NEWSLETTER

grupobeit.com

BLOG DEL CEO

En un entorno donde las operaciones industriales están cada vez más interconectadas, la ciberseguridad OT (Operational Technology), se ha convertido en un pilar esencial para la continuidad del negocio...

EDICIÓN 55

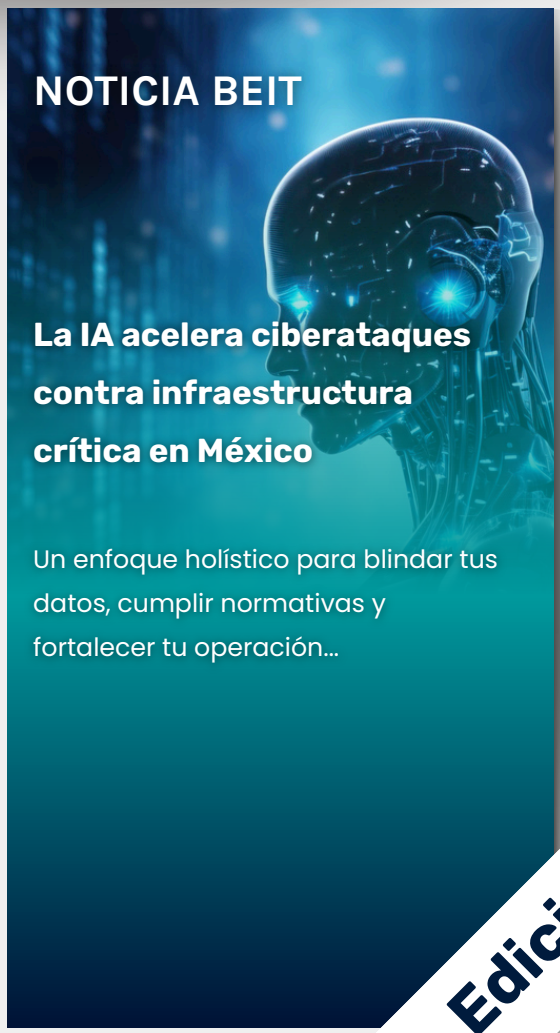
Operational Technology: proteger hoy la operación que sostiene tu negocio

Es el motor que mantiene en marcha a las organizaciones industriales...

EVENTOS

Adopción de IA y la Propuesta de Valor de Netskope: Smart IA Security
La adopción de IA empresarial avanza a un ritmo sin precedentes, convirtiéndose en un habilitador estratégico para innovación...

Protección de los datos: Estrategia de Ciberseguridad
Un enfoque holístico para blindar tus datos, cumplir normativas y fortalecer tu operación...



Edición 55

Madurez OT: Cómo evaluar, entender y fortalecer la ciberseguridad industrial

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

En un entorno donde las operaciones industriales están cada vez más interconectadas, la ciberseguridad OT (Operational Technology), se ha convertido en un pilar esencial para la continuidad del negocio. La norma IEC 62443 establece estándares para proteger los sistemas de automatización y control industrial (IACS). Ahora, ¿cómo saber en qué nivel de riesgo se encuentra una organización y qué acciones tomar?

- En este blog te explicamos tres componentes clave del proceso:
- La evaluación de madurez OT
- El análisis de riesgos
- La creación de un roadmap de ciberseguridad OT

1. Evaluación de Madurez OT: Los 8 dominios que muestran tu realidad actual

La madurez OT se analiza a través de 8 dominios, que permiten conocer el nivel de protección, visibilidad, procesos y controles con los que cuenta una organización. Estos dominios sirven como punto de partida para entender brechas, prioridades y riesgos.
Los 8 dominios típicos son:

1. Estratégico
Evaluación de riesgos, planeación de estrategias y madurez organizacional para administrar la seguridad OT.

2. Activos
Inventario, clasificación y estado de los activos OT. Incluye el ciclo de vida, criticidad y actualizaciones.

3. Riesgos
Identificación y análisis de amenazas, vulnerabilidades y su impacto sobre la operación.

4. Acceso
Gestión de usuarios, autenticación, accesos remotos y permisos dentro de los sistemas OT.

5. Gestión
Procesos, roles y responsabilidades internas relacionadas con la operación segura.

6. Operaciones
Controles operativos que incluyen monitoreo OT, UTM, SOC OT, segmentación, detección de incidentes y respuesta.

7. Organización
Estructura interna, cultura, personal capacitado, gobernanza e iniciativas de concientización.

8. Continuidad
Planes de contingencia, copias de seguridad, redundancia, recuperación y medidas para garantizar la resiliencia operativa.

