Grupo BeIT

NEWSLETTER

Blog CEO

Integración de la ciberseguridad en la estrategia corporativa.

Noticia BeIT

Hacker expone ubicación de todos los policías auxiliares de CDMX.

Edición 42

CISO y Ciberseguridad piezas claves.

Edición 42

ELIT INFRASTRUCTURE SERVICES

BURÖMC SEGURIDAD INFORMÁTICA

Dentro de la Gerencia de Ingeniería - Ciberseguridad, apoyamos la visión del Sistema de Gestión de la Ciberseguridad Industrial (SGCI) mediante un enfoque integral que promueve la resiliencia operativa y la innovación tecnológica. Nuestro compromiso se centra en proteger los activos críticos, incluyendo aquellos pertenecientes al personal de soporte técnico involucrado en proyectos estratégicos, asegurando que no se conviertan en vectores de riesgo dentro de la cadena de la operación tecnológica.

Este objetivo se materializa a través de nuestro CyberSOC, una plataforma de monitoreo continuo que permite:

- detectar desviaciones operativas en tiempo real.
- prevenir fugas de información y prácticas no alineadas con los estándares de seguridad.
- generar inteligencia operativa para la mejora continua de procesos.

Estas capacidades no solo mitigan riesgos, sino que también habilitan una convergencia transparente entre los entornos OT e IT, clave para la transformación digital industrial.

El mercado industrial está evolucionando hacia soluciones que integran software especializado, inteligencia artificial y gemelos digitales, permitiendo simular y optimizar procesos antes de su implementación física. Esta tendencia abre oportunidades para:

- reducir costos operativos.
- aumentar la eficiencia de los activos.
- mejorar la toma de decisiones basada en datos.

En este contexto, el CyberSOC de GrupoBeIT se posiciona como un habilitador estratégico, operando bajo un esquema de monitoreo 24/7 con tecnologías de vanguardia como machine learning, big data y análisis de comportamiento, que permiten detectar y responder a incidentes con agilidad y precisión.

GrupoBeit potencia la capacidad de escalar soluciones de ciberseguridad industrial, alineadas con los objetivos de negocio y las exigencias del mercado, impulsando:

·modelos de gobernanza tecnológica robustos.
·capacidades de respuesta ante amenazas emergentes.
·innovación continua en la protección de infraestructuras críticas.

Este enfoque empresarial no solo protege el presente, sino que construye las bases para un futuro industrial más seguro, eficiente y competitivo.

Álvaro Carrasco
GrupoBeIT
Gerente de Ingeniería

Integración de la ciberseguridad en la estrategia corporativa

Por: Elías Cedillo , Fundador y *CEO GrupoBeIT*

LLa ciberseguridad ha dejado de ser un asunto técnico para convertirse en una decisión estratégica de negocio. Gartner lo afirma con claridad: tratar la ciberseguridad como un gasto operativo es un error que puede resultar muy costoso.

Hoy, el 85% de los CEOs reconocen que la ciberseguridad es crítica para el crecimiento del negocio. No se trata solo de proteger sistemas, sino de preservar la confianza del mercado, la continuidad operativa, la reputación corporativa y la información de los clientes. En otras palabras, la ciberseguridad es una inversión directa en el valor empresarial.

Actuar es urgente e inminente, no solo por el aumento de los riesgos, sino también por la hiperconectividad entre las tecnologías IT y OT. Los directorios están exigiendo a los líderes de seguridad que aceleren su capacidad de respuesta y su alineación con los objetivos digitales. Ya no basta con ser preventivos; ahora es necesario estar un paso adelante de las amenazas actuales y futuras.

La tecnología avanza más rápido que la gobernanza. Las decisiones de adopción tecnológica —como el uso de IA generativa— se están tomando sin considerar plenamente sus implicaciones en seguridad. El Centro de Ciberseguridad presenta una guía de sistemas de gestión para la ciberseguridad industrial, donde se observa la convergencia entre marcos internacionales para la protección tanto de tecnologías de la información (TI) como de tecnologías operativas (OT).

El modelo tradicional de ciberseguridad es solo el primer paso, pero no ofrece una protección integral. Gartner advierte que los enfoques centralizados y rígidos ya no funcionan. Se requiere una hoja de ruta ágil, integrada y orientada al negocio. Y es ahí donde GrupoBeIT, junto a sus partners líderes del mercado, comienza a enfocarse: en que la implementación tecnológica esté alineada con los objetivos estratégicos del negocio, sea efectiva en todos los niveles de la organización e integradora con sus tecnologías actuales. Todo esto va desde la planeación hasta la ejecución, brindando propuestas diseñadas para potenciar el crecimiento, optimizar recursos y asegurar que cada tecnología adoptada contribuya directamente al éxito de la organización. Todo ello debe ir acompañado de una estrategia financiera y logística sólida.

Gartner propone un marco de acción concreto para los líderes empresariales y de seguridad:

- Replantear el mindset del equipo de seguridad.
- Fortalecer las relaciones con stakeholders.
- Optimizar recursos y eliminar ineficiencias.
- Comunicar el valor de la seguridad en lenguaje de negocio.
- Establecer niveles de protección alineados con operaciones, regulaciones y expectativas de socios y clientes.

Como líderes, no podemos delegar la ciberseguridad exclusivamente al área técnica. Es momento de asumirla como lo que realmente es: una decisión empresarial que impacta directamente en el valor para accionistas, clientes y empleados.

La pregunta no es si invertir en ciberseguridad. La pregunta es: ¿estamos invirtiendo lo suficiente, en el lugar correcto y con la velocidad que el negocio exige?

Referencia:

Gartner: Valor de la ciberseguridad como decisión empresarial
Gartner: Programa de ciberseguridad
Gartner: Roadmaps for Cybersecurity excertpt
Gartner: 12 ways to deliver cybersecurity business value

Panorama Global

Hacker expone ubicación de todos los policías auxiliares de CDMX.

NOTICIA BeIT

Una grave falla en los sistemas de seguridad digital de la Secretaría de SeguridadUna grave falla en los sistemas de seguridad digital de la Secretaría de Seguridad Ciudadana (SSC) ha dejado expuesta información altamente sensible de más de 28,000 policías auxiliares de la capital. La filtración, que ya circula en foros clandestinos de internet, incluye nombres completos, números de placa, rangos, géneros y, lo más preocupante, las ubicaciones exactas donde cada oficial está asignado.

El archivo, un documento de Excel de 18 MB, fue difundido por un ciberatacante identificado como "Ipzi", quien lo promocionó abiertamente en su canal de Telegram. Sin embargo, expertos en ciberseguridad advierten que no se trató de un hackeo tradicional, sino de una negligencia grave: el sistema estaba expuesto públicamente, sin contraseñas, sin captcha y sin ningún tipo de autenticación.

Este descuido ha encendido las alarmas en múltiples niveles. La base de datos permite identificar qué oficiales están asignados a instituciones estratégicas como el Aeropuerto Internacional de la Ciudad de México (AICM), el Instituto Nacional Electoral (INE) y diversas alcaldías. El riesgo no es solo institucional: los agentes podrían ser blanco de extorsiones, amenazas o incluso suplantaciones de identidad.

Ya se han reportado casos de llamadas fraudulentas en las que delincuentes se hacen pasar por mandos policiales para solicitar documentos fiscales y laborales, aprovechando la información filtrada.

La exposición de datos no fue producto de una sofisticada operación cibernética, sino de una falla básica en la protección de sistemas públicos. La SSC permitió el acceso libre a una dirección IP que contenía la base de datos, sin ningún tipo de barrera digital. Como lo describen los expertos: “la puerta estaba abierta y nadie la cerró”.

Este incidente no solo pone en riesgo la seguridad de miles de servidores públicos, sino que también socava la confianza ciudadana en las instituciones encargadas de protegernos. La falta de respuesta oficial hasta el momento agrava la preocupación: ¿cuántas otras bases de datos están igual de vulnerables?

La ciudadanía, los medios y los expertos en tecnología exigen una revisión inmediata y profunda de los protocolos de seguridad digital en todas las dependencias gubernamentales. La protección de datos no es un lujo, es una necesidad urgente en un país donde la información puede convertirse en un arma.

Referencia:

MSN

CISO y Ciberseguridad piezas claves

ELos datos son el nuevo oro, y el Chief Information Security Officer (CISO) se ha convertido en una figura clave para la supervivencia digital de las organizaciones. Su rol ha evolucionado de ser un técnico especializado a convertirse en un estratega corporativo, capaz de influir en decisiones de negocio, proteger activos críticos y anticipar amenazas emergentes, especialmente en un entorno potenciado por inteligencia artificial.

El CISO es el ejecutivo responsable de la seguridad de la información, ciberseguridad y tecnología de una organización. Su misión va más allá de prevenir ataques: debe diseñar políticas, liderar estrategias, formar equipos, reportar riesgos al más alto nivel y garantizar el cumplimiento normativo.

En México, su relevancia es crítica. En los primeros seis meses de 2022, el país sufrió 85 mil millones de intentos de ciberataques, mientras que en 2024 México recibió el aproximado de 324 mil millones intentos de ciberataques. Según el Global Threat Landscape Report 2025 México no solo es el país de Latino América con mayor cantidad de intentos de ciberataques recibidos. Instituciones Gubernamentales y diferentes sectores industria como Food & Beverage, Retail, Energía y Petróleo, han sido blanco de ataques sofisticados, lo que evidencia la urgencia de contar con líderes en ciberseguridad.

La IA ha transformado el panorama de amenazas. Según Netskope, la IA no solo es una herramienta de defensa, sino también un vector de ataque. Los CISO deben ahora anticipar ataques impulsados por IA, como el phishing automatizado o la manipulación de datos mediante modelos generativos.

La estrategia moderna exige un enfoque de “seguridad por diseño”, donde la IA se integra cuidadosamente en los sistemas, con monitoreo constante para evitar falsos positivos y omisiones críticas. Además, se requiere colaboración transversal entre áreas legales, operativas y de cumplimiento para gestionar los riesgos de forma integral.

- 65% de los CISO consideran que su rol está cambiando rápidamente.
- 59% se ven ahora como habilitadores de negocio, no solo como defensores técnicos.

En empresas Fortune 500, el CISO ya no reporta al CIO, sino directamente al CEO o al consejo directivo, reflejando su peso estratégico.

Un CISO debe tener formación en sistemas, telecomunicaciones o matemáticas, complementada con una Maestría en Ciberseguridad y certificaciones como CISSP, CISM o CRISC. Pero también necesita liderazgo, comunicación, visión de negocio y capacidad de análisis para navegar en entornos complejos y cambiantes.

El CISO ya no es solo un técnico detrás del firewall. Es un líder estratégico, un educador corporativo, un negociador de riesgos y un visionario tecnológico. En la era de la IA, su papel es más crucial que nunca: proteger, anticipar y transformar.

Referencia:

UNIR
CISO
Netskope

BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

CybrHawk Transforming Cybersecurity · netskope · vicarius · PARTNERS BeIT

SAVE THE DATE

En un entorno donde la eficiencia, trazabilidad y la experiencia del usuario son claves para la competitividad, **Field Services 2.0** se presenta como el siguiente gran paso en la evolución del soporte técnico especializado en ciberseguridad.

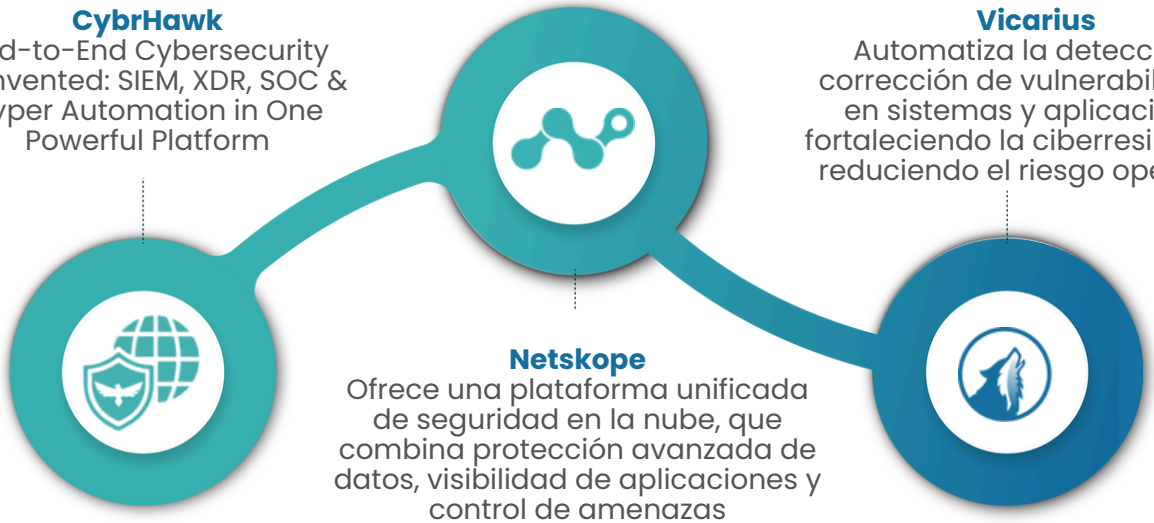
Tenemos el gusto de invitarte a una experiencia exclusiva diseñada para **los líderes** en transformación operativa y tecnológica en las organizaciones.

Fecha: Jueves, 28 de agosto
Horario: 2 – 6 pm
Sede: *La Hacienda de los Morales* ubicada en Juan Vázquez de Mella 525, Polanco, Polanco I Secc, Miguel Hidalgo, 11510 Ciudad de México, CDMX

Durante el evento junto con nuestros aliados tecnológicos descubrirás como:

CybrHawk
End-to-End Cybersecurity Reinvented: SIEM, XDR, SOC & Hyper Automation in One Powerful Platform

Vicarius
Automatiza la detección y corrección de vulnerabilidades en sistemas y aplicaciones, fortaleciendo la ciberresiliencia y reduciendo el riesgo operativo



Netskope
Ofrece una plataforma unificada de seguridad en la nube, que combina protección avanzada de datos, visibilidad de aplicaciones y control de amenazas

Esperamos contar con tu valiosa presencia.

Atentamente,

Elías Cedillo
CEO y Fundador de GrupoBeIT

Registro

Escríbenos y aparta tu lugar ó **52 56 5100 8613**

CybrHawk Transforming Cybersecurity · netskope · vicarius · PARTNERS BeIT

SAVE THE DATE

Estimado Ing. Martín Velázquez,

En un entorno donde la eficiencia, trazabilidad y la experiencia del usuario son claves para la competitividad, **Field Services 2.0** se presenta como el siguiente gran paso en la evolución del soporte técnico especializado en ciberseguridad.

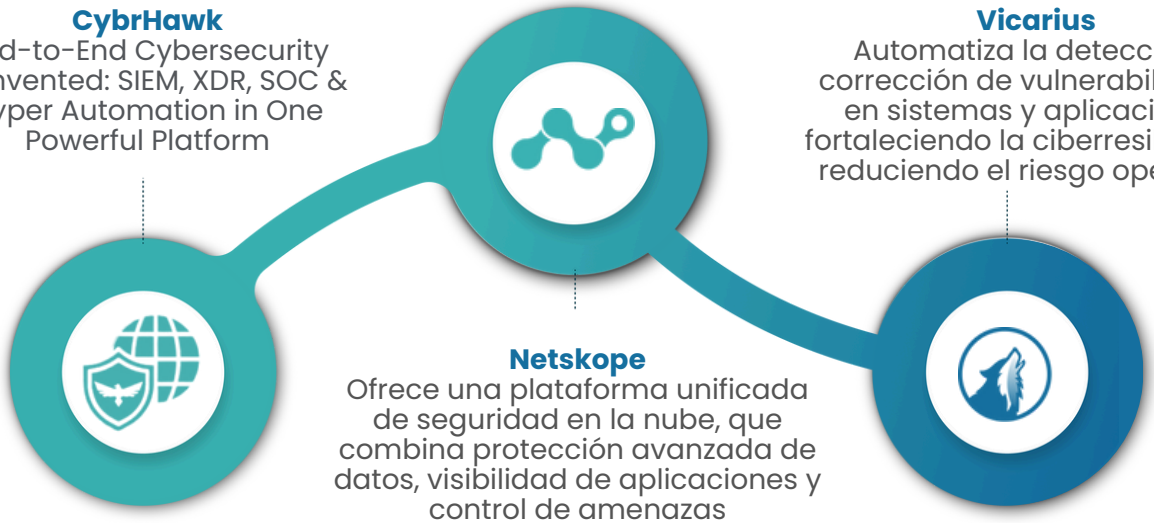
Tenemos el gusto de invitarte a una experiencia exclusiva diseñada para **los líderes** en transformación operativa y tecnológica en las organizaciones.

Fecha: Jueves, 28 de agosto
Horario: 2 – 6 pm
Sede: *La Hacienda de los Morales* ubicada en Juan Vázquez de Mella 525, Polanco, Polanco I Secc, Miguel Hidalgo, 11510 Ciudad de México, CDMX

Durante el evento junto con nuestros aliados tecnológicos descubrirás como:

CybrHawk
End-to-End Cybersecurity Reinvented: SIEM, XDR, SOC & Hyper Automation in One Powerful Platform

Vicarius
Automatiza la detección y corrección de vulnerabilidades en sistemas y aplicaciones, fortaleciendo la ciberresiliencia y reduciendo el riesgo operativo



Netskope
Ofrece una plataforma unificada de seguridad en la nube, que combina protección avanzada de datos, visibilidad de aplicaciones y control de amenazas

Esperamos contar con tu valiosa presencia.

Atentamente,

Elías Cedillo
CEO y Fundador de GrupoBeIT

Registro

Escríbenos y aparta tu lugar ó **52 56 5100 8613**