BTR CONSULTING
BUSINESS DIGITAL SOLUTIONS

PANORAMA 2025 Y PRIORIDADES 2026

AMENAZAS SOBRE INFRAESTRUCTURAS DE MISIÓN CRÍTICA

https://btrconsulting.com/

VISIÓN ESTRATÉGICA

En 2025, hemos alcanzado un punto de inflexión sin precedentes en ciberseguridad OT (Operational Technology). Durante años, la digitalización industrial fue aclamada como sinónimo de eficiencia y productividad. Pero esa misma transformación también nos expuso: habilitó accesos que los adversarios no dudaron en atravesar.

Como profesionales en ciberseguridad, hemos visto cómo el ransomware dejó de ser una amenaza aislada para convertirse en un ataque sistémico contra infraestructuras que las economías no pueden permitirse pausar. El malware industrial ganó sofisticación. Los conflictos geopolíticos invadieron entornos productivos y la inteligencia artificial, esa herramienta que promete defensa, se convirtió también en el arma más poderosa de los atacantes.

Este informe reúne datos globales, análisis regionales de América Latina y lineamientos estratégicos para hacer frente a este panorama. Pero más importante aún: sintetiza una realidad que muchas organizaciones enfrentan en silencio.

Vimos que el 50% del ransomware global ya apunta a sectores críticos. América Latina registró un incremento del 108% en ciberataques, posicionándose como "cantera" de prueba para futuras campañas. Las organizaciones comprendieron la importancia de la ciberseguridad OT, pero persisten obstáculos estructurales: un déficit severo de talento especializado, sistemas heredados imposibles de actualizar sin paralizar operaciones, y presupuestos fragmentados que no reflejan el riesgo real.

Con incidentes reales y de impacto global —Aeroflot, Jaguar Land Rover, por mencionar algunos—somos testigos acerca de cómo una brecha de ciberseguridad en entornos OT ya no es un problema tecnológico aislado, sino una amenaza para la continuidad del negocio y, en algunos casos, para la seguridad física de las poblaciones que dependen de esas infraestructuras.

Lo que queremos comunicar es claro: la verdadera defensa no reside en sumar herramientas. Reside en comprender nuestros propios controles, fortalecer los existentes, e integrar tecnología, procesos y capacidades humanas en una estrategia cohesiva, pero con sentido de negocio.

Nuestro informe aborda no sólo 10 áreas de interés, sino prioridades para 2026, que en su conjunto resumen caminos viables basados en datos y experiencia. Porque en un contexto donde actores estatales convergen con cibercriminales, y donde la IA amplifica capacidades ofensivas sin tregua, esperar no es una opción.

La resiliencia de nuestras infraestructuras críticas y la continuidad de nuestras operaciones depende de decisiones que tomemos hoy.

GASPAR POCA

PARTNER BTR CONSULTING

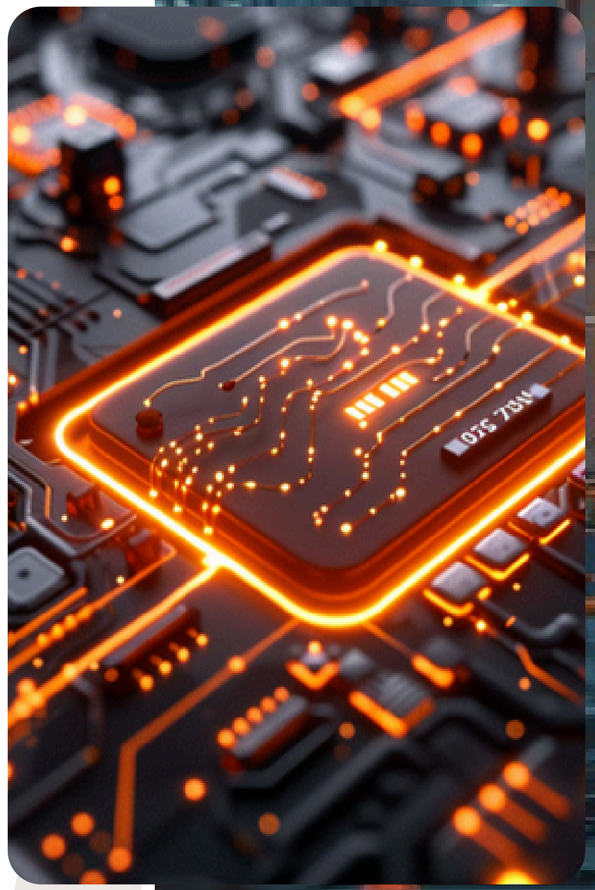
https://btrconsulting.com/

RESUMEN EJECUTIVO

El ecosistema de ciberseguridad OT (Operational Technology) atravesó en 2025 su mayor punto de inflexión. La aceleración de la digitalización industrial, sumada a la convergencia IT/OT, expuso a las infraestructuras críticas a una ola de amenazas sin precedentes: ransomware, malware especializado para ICS (Industrial Control Systems), ataques a cadenas de suministro y operaciones dirigidas por actores de Estado.

A nivel global, **el 50% de los ataques de ransomware ya se concentra en sectores críticos**, con la manufactura como el blanco más afectado (+61% de incidentes vs. 2024). En paralelo, **América Latina registró un incremento del 108% en ciberataques año contra año**, posicionándose como región prioritaria para los cibercriminales que buscan terreno de prueba para campañas futuras.

Si bien crece la inversión en seguridad OT y aumenta la centralización bajo liderazgo del CISO, persisten desafíos estructurales: déficit de talento especializado, sistemas heredados vulnerables, presupuestos fragmentados y la irrupción de inteligencia artificial en capacidades ofensivas y defensivas.



https://btrconsulting.com/

01 | CONTEXTO OT

Los entornos OT se encuentran constituidos por diferentes componentes: PLCs, SCADA y dispositivos que controlan procesos físicos en sectores como energía, manufactura, transporte y agua. A diferencia de IT, la cual se centra en la confidencialidad, OT prioriza la disponibilidad, integridad y principalmente la seguridad física.
La modernización industrial integró OT e IT en ecosistemas conectados e híbridos, desbloqueando análisis avanzados pero abriendo brechas antes impensadas. Los adversarios adaptaron su arsenal: malware ICS, exploits para sistemas legados y operaciones que combinan impacto financiero con objetivos geopolíticos.

La manufactura concentra **25.7%** de todos los ciberataques globales,

con 6.000 intentos semanales.

En 2025, cerca del **80% de las organizaciones unificó la gestión de la ciberseguridad OT** bajo el CISO.

https://btrconsulting.com/

02 | MADUREZ ORGANIZACIONAL

Las organizaciones muestran avances significativos en la formalización de procesos, pero un rezago crítico en la implementación tecnológica:

GOBIERNO

52% de las organizaciones ya asigna la responsabilidad de ciberseguridad OT al CISO, vs. 16% en 2022. Se espera que el **80% lo haga en los próximos 12 meses.**

La centralización mejora la alineación estratégica, presupuesto y gestión de riesgos, pero obliga a los CISOs a adquirir expertise profundo en procesos industriales y equipos preparados en esta materia.

PROCESOS

49% ha incrementado su nivel de madurez respecto a la inteligencia de amenazas, automatización y mejora continua.

El cumplimiento con NIST e IEC 62443 impulsa estándares comunes y mejores frameworks.

TECNOLOGÍA

Persisten limitaciones en segmentación de red, visibilidad profunda y gestión de accesos.

Este desbalance evidencia que las organizaciones avanzan más rápido en el gobierno que en despliegue técnico, abriendo una brecha crítica frente a adversarios cada vez más sofisticados.

03 PANORAMA DE AMENAZAS

Ransomware, Malware ICS y Geopolítica

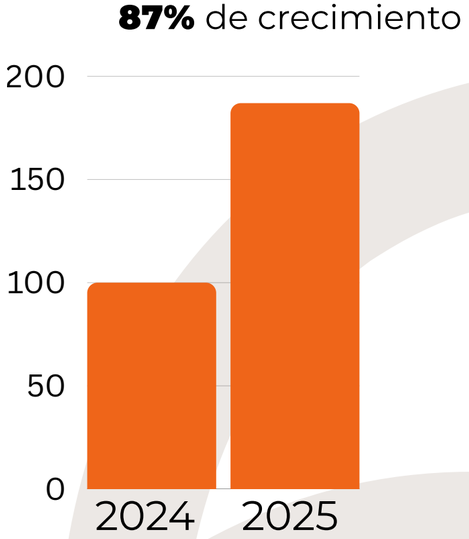
Ransomware como amenaza sistémica
El ransomware dejó de ser un riesgo aislado: ahora apunta a **infraestructuras que no pueden detenerse**, aumentando el poder de extorsión.

87% de crecimiento en ataques contra industrias en 2025.

Manufactura sigue siendo el principal objetivo por su dependencia operativa, sistemas legados y presión económica ante paradas.

El ransomware se mantiene como un riesgo estructural crítico, amplificado por la creciente automatización habilitada por la IA.

La verdadera defensa no reside en sumar herramientas, sino en comprender y fortalecer los controles existentes, integrando tecnología, procesos y capacidades de los equipos de seguridad.



https://btrconsulting.com/

04 | MALWARE ICS Y OPERACIONES DE ESTADO

El malware diseñado para ICS (Industrial Control Systems) marca un salto cualitativo, demostrando conocimiento íntimo de entornos OT.

La inestabilidad global se trasladó al ciberespacio, convirtiéndolo en un nuevo frente de confrontación. Las organizaciones enfrentan ataques dirigidos por actores estatales con objetivos geopolíticos, en un entorno marcado por la asimetría estratégica. Los regímenes de “capitalismo dictatorial” han entendido que la ciberguerra es la fase previa y permanente de cualquier conflicto físico.

Las operaciones digitales replican los objetivos de las campañas militares clásicas: incapacitar al adversario antes de cualquier movimiento físico. Se compromete infraestructura crítica, se interrumpen telecomunicaciones y se despliega desinformación para generar caos.

AEROFLOT CYBERATTACK

IT DEVASTADO, VUELOS INTERRUMPIDOS

Reuters / The Moscow Times
Este incidente se encuentra entre los ciberataques más graves que ha sufrido Rusia.

Forma parte del creciente ciclo de ciberguerra que se ha desarrollado desde que estalló el conflicto entre Rusia y Ucrania en 2022.
Dos grupos hacktivistas pro-ucranianos, Silent Crow y Belarusian Cyber Partisans, reivindicaron autoría del ataque, que ha provocado una disrupción de la flota de Aeroflot.

Silent Crow y Cyber Partisans han atacado anteriormente instituciones, entre ellas empresas estatales y registros de la propiedad, entes gubernamentales y entidades financieras, denunciando un enfoque hacktivista, sin motivaciones económicas.

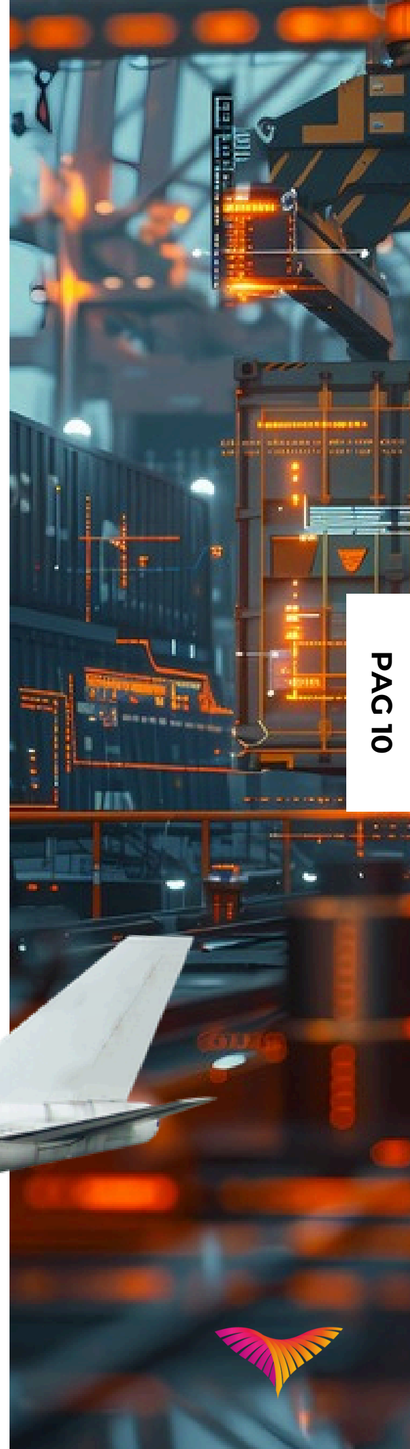
Silent Crow alega que destruyó aproximadamente **7000 servidores, extrajo entre 12 y 22 terabytes de datos** y accedió a comunicaciones internas y de pasajeros, incluida información de viajes.