¿El objetivo?
Tener un diagnóstico claro y medible del estado actual de la ciberseguridad industrial.

2. Análisis de Riesgo OT: Priorizando lo que realmente importa

Una vez comprendida la madurez inicial, el siguiente paso es calcular el nivel de riesgo al que están expuestos los activos críticos, considerando probabilidad e impacto.

El análisis de riesgo permite identificar:

- qué amenazas pueden materializarse,
- con qué probabilidad,
- y cuál sería el daño generado.
- Esto guía la toma de decisiones y las estrategias de remediación.

Criterios del análisis de riesgo

- Impacto (1 a 5)
- Insignificante
- Menor
- Moderado
- Grave
- Crítico

Probabilidad (1 a 5)

- Rara
- Improbable
- Posible
- Probable
- Muy probable

Ecuación del riesgo

Riesgo = Impacto × Probabilidad
1-4 = Bajo
5-9 = Medio
10-16 = Alto

El entregable clave es un informe de amenazas, mostrando dónde existe mayor exposición y cuáles son las prioridades de protección.

3. Roadmap OT: La hoja de ruta para madurar tu ciberseguridad
Con el diagnóstico de madurez y el análisis de riesgos, se desarrolla un roadmap progresivo, que ordena las acciones a tomar en el tiempo para fortalecer los sistemas industriales.

Fases del Roadmap

Corto plazo (0–6 meses)
- Controles iniciales, visibilidad mínima, y establecimiento de gobernanza básica.

Mediano plazo (6–18 meses)
- Estandarización, formalización de procesos y fortalecimiento de capacidades.

Largo plazo (18–36 meses)
Optimización, automatización y resiliencia operativa integral.

Niveles y propósito

Nivel	Propósito
N1-N2	Establecer controles iniciales, visibilidad y gobierno mínimo.
N2-N3	Estandarizarte, formalizar procesos y fortalecer capacidades.
N3-N4	Optimizar, automatizar y garantizar resiliencia operacional.

El roadmap permite que la organización avance de forma medible y estratégica hacia un estado de mayor madurez y seguridad.

¿ La ciberseguridad OT requiere método, visión y estrategia

Proteger sistemas industriales no es un proyecto aislado: es un proceso continuo.
La evaluación de madurez, el análisis de riesgos y un roadmap bien diseñado permiten:

- Conocer el estado real de la organización
- Priorizar inversiones y esfuerzos
- Reducir vulnerabilidades
- Aumentar la disponibilidad operativa
- Construir resiliencia a largo plazo

Si tu organización busca fortalecer su postura de ciberseguridad OT, estos tres componentes son el punto de partida ideal.

Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Edición 55

NEWSLETTER BeIT

Operational Technology: proteger hoy la operación que sostiene tu negocio

Cuando la continuidad operativa depende de la ciberseguridad

La **Operational Technology (OT)** es el motor que mantiene en marcha a las organizaciones industriales. Desde líneas de producción y plantas de energía hasta sistemas de agua y transporte, la ciberseguridad OT garantiza que los procesos críticos funcionen de manera segura y continua.

Sin embargo, el entorno operativo ha cambiado radicalmente. La digitalización, la integración entre IT y OT, el acceso remoto y el uso de tecnologías inteligentes han transformado el modelo tradicional de operación. Sistemas que antes estaban completamente aislados ahora se encuentran conectados a redes corporativas, proveedores externos y plataformas digitales. Este avance, aunque necesario para la eficiencia y la competitividad, ha abierto un nuevo y complejo panorama de riesgo cibernético.

Hoy, los sistemas industriales ya no están fuera del alcance de los atacantes. Por el contrario, se han convertido en uno de los objetivos más atractivos debido al impacto directo que un incidente puede generar en la producción, la seguridad física, la reputación de la marca y los resultados financieros.

De acuerdo con el **State of Operational Technology and Cybersecurity Report** de **Fortinet,** el 37 % de las organizaciones industriales reportaron seis o más intrusiones en un solo año, un aumento significativo frente a periodos anteriores, lo que confirma que los entornos OT están bajo presión constante. Esta tendencia no solo continúa, sino que se intensifica conforme más activos operativos se conectan a redes corporativas y externas.

OT: un riesgo distinto que exige una estrategia distinta

A diferencia de los entornos tradicionales de IT, la OT no puede detenerse fácilmente para aplicar parches, reiniciar sistemas o hacer cambios constantes. Muchas infraestructuras operan con tecnología heredada diseñada para durar décadas, no para resistir amenazas digitales modernas. Un solo incidente puede traducirse en paros no planeados, pérdidas millonarias o incluso riesgos para las personas.

El mayor desafío es que muchas organizaciones creen tener el control de su entorno OT, cuando en realidad no cuentan con una visibilidad completa de sus activos, sus interconexiones ni las verdaderas exposiciones al riesgo. Sin un entendimiento claro del entorno, cualquier decisión de seguridad se vuelve reactiva.

La nueva realidad: el riesgo no siempre se ve, pero siempre impacta

Los ataques dirigidos a entornos industriales ya no son escenarios hipotéticos. Ransomware, accesos no autorizados, movimientos laterales desde redes IT hacia OT y alteraciones en procesos críticos forman parte de una realidad cada vez más frecuente. En muchos casos, las organizaciones descubren estas brechas cuando el daño ya está hecho.

El problema no es únicamente la sofisticación de las amenazas, sino la falta de una evaluación clara del riesgo real. Sin saber qué activos existen, cuáles son críticos y dónde están las vulnerabilidades, la operación queda expuesta.

El impacto real: producción detenida y pérdidas millonarias

Cuando un ataque afecta OT, las consecuencias trascienden lo digital. El costo promedio de recuperación de un incidente de ransomware en manufactura alcanzó **1.67 millones de dólares en 2024,** con afectaciones directas a producción, logística y servicio al cliente, según Sophos.

Más aún, investigaciones de IBM señalan que una sola hora de inactividad en una línea de producción puede costar **hasta 22,000 dólares por minuto** en industrias altamente automatizadas, lo que convierte a la OT en uno de los activos más valiosos y vulnerables del negocio.

De la incertidumbre a la toma de decisiones informada

La ciberseguridad en OT no comienza con la implementación de herramientas, sino con **claridad.** Conocer el entorno operativo, entender su nivel de exposición y evaluar el impacto potencial de un incidente permite a las organizaciones pasar de la reacción a la prevención.

Cuando el riesgo se analiza en contexto, considerando la operación, la seguridad física y los objetivos del negocio, se vuelve posible priorizar acciones de manera inteligente. La protección deja de ser un gasto reactivo y se convierte en una inversión estratégica para garantizar la continuidad, cumplir regulaciones y fortalecer la confianza de clientes y socios.

Las organizaciones más maduras en ciberseguridad OT no son aquellas que implementan más tecnología, sino las que saben exactamente dónde están paradas y hacia dónde deben avanzar. Este enfoque permite construir hojas de ruta realistas, alineadas con la operación y con impacto tangible en la reducción del riesgo.

La diferencia entre reaccionar y anticiparse

Los datos demuestran que las organizaciones que entienden su nivel de riesgo toman mejores decisiones. Fortinet señala que las empresas con mayor madurez en seguridad OT reportan menos incidentes y una reducción significativa en el impacto de intrusiones, incluyendo una disminución de paros operativos que afectan ingresos, del 52% al 42%.

Este nivel de madurez no se logra por casualidad. Comienza con una evaluación clara, objetiva y alineada a la operación del negocio. Comprender el estado actual del entorno OT permite priorizar inversiones, proteger los activos más críticos y fortalecer la resiliencia operativa sin afectar la continuidad.

OT ya no es un tema exclusivo del área técnica

Hoy, la seguridad de los entornos industriales es un tema que involucra a la alta dirección. Un incidente en OT no solo afecta a ingenieros o equipos de IT, afecta a la operación completa del negocio. Por eso, contar con una visión clara del riesgo permite a líderes y tomadores de decisión hablar el mismo idioma y actuar con información confiable.

El verdadero diferenciador está en anticiparse. Entender el estado actual del entorno OT permite fortalecer la resiliencia operativa, optimizar la inversión en seguridad y proteger aquello que realmente mantiene al negocio en funcionamiento.

Conoce el estado actual de riesgo de tu organización es el primer paso para fortalecer su ciberseguridad.

Agenda una sesión con nuestro equipo.

Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Fuentes:

- Fortinet finds OT security maturity reduces attacks, as more CISOs are at the helm in 2025: Fortinet finds OT security maturity reduces attacks, as more CISOs are at the helm in 2025 - Industrial Cyber

- Fortinet 2025 State of Operational Technology and Cybersecurity Report Released: Fortinet 2025 State of Operational Technology and Cybersecurity Report Released

- 2025 OT Cyber Threat Report: 2025-OT-Cyber-Security-Threat-Report.pdf

- The State of Ransomware in Manufacturing and Porduction 2024: **Message from Sophos**

- State of CPS: OT Exposures 2025: claroty-team82-state-of-ot-exposures-report.pdf

La IA acelera ciberataques contra infraestructura crítica en México

NOTICIA BeIT

El 2 de marzo de 2026, El Economista publicó un reporte clave que confirma un punto de quiebre para la ciberseguridad en México: los ciberataques asistidos por inteligencia artificial ya están presionando directamente a la infraestructura crítica del país, incrementando la velocidad, el alcance y la sofisticación de los ataques contra sistemas industriales y operativos.

El informe se basa en el International AI Safety Report 2026, elaborado por un panel internacional de expertos en ciberseguridad, y documenta evidencia sólida del uso activo de modelos de IA para apoyar tareas típicas de ataques cibernéticos, como identificación de vulnerabilidades, automatización de intrusiones y generación de malware. En infraestructuras críticas, esto tiene un impacto inmediato: reduce drásticamente los tiempos de detección y respuesta en sistemas que no fueron diseñados para amenazas digitales modernas, como muchos entornos OT en México.

Infraestructura crítica bajo presión operativa real

El reporte destaca que sectores clave para el país como energía, manufactura, logística, servicios públicos y dependencias gubernamentales, están enfrentando una presión operativa constante, ya que los atacantes pueden ejecutar fases completas de reconocimiento y explotación en minutos o incluso segundos. En 2024, los atacantes tardaban en promedio 48 minutos en comprometer un sistema, y el caso más rápido documentado ocurrió en 51 segundos, una velocidad incompatible con los modelos tradicionales de seguridad industrial.

Además, el análisis subraya que la falta de monitoreo continuo, visibilidad de activos OT y reportes estructurados de incidentes dificulta que las organizaciones mexicanas diferencien entre fallas operativas y ataques cibernéticos reales. En contextos industriales, esta ceguera puede traducirse en paros de producción, fallas de seguridad física y afectaciones a servicios esenciales.

Un llamado directo a fortalecer OT en México

La nota es clara en su conclusión: México está altamente expuesto debido a la combinación de alta digitalización, cadenas de suministro interconectadas y entornos OT históricamente desprotegidos. Aunque el país avanza en planes y marcos normativos, como el primer Plan Nacional de Ciberseguridad anunciado para 2026, los ataques ya están ocurriendo a una velocidad superior a la capacidad de reacción tradicional.

Este contexto refuerza que la seguridad OT no puede seguir tratándose como un complemento de IT, sino como un pilar estratégico para la continuidad del negocio y la resiliencia nacional.

Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Fuentes:

El Economista – Uso de IA en ciberataques contra infraestructura crítica (México): La IA acelera los ciberataques y presiona la seguridad de la infraestructura crítica en México:

Adopción de IA y la Propuesta de Valor de Netskope: Smart IA Security

La adopción de IA empresarial avanza a un ritmo sin precedentes, convirtiéndose en un habilitador estratégico para innovación, productividad y eficiencia operativa. Sin embargo, este crecimiento acelerado también exige reforzar la seguridad, garantizar la gobernanza del dato y mantener un desempeño óptimo sin fricciones para el usuario.

Las cifras evidencian este salto exponencial. Claude Anthropic pasa de 58.3% a 90% de adopción organizacional; Microsoft Copilot avanza de 35.4% a 86.4%; y Google NotebookLM crece del 10.4% al 64.6%. A nivel de aplicaciones, ChatGPT se mantiene como la más popular con 98.6% de adopción y la categoría de IA conversacional alcanza al 99.9% de las organizaciones. Norteamérica registra el mayor dinamismo +131.2% en 54 semanas. En paralelo, el escenario de seguridad refleja nuevos desafíos: las violaciones de DLP alcanzan 2.4%, y los datos regulados participan en 57.6% de los incidentes.

Perspectiva regional

En América Latina la adopción promedio llega al 83.2%, con Brasil al frente (80.3%). México registra 65.8% de adopción y un crecimiento mensual de 3.8%, con ChatGPT como aplicación principal.

Adopción por tamaño de organización

La penetración escala con el tamaño de la empresa: small business 72.9%; mid market 91%; enterprise 95.6%; y Global 2000 98.5%, siendo la IA conversacional el caso de uso dominante.

¿Cómo responde Netskope a este contexto?

El consumo acelerado de IA, crea nuevas superficies de ataque y eleva el riesgo de fuga de información, un escenario que los enfoques de seguridad tradicionales no pueden cubrir.

Aquí es donde Netskope One AI Security se posiciona como un habilitador clave para proteger cada interacción con IA sin comprometer experiencia, velocidad ni productividad.

