Sesión Plenaria
Comunidad de Seguridad

Ciberseguridad y Riesgo Operativo

Panel

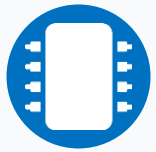
Retos de la Ciberseguridad

Cuando un director de planta duda antes de conectar un nuevo sistema, en realidad está haciendo dos preguntas distintas.

Reto 1

“¿Podemos vulnerar nuestra propia red corporativa?”

- La convergencia IT/OT multiplica los puntos de entrada: PLCs, HMIs, sensores IoT y redes corporativas ya comparten el mismo entorno digital.
- Cada dispositivo nuevo, cada acceso remoto y cada integración amplían la superficie de ataque
- **Evaluar de forma controlada de acuerdo al nivel de madurez de ciberseguridad**



Reto 2

“¿Confiamos en quién diseñó y fabricó nuestra tecnología?”

- Detrás de cada PLC, gateway o software de planta hay varios terceros: diseñador, fabricante, integrador, proveedor de firmware.
- **Tecnología diseñada específicamente para entornos OT, no adaptada de IT; y que el integrador tenga el conocimiento y la experiencia en OT para implementarla y obtener los resultados esperados.**

Un caso que confirma ambos retos a la vez

Jaguar Land Rover, agosto de 2025 — el ciberataque más costoso en la historia del Reino Unido

1 El punto de entrada

Los atacantes ingresaron a través de un proveedor externo de servicios de TI, no directamente por la red de la armadora.

2 El impacto en planta

Las líneas de producción se detuvieron por completo durante más de cinco semanas.

3 El efecto en cadena

Proveedores Tier 2 y Tier 3 quedaron bloqueados de sistemas de pedidos e inventario; algunos suspendieron operaciones.

4 El costo total

Caída de 25% en producción de vehículos del Reino Unido y más de £1,900 millones en daños; el gobierno británico emitió una garantía de emergencia por £1,500 millones.

Fuente: welivesecurity.com / Epicor, 2026 — análisis del incidente JLR

Los riesgos tienen fundamento: los datos lo confirman

Manufactura — el sector del que forma parte la industria automotriz — es hoy el vertical más atacado a nivel global.

27.7%

de todos los ciberataques globales en 2025 afectaron a manufactura — más que salud y finanzas juntas

IBM X-Force 2025

29.8%

de los intentos de ciberataque en México se concentraron en el sector manufacturero

NextGuard Insurance, 2026

+61%

aumento del ransomware contra manufactura durante 2025 a nivel global

NextGuard Insurance, 2026

20.1%

de los sistemas industriales (OT) sufrió al menos un intento de ataque con malware en el 3T de 2025

Kaspersky ICS CERT

Riesgos de la industria automotriz en Silao

Clúster automotriz de primer nivel

Ensambladora ancla y decenas de proveedores Tier 1 y Tier 2 operando en el mismo corredor logístico.

Alta interdependencia IT/OT

Líneas de producción, robótica y logística cada vez más conectadas a sistemas corporativos y a la nube.

Tecnología de múltiples orígenes

Equipos, PLCs y software integrados por distintos fabricantes e integradores a lo largo de años de expansión.

Parte de una cadena global

Un incidente local se propaga a clientes OEM (Original Equipment Manufacturer) y proveedores en cuestión de horas, no de semanas.

Tendencias OT 2026

La seguridad de OT ya es un asunto de la alta dirección

Gestión coordinada que involucre seguridad, operaciones, gestión de riesgos, cumplimiento regulatorio y liderazgo corporativo.

Autoevaluaciones más realistas y honestas

El Nivel 4 cayó del 19% al 14%, lo que demuestra que muchas empresas aún están consolidando los **pilares fundamentales: visibilidad de activos, segmentación de redes y acceso remoto seguro.**

Mayor detección de intrusiones

Incremento en el registro de incidentes: el **71% de los encuestados reportó entre una y nueve intrusion**es, un aumento significativo frente al 47% del año pasado

El tiempo de permanencia sigue representando una señal de alerta

En entornos OT, donde coexisten equipos heredados (legacy), protocolos propietarios y la necesidad de mantener la continuidad operativa las 24 horas, lo que dificulta una respuesta y remediación rápidas.

Aceleración de la presión regulatoria

El **89% de los encuestados** espera un incremento en las regulaciones dentro de los próximos cinco años, en comparación con el **66%** que lo preveía en 2025.

Fuente Informe global sobre el Estado de la Tecnología Operativa y la Ciberseguridad elaborado por Fortinet

Cinco mejores prácticas para acelerar la madurez en OT

No requiere una transformación total el primer día — requiere empezar en el orden correcto.

1 Segmentación y microsegmentación

Aislar las redes de TI y OT para evitar el movimiento lateral de las amenazas.

2 Acceso remoto seguro

Implementar **controles** estrictos para **proveedores y terceros**, eliminando los accesos persistentes o sobreprivilegiados.

3 Operaciones de seguridad integradas

Incluir a **OT en los planes de respuesta a incidentes**, alineando la ciberseguridad con las necesidades reales de producción.

4 Inteligencia de amenazas especializada

Invertir en feeds de amenazas **diseñados para protocolos industriales** y comportamientos específicos de activos OT.

5 Enfoque de plataforma unificada

Consolidar las herramientas de seguridad para **simplificar las operaciones, mejorar la visibilidad y coordinar respuestas rápidas.**

Fuente https://itwarelatam.com/2026/06/24/ciberseguridad-industrial-reporte-fortinet-2026/

Grupo BeIT BUROMC SEGURIDAD INFORMÁTICA ELIT INFRASTRUCTURE SERVICES

Gracias

Grupo BeIT

BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES