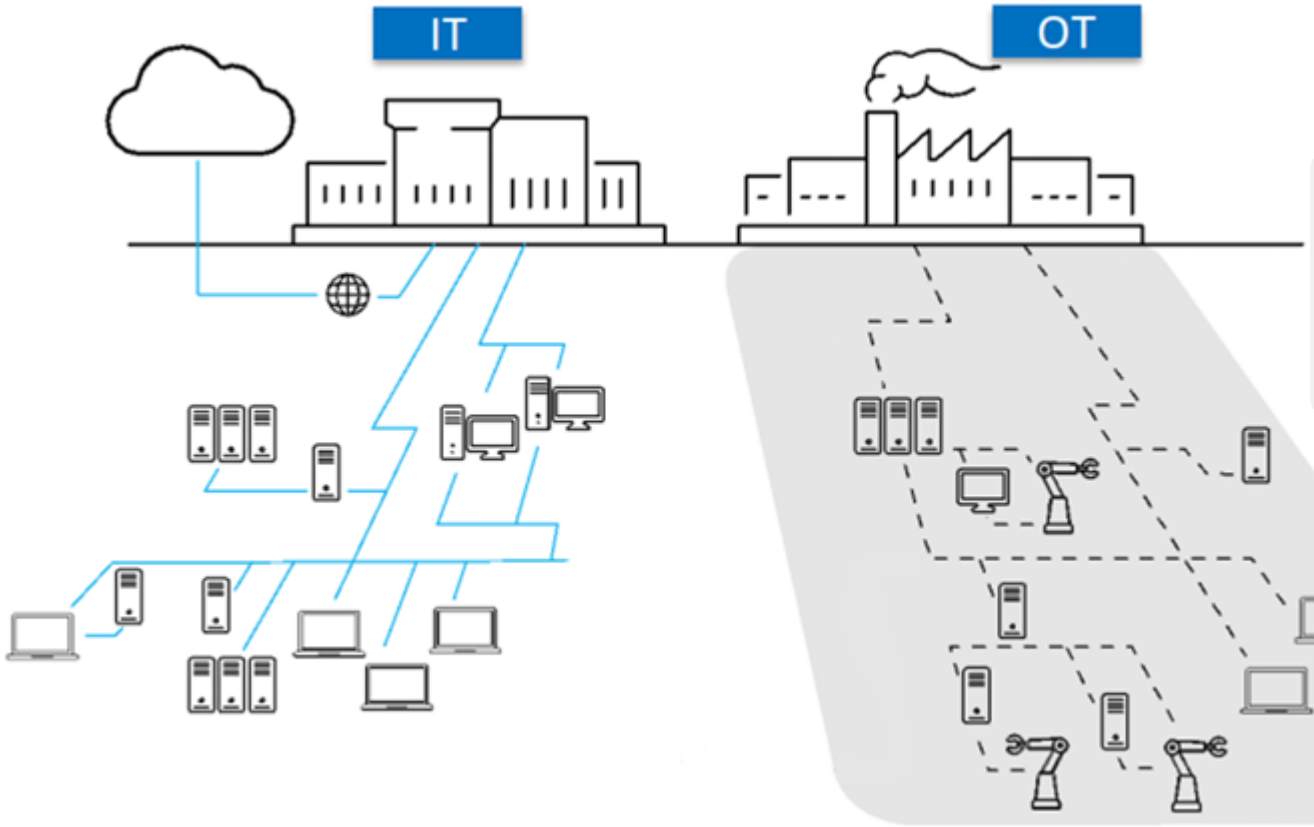


OT

Sistemas independientes
Funciones específicas
Tiempo de vida muy largo
Protocolos propietarios
Sin posibilidad de parada
Volumen de datos pequeño
Sin seguridad
Seguridad “lógica” y “física”

“Predecibles”

