ATENCIÓN A LA BRECHA: CIBERSEGURIDAD INDUSTRIAL CON KASPERSKY LAB

Como líder mundial en seguridad de IT empresarial, Kaspersky Lab desempeña un papel de liderazgo a la hora de cubrir las necesidades exclusivas de la ciberseguridad industrial.

Los ataques maliciosos contra sistemas industriales, como los sistemas de control industrial (ICS) y los sistemas de control de supervisión y adquisición de datos (SCADA), han aumentado significativamente en los últimos años.

Como los ataques Stuxnet y BlackEnergy han demostrado, una unidad USB infectada o un único correo electrónico de spear-phishing es todo lo que se necesita para que los atacantes crucen el aislamiento físico air-gap y penetren en una red aislada. La seguridad tradicional ya no es suficiente para proteger los entornos industriales frente a las ciberamenazas.

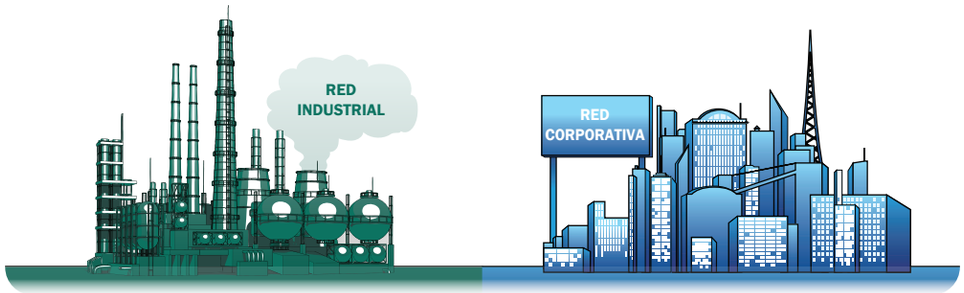
En un mundo donde los riesgos para la cadena de suministro y la continuidad del negocio se han considerado la principal preocupación empresarial a nivel global durante los últimos cuatro años, no es de extrañar que el ciberriesgo sea el interés emergente número uno.[1]

En lo que respecta a las empresas con sistemas de infraestructuras industriales o vitales, los riesgos nunca han sido tan abundantes.

La ciberseguridad industrial es diferente

Puede haber cierta superposición en las amenazas, pero hay importantes diferencias entre los requisitos de ciberseguridad de los entornos de ICS y los de carácter empresarial general.

Los entornos corporativos se centran en la protección de datos confidenciales; pero cuando se trata de sistemas industriales, donde cada minuto de inactividad o error cuenta, el funcionamiento ininterrumpido de las operaciones es la principal prioridad. Esto es lo que distingue a la ciberseguridad industrial de otros negocios, y lo que hace que sea tan importante trabajar con el proveedor de seguridad correcto.



Las prioridades de la ciberseguridad industrial de disponibilidad, integridad y confidencialidad son a menudo opuestas a las de las empresas estándar.

1 Allianz Risk Barometer (Barómetro de riesgos de Allianz), 2016.

LAS SOLUCIONES DE CIBERSEGURIDAD INDUSTRIAL DEBEN INCLUIR TRES PILARES FUNDAMENTALES:

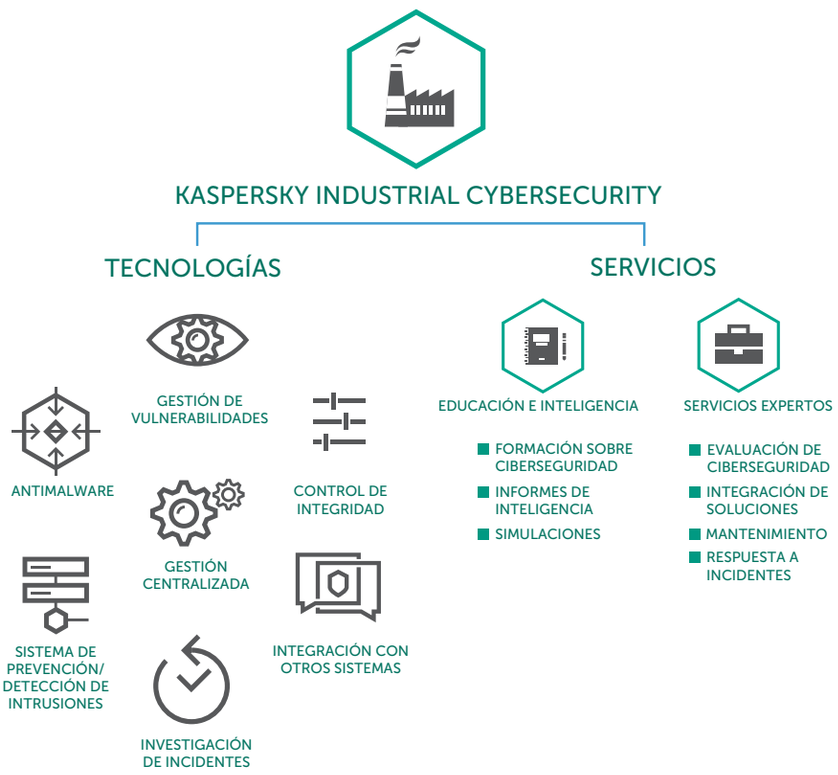
- Enfoque basado en procesos para la implementación de la seguridad
- Educación/concienciación de los empleados
- Tecnologías creadas específicamente para los entornos industriales

EL ENFOQUE DE CIBERSEGURIDAD INDUSTRIAL DE KASPERSKY LAB ES DE TIPO HOLÍSTICO:

- **Proceso:** no hay soluciones listas para su uso en la ciberseguridad industrial. Es un proceso que comienza con una auditoría, prepara a las personas para el cambio y se despliega gradualmente con una interrupción mínima.
- **Personas:** cada empleado, desde la oficina hasta la planta de la fábrica, tiene su papel en la ciberseguridad. La formación y la educación, como las del juego Kaspersky Industrial Protection Simulation (KIPS), son vitales.
- **Tecnología:** Kaspersky Lab ha desarrollado soluciones basadas en tecnologías exclusivas, diseñadas específicamente para las necesidades de la seguridad industrial. Tolerantes a fallos y sin interrupciones, pueden trabajar incluso en condiciones de aislamiento físico air-gap.

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity es una cartera de tecnologías y servicios diseñada para proteger cada capa industrial, lo que incluye servidores SCADA, paneles HMI, estaciones de trabajo de ingeniería, PLC, conexiones de red y personas, sin afectar a la continuidad operativa ni a la coherencia de los procesos tecnológicos.



A medida que aumentan las amenazas dirigidas a infraestructuras vitales, elegir el mejor consejero y partner tecnológico para proteger los sistemas nunca había sido tan importante.

Hable con nuestros expertos hoy y obtenga más información sobre el futuro de la ciberseguridad industrial.

www.kaspersky.com/ics

INTERPOL STRATEGIC PARTNER

IIC MEMBER industrial internet CONSORTIUM

MÁS PROBADO*
MÁS PREMIADO*
LA PROTECCIÓN DE KASPERSKY LAB
* kaspersky.es/top3

KASPERSKY lab