Su propuesta se sostiene en cuatro pilares estratégicos:

- **Seguridad integral del ecosistema de IA:** Control, protección y visibilidad en cada aplicación, agente o modelo utilizado.
- **Operación ágil desde un motor de políticas unificado:** Implementación rápida y consistente desde una sola consola.
- **Liderazgo en seguridad de datos:** DLP avanzado y protección inteligente ante fugas e interacciones riesgosas.
- **Desempeño sin fricciones:** Con NewEdge AI Fast Pass, que optimiza rutas de red hacia destinos críticos de IA para minimizar latencia y mejorar la experiencia del usuario.

Complementando esta estrategia, Netskope One AI Gateway aporta un punto centralizado de control para aplicaciones, agentes y modelos de lenguaje (LLMs), permitiendo una gobernanza consistente y escalable:

- **Unificación multi-LLM:** Políticas homogéneas para OpenAI, Gemini y Claude.
- **Eficiencia en SecOps:** Detecciones alineadas a MITRE ATLAS y OWASP Top 10 for LLMs para acelerar análisis e investigaciones.
- **Gestión y visibilidad de tráfico:** Auditoría completa de llamadas API, rate limiting y trazabilidad total.
- **Despliegue flexible:** Appliance virtual ligero para AWS o VMware ESXi, ideal para arquitecturas híbridas.

Beneficios claves para las organizaciones

Gobernanza unificada del tráfico autónomo entre agentes y LLMs, invisible para la seguridad tradicional.

- Autenticación reforzada de agentes con tokens únicos del gateway.
- Logs detallados para monitoreo, cumplimiento y análisis de uso.
- Integración con DLP, Threat Protection y AI Guardrails para políticas coherentes y profundas.

En un entorno donde las amenazas digitales evolucionan cada día y las regulaciones son cada vez más estrictas, proteger la información crítica de tu organización ya no es una opción, sino un pilar indispensable de continuidad, cumplimiento y confianza.

Te invitamos a un evento exclusivo:

Protección de los datos: Estrategia de Ciberseguridad

Un enfoque holístico para blindar tus datos, cumplir normativas y fortalecer tu operación.
Durante esta **sesión y desayuno**, presentaremos una solución diseñada para fomentar un nivel de ciberseguridad de la información robusto, alineado tanto con los requerimientos internos de cada organización como con las regulaciones establecidas por entidades gubernamentales.

Nuestra estrategia se basa en tres pilares fundamentales:

1. Compliance

Garantiza el cumplimiento normativo mediante políticas, controles y procesos que aseguran integridad, trazabilidad y apego a estándares.

2. Trazabilidad y visibilidad del Dato (Arexdata DSPM)

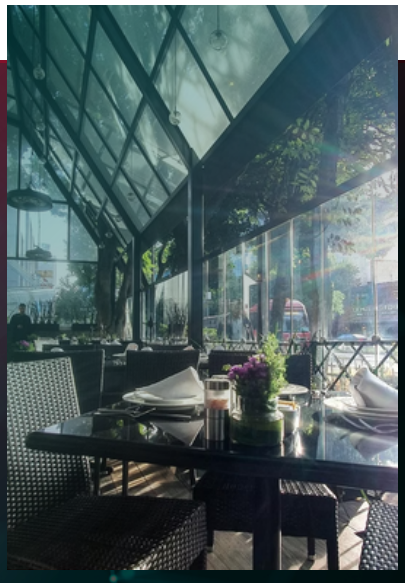
Ofrece una visibilidad profunda sobre el uso, movilidad y acceso a la información, permitiendo tomar decisiones informadas y prevenir riesgos asociados al manejo de datos.

3. Data Loss Prevention (DLP)

Previene fugas, filtraciones y uso indebido de información sensible mediante controles avanzados que protegen el ciclo de vida completo de los datos.

¿Por qué asistir?

- Comprender cómo adaptar una estrategia de ciberseguridad a las necesidades particulares de tu organización
- Integrar nuestros tres pilares para fortalecer la protección de tus activos de información
- Obtener recomendaciones prácticas para elevar tu postura de protección y cumplir normativas vigentes



Registro

Fecha y hora
Jueves 16 de abril de 8 a 11 a.m

Modalidad
Presencial Saks Barranca ubicado en: Av. Insurgentes Centro 1641, San José Insurgentes, Benito Juárez, 03900 Ciudad de México, CDMX y virtual.
Será un gusto contar con tu participación y acompañarte en la evolución de tu estrategia de ciberseguridad.

Contacto: ***+52 56 5100 8613*** ***admmarketing@buromc.com***