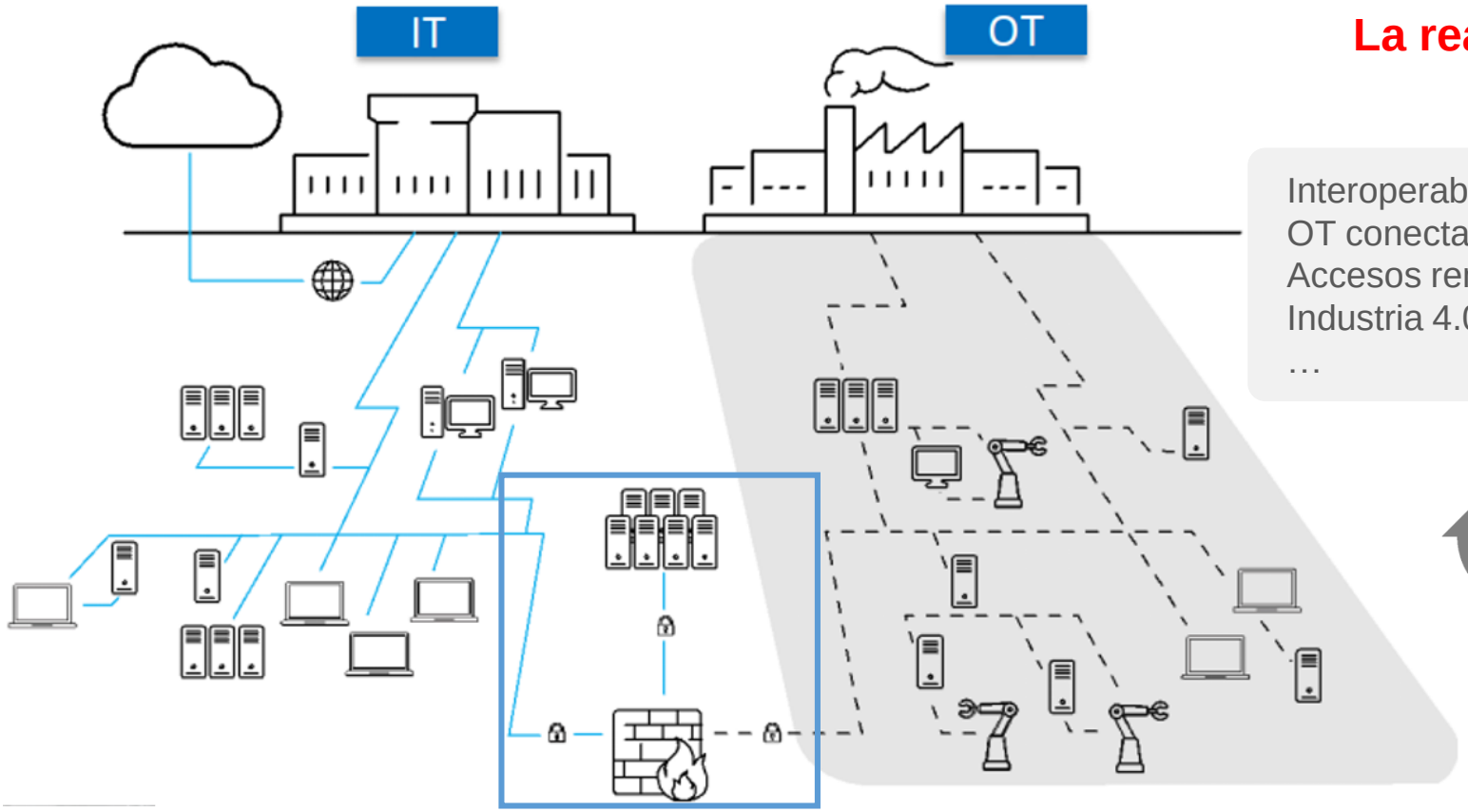
La complejidad de las redes IT/OT



La situación ideal

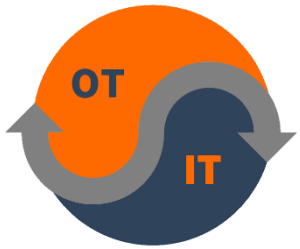
Entornos aislados
Sin integración
IT conectado a Internet
OT sin conexión a Internet

La complejidad de las redes IT/OT



La realidad

Interoperabilidad IT-OT
OT conectado a Internet
Accesos remotos
Industria 4.0
…



Los retos en entornos OT

… habitualmente complejos

01

CAJA NEGRA
No hay conocimiento exhaustivo de los elementos conectados a las redes de planta. No es posible proteger algo de lo que se desconoce su existencia.

02

SIN MEDIDAS DE PROTECCIÓN
Instalaciones que no se han actualizado desde su puesta en producción en tiempos en los que la ciberseguridad no era un requisito en el diseño.

03

SIN POSIBILIDAD DE PARADA
La disponibilidad desbanca a la confidencialidad en cuanto a las dimensiones de seguridad prioritarias. Ventanas de actuación limitadas.