https://btrconsulting.com/

Los grupos publicaron mensajes en Telegram declarando su victoria y amenazando con publicar los datos robados, incluyendo declaraciones como: **“Los datos personales de los pasajeros han volado como una alfombra mágica”.**

Aeroflot canceló aproximadamente **54 vuelos** solo el 28 de julio, y decenas más al día siguiente. La mayoría de los vuelos afectados fueron mayormente nacionales, aunque también se vieron afectadas rutas internacionales a **Minsk (Bielorrusia), Ereván (Armenia) y Taskent (Uzbekistán).**

Los servicios de las filiales de Aeroflot, Rossiya y Pobeda, también se vieron interrumpidos.



JAGUAR LAND ROVER CYBERATTACK

Lecciones aprendidas

Cada hora de inactividad puede traducirse en millones de dólares en pérdidas de producción y ventas.

Los concesionarios no pudieron registrar los vehículos nuevos, por lo tanto, los clientes no pudieron recibir sus entregas, provocando pérdidas de ingresos para JLR y su red minorista.

Una situación similar vivió Honda en 2020, cuando el ransomware “Ekans” generó el mismo impacto.

Para sortear múltiples defensas perimetrales, los atacantes utilizaron ingeniería social junto con acceso de nivel interno (cuentas legítimas).

El acceso se amplió de forma sigilosa y se mantuvo la persistencia tanto en los dominios de TI como de OT.

El colectivo de hackers «Scattered Lapsus$ Hunters» reivindicó la autoría del incidente.

Estos grupos conocidos (Scattered Spider, Lapsus$, ShinyHunters) están colaborando entre sí, contando historial de ataques contra grandes empresas minoristas e infraestructuras del Reino Unido.

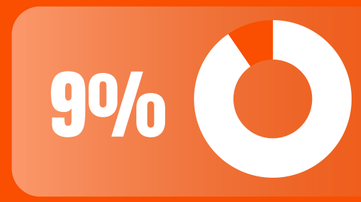
Más de 200.000 puestos de trabajo en toda la cadena de suministro se vieron amenazados. Muchos proveedores pequeños y medianos, que dependen en gran medida de los pedidos de JLR, informaron despidos, crisis o cambios a contratos.

JLR no contaba con un ciberseguro activo en ese momento, lo que significa que tuvo que absorber todos los costos.

Las estimaciones sitúan las pérdidas de JLR en USD 70M.

05 DESAFÍOS CORPORATIVOS CRÍTICOS

Brecha de talento OT
Solo 9% de los profesionales de ciberseguridad trabaja full-time en seguridad OT.



Se destaca alta rotación y competencia por talento especializado.

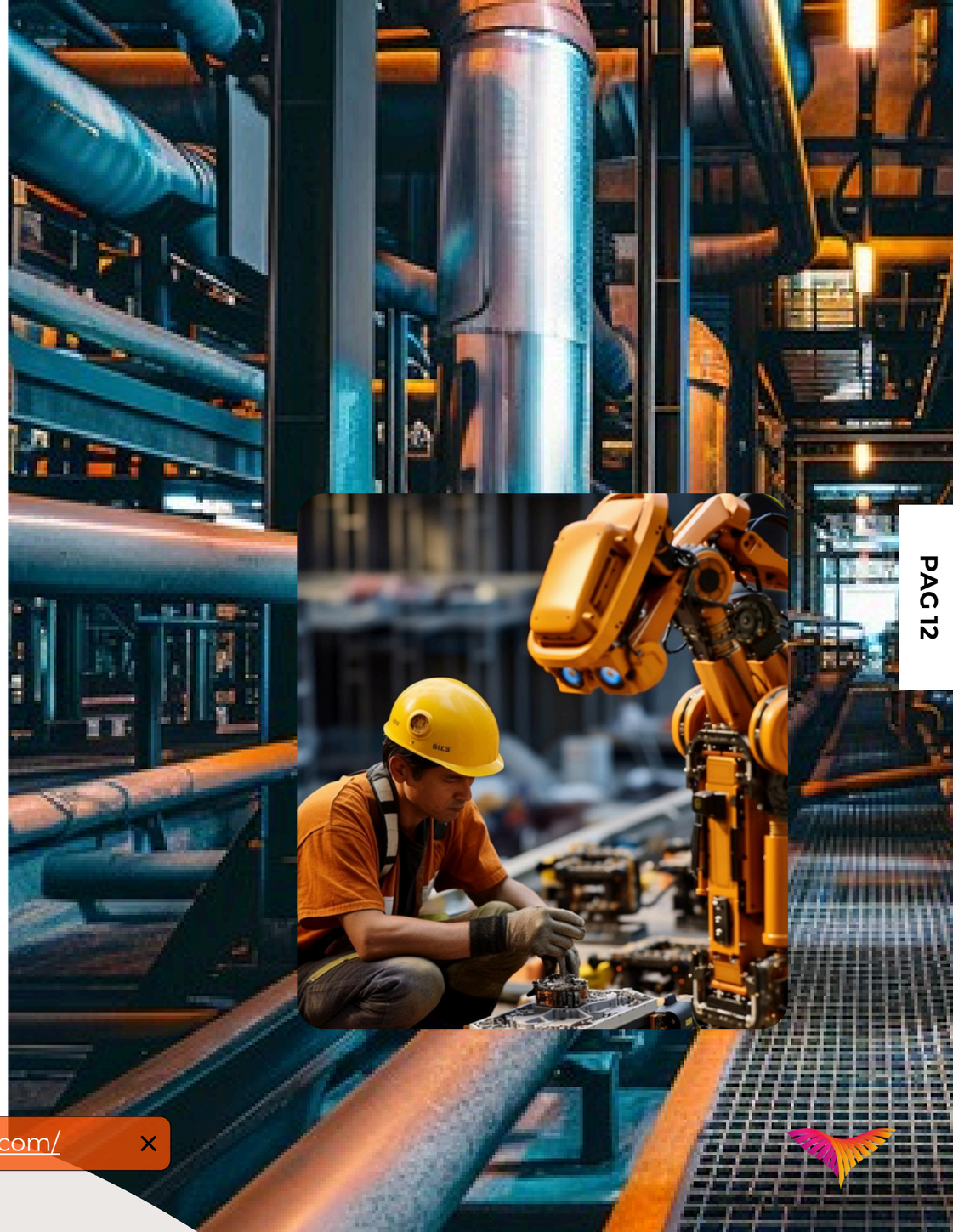
Presupuestos fragmentados
Aunque 55% aumentó la inversión, la asignación de presupuesto sigue siendo insuficiente y desalineada.

Solo 26%

cuenta con presupuesto específico para OT.

Solo 9%

destina más del 75% del presupuesto de ciberseguridad a OT.

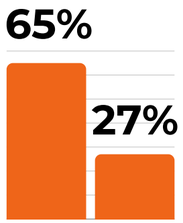


https://btrconsulting.com/

06 | CONVERGENCIA IT/OT

La falta de experiencia específica en aspectos relacionados con OT en equipos IT genera riesgos operacionales directos:

Respuestas de seguridad inapropiadas pueden causar salidas de producción o incidentes físicos.



65% cree que la ciberseguridad en entornos OT es prioridad, pero solo **27%** de los presupuestos está en manos de posiciones idóneas en el tema.

Sistemas heredados

Los entornos OT legados representan uno de los mayores vectores de riesgo.

22% de las vulnerabilidades reportadas sobre ICS (Industrial Control Systems) son explotables desde internet.

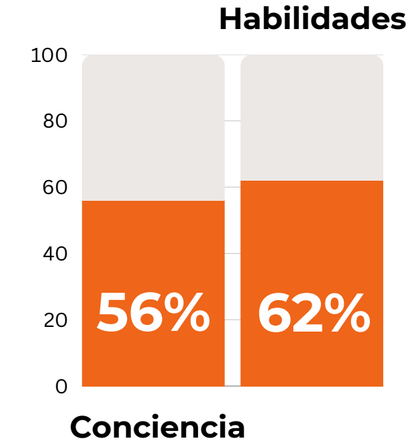
La modernización es costosa y disruptiva, pero la permanencia prolongada es peligrosa.

https://btrconsulting.com/

07 | TALENTO, CONCIENTIZACIÓN Y BRECHA REGIONAL EN LATAM

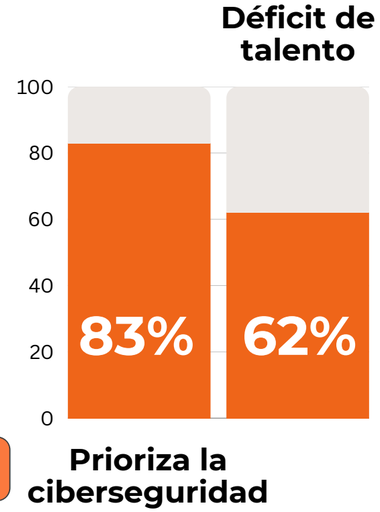
Programas de concientización insuficientes

Solo **56% implementa programas integrales de awareness** para personal en ámbitos OT.
Principales factores de brecha:
Falta de concientización del empleado (56%)
Falta de habilidades técnicas (62%)

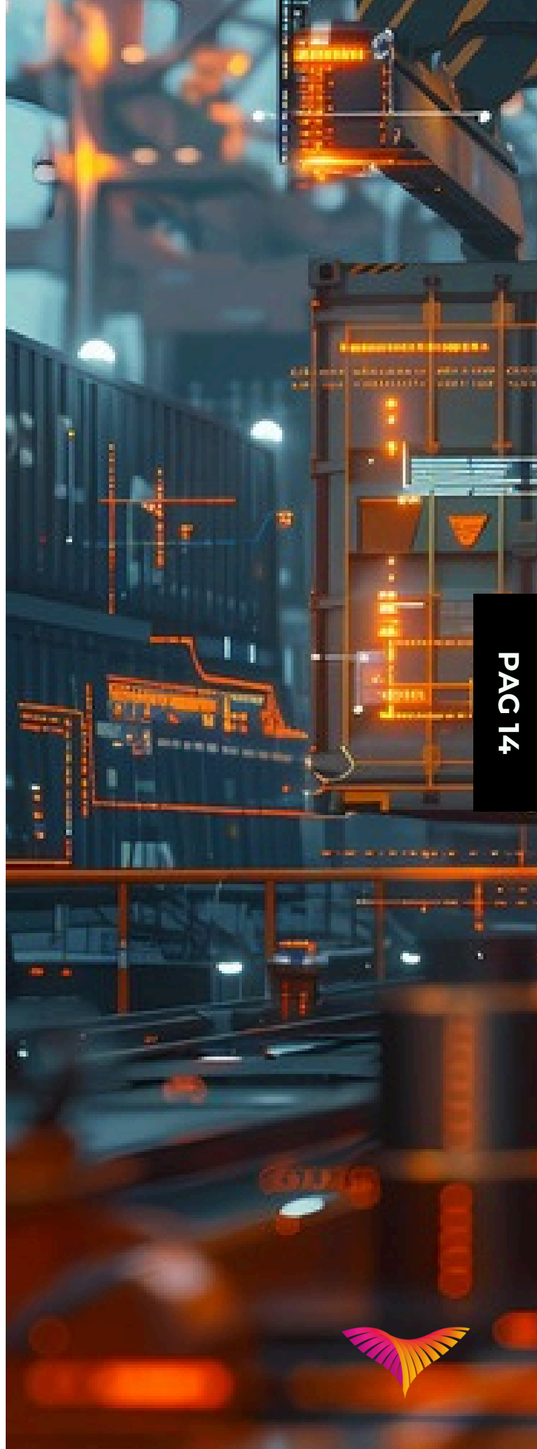


Brecha de habilidades en LATAM

Aún cuando el **83%** de los “boards” en LATAM prioriza la ciberseguridad, la región presenta una brecha más profunda que el resto del mundo: **62%** de déficit de talento, por encima de Norteamérica y EMEA.



https://btrconsulting.com/



08| INTELIGENCIA ARTIFICIAL

COMO HERRAMIENTA DE DEFENSA

Automatiza la detección, respuesta y análisis con precisión creciente:

- **84%** asegura que su implementación para la detección de amenazas incrementó la efectividad de sus controles.
- Reducción promedio de **USD 1.9 millones** en costo de brechas vs. compañías que no implementan IA.
- Reducción de **80 días** en ciclos de respuesta.
- Aporta especialmente a SOCs OT, donde la rapidez evita paradas críticas.

A MERCED DE LOS DELINCUENTES

Los adversarios la utilizan para:

- Generar malware adaptativo.
- Automatizar campañas de phishing hiperrealistas.
- Crear deepfakes para ingeniería social dirigida.
- Escalar ataques con menor esfuerzo humano.

La Inteligencia Artificial marca un punto de inflexión histórico. Lo que alguna vez fue una herramienta de optimización se convirtió en un motor central del crimen digital, impulsando el crecimiento acelerado de ataques de ingeniería social, phishing y ransomware. La automatización no sólo elevó la sofisticación de estas amenazas, sino también su velocidad de ejecución, obligándolos a reconocer que la seguridad dejó de ser una opción: hoy es estrategia.

90% de las organizaciones reconoce no estar preparadas para contrarrestar amenazas avanzadas habilitadas por IA.

09 | GOBIERNO Y RIESGOS

La IA requiere controles y marcos de gobierno específicos para OT:

- Supervisión humana obligatoria (human-in-the-loop).
- Modelos ajustados a patrones operacionales.
- Prevención de decisiones que afecten disponibilidad o seguridad física.

10| PRIORIDADES PARA EL 2026

Gobierno Unificado OT

Establecer estructuras de gobierno dedicadas con equipos especializados en OT y expertos operacionales. Esto implica fortalecer los lazos de la gestión OT y de IT tradicional, crear marcos de decisión ágiles y asegurar que la dirección técnica esté orientada a dinámicas de operaciones.

Modernización Tecnológica Acelerada

Implementar estrategias de segmentación de redes, monitoreo continuo y control de acceso granular. Esto fortalece la postura de seguridad mediante visibilidad total de dispositivos, reducción de superficies de ataque y capacidad de detección temprana de anomalías operacionales.

Programas de Concientización en OT

Diseñar entrenamientos y programas de sensibilización exclusivos para personal operacional que consideren riesgos específicos de OT, no adaptaciones genéricas de IT. Incluir protocolos de respuesta ante incidentes, identificación de amenazas y prácticas seguras en entornos de control industrial.

Retención de Talento OT

Crear estrategias de desarrollo profesional con especialización técnica profunda y carreras claras. Esto incluye certificaciones en ciberseguridad industrial, programas de mentoría y esquemas de compensación competitivos que reconozcan la escasez de expertos OT en el mercado.

Adopción de IA bajo Gobierno

Implementar inteligencia artificial con marcos de control claros, ajustados a dinámicas operacionales reales. IA para predicción de fallos, optimización de procesos y detección de anomalías.

Resiliencia de Cadenas de Suministro

Priorizar la continuidad de cadenas de suministro mediante mecanismos de evaluación continua de proveedores críticos, redundancia operacional y planes de contingencia.

CONTACTOS BTR CONSULTING:

Gaspar Poca
Partner @ BTR Consulting
E: gaspar.poca@btrconsulting.com

Rodrigo Montenegro
Partner @ BTR Consulting
E: rodrigo.montenegro@btrconsulting.com

VISITA LA WEB

FUENTES:

Fortinet – 2025 State of Operational Technology and Cybersecurity Report.
Opswat – 2025 ICS/OT Cybersecurity Budget: Spending Trends, Challenges, and the Future.
Dragos – 2025 OT Security Financial Risk Report.
KPMG – Industrial Control System (ICS) or Operational Technology (OT) Threat Landscape.
Dragos – OT/ICS Cybersecurity Report.

https://btrconsulting.com/


BTR CONSULTING
BUSINESS DIGITAL SOLUTIONS
CONSTRUIMOS UN MUNDO
DIGITAL MÁS SEGURO Y HUMANO
https://btrconsulting.com/