04

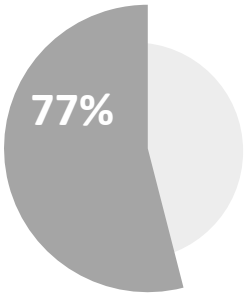
ACCESOS DE TERCEROS
Para tareas de mantenimiento y soporte, desde accesos remotos o bien con conexiones in-situ... Sin un control previo de los equipos que minimice la posibilidad de un incidente.

05

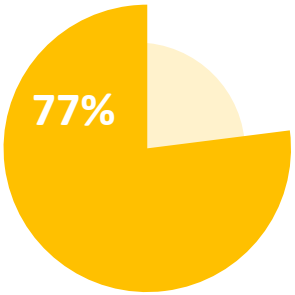
RESPONSABILIDAD DE LA GESTIÓN DE LA SEGURIDAD
¿Quién determina las medidas de seguridad de las instalaciones? ¿Hasta donde llega IT? ¿Y el personal de planta?

Riesgos y realidad

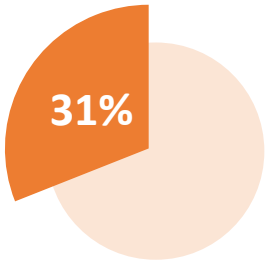
Los ciberriesgos en entornos industriales son reales



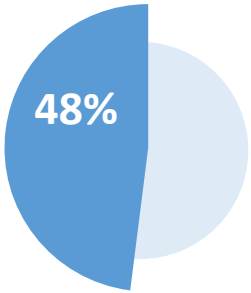
El 77% de las empresas consideran la ciberseguridad como su mayor prioridad



Tres de cada cuatro empresas (77%) esperan un ataque inminente que afecte al entorno ICS



El 31% de las compañías han experimentado al menos un incidente de seguridad ICS en los últimos 12 meses



El 48% de las empresas no cuentan con un programa de respuesta ante incidentes en el entorno OT

Fuente: The state of Industrial Cybersecurity 2018 - Karspersky

Conclusión

El nivel de riesgo como factor determinante

CIBERSEGURIDAD

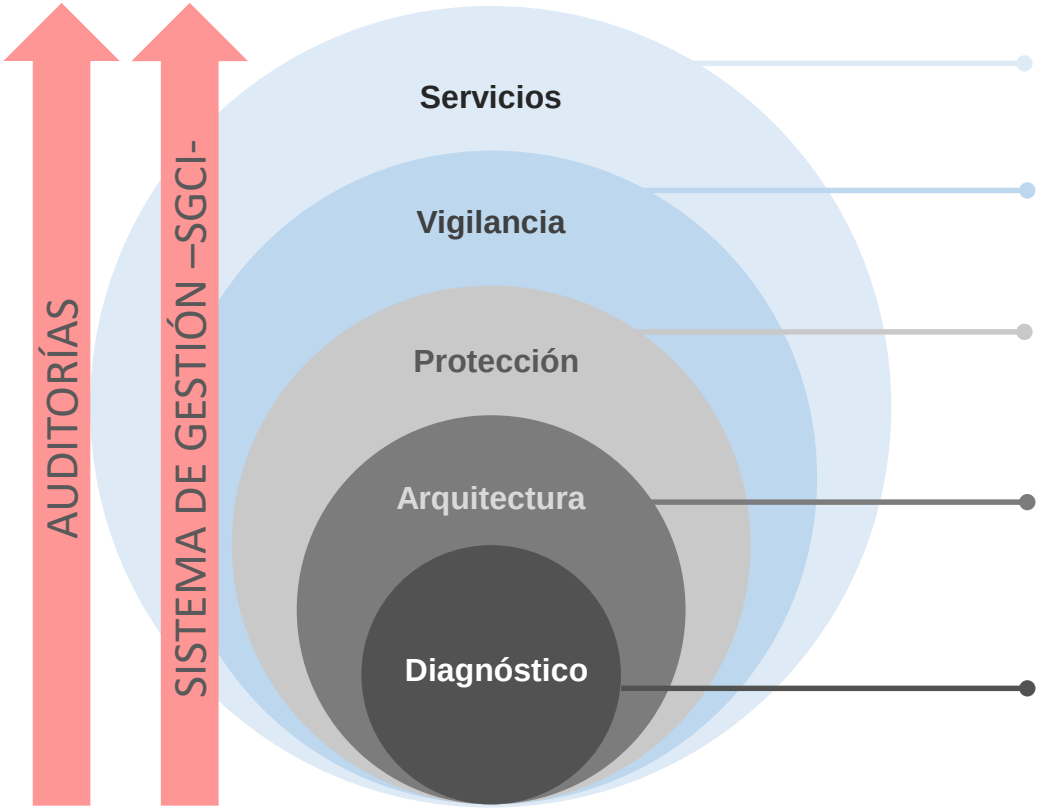
+

Escenario global de ciberamenazas
Arquitecturas de red heredadas
Desconocimiento de “lo que hay”
Seguridad OT gestionada desde IT
Carencia de conocimientos para la protección ICS
Esfuerzos puntuales voluntariosos
Escasez de medios y recursos

Nivel de riesgo elevado

Seguridad ordenada

Desde el diagnóstico hasta los servicios gestionados



Servicios gestionados (MSSP)
Gestión experta de la ciberseguridad

Monitorización permanente
Supervisión de tráfico de red, anomalías de comportamiento y vulnerabilidades.

Despliegue de soluciones de seguridad
Integración de soluciones para la protección de la red, los sistemas y la información.

Arquitecturas seguras
La base fundamental sobre la que articular todas las medidas de protección y monitorización de nuestra infraestructura.

El estado de las cosas
Análisis diagnóstico que permita definir un escenario objetivo y las acciones necesarias a llevar a cabo para poder alcanzarlo.

Sistema de Gestión de Ciberseguridad Industrial SEC-ICSF:2021

SEC-ICSF:2021

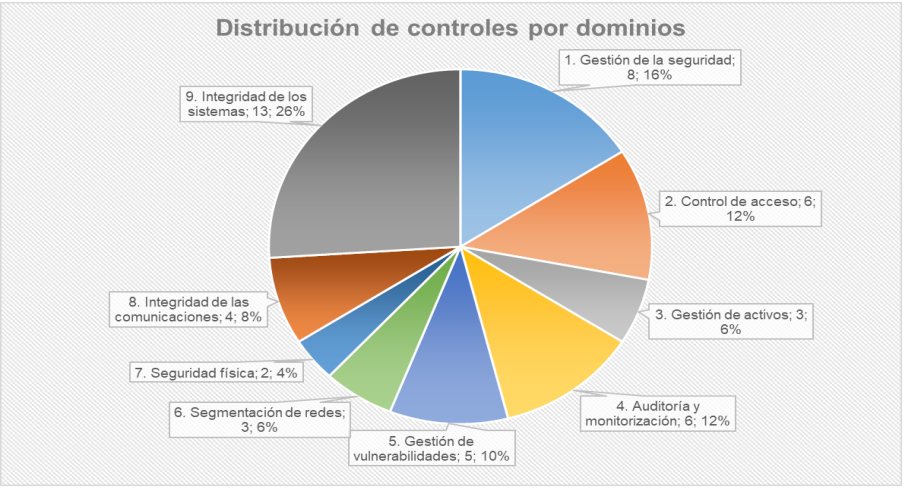
Marco de control **Ciberseguridad Industrial**

Alcanzable **sin grandes esfuerzos** ni inversiones

Orientado a **todo tipo de empresas industriales**

Niveles de **riesgo** y **cumplimiento** controlados

Compatible y complementario a **SGSI**



VENTAJAS SEC-ICSF:2021

Limita los "ciberriesgos" en entornos industriales

Mejora y complementa su Sistema de Gestión de Seguridad

Sirve de base para cualquier norma (TISAX, IEC62443, ALCOA (FDA/EMA), etc.)

Servicio "de principio a fin" con Secure&IT

Certificado por importante entidad certificadora reconocida internacionalmente: OCA GLOBAL

OCA GLOBAL "Posiblemente, la compañía de ensayos, inspección y certificación con **mayor crecimiento orgánico en el mundo.**"

Secure&IT by LKS Next

www.secureit.es

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría MEDIA RD 3/2010

FIRST Improving Security Together

CSIRT.es

Calidad Certificada ABS Quality Evaluations, Inc. Management System Certification ISO 9001:2015 Certificate Nº:57146

Seguridad Certificada ABS Quality Evaluations, Inc. Management System Certification ISO/IEC 27001:2013 Certificate Nº:48038

CYBERSECURITY MADE IN EUROPE

MUCHAS GRACIAS

Francisco Valencia
Director General
Secure&IT
francisco.valencia@secureit.es
911 196 995