Grupo BeIT

NEWSLETTER

Blog CEO

La ciberseguridad
es una inversión
para las organizaciones.

Noticia BeIT

La brecha de ciberseguridad en el tiempo de actividad:
por qué las empresas deben cerrarla antes de que sea demasiado tarde.

Edición 45

SmartBits

Partners BeIT

Thales - "Top IAM Partner 2024"

Eventos

Webinars: Defensa Industrial: La Ciberseguridad en entornos Operational Technology (OT) al descubierto

Edición 45

ELIT
INFRASTRUCTURE
SERVICES

BURÓMC
SEGURIDAD INFORMÁTICA

La ciberseguridad es una inversión para las organizaciones.

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

La inteligencia artificial está transformando radicalmente el enfoque empresarial hacia la ciberseguridad, redefiniendo el perímetro de protección más allá de los límites tradicionales. En lugar de depender exclusivamente de firewalls, antivirus y controles de acceso estáticos, las organizaciones líderes están adoptando sistemas inteligentes capaces de anticipar, detectar y responder a amenazas en tiempo real, con una precisión y velocidad que antes eran inalcanzables.

Empresas como IBM han demostrado que la integración de IA en sus plataformas de seguridad permite reducir significativamente el impacto financiero de las filtraciones de datos, optimizando la detección de anomalías y automatizando la respuesta a incidentes. Esta evolución no solo mejora la eficiencia operativa, sino que también fortalece la resiliencia organizacional frente a ataques cada vez más sofisticados. La IA permite analizar grandes volúmenes de datos en segundos, identificar patrones de comportamiento sospechosos y activar mecanismos de defensa sin intervención humana, lo que representa un cambio de paradigma en la gestión del riesgo digital.

Fortinet, por su parte, ha incorporado algoritmos de aprendizaje automático en sus soluciones para anticipar vulnerabilidades antes de que sean explotadas. Esta capacidad predictiva convierte a la IA en un aliado estratégico, capaz de adaptarse dinámicamente a nuevas tácticas de ataque y reducir la dependencia de la intervención manual. La automatización inteligente no solo acelera la respuesta, sino que también minimiza los errores humanos, que históricamente han sido una de las principales causas de brechas de seguridad.

Sin embargo, esta revolución tecnológica también trae consigo nuevos desafíos. Se advierte sobre el uso malicioso de la IA por parte de actores criminales, quienes emplean herramientas como deepfakes, modelos generativos y minería automatizada de datos robados para vulnerar sistemas empresariales. La sofisticación de estos ataques exige una postura de seguridad más proactiva, donde la IA no solo defienda, sino también anticipe y neutralice amenazas emergentes antes de que se materialicen.

En este contexto, Palo Alto Networks proyecta que la IA será el núcleo de las futuras arquitecturas de seguridad empresarial. Su capacidad para escalar con el crecimiento exponencial de los datos, automatizar decisiones críticas y adaptarse a entornos híbridos y multicloud la convierte en una herramienta indispensable para los líderes tecnológicos.
Además, se espera que la IA juegue un papel clave en el desarrollo de nuevas técnicas criptográficas resistentes a la computación cuántica, asegurando la confidencialidad y la integridad de la información en el largo plazo.

La redefinición del perímetro empresarial ya no se basa en ubicaciones físicas ni en dispositivos específicos, sino en identidades digitales, comportamientos contextuales y análisis continuo de riesgos. La inteligencia artificial permite construir un perímetro dinámico, adaptativo y centrado en el usuario, donde cada interacción es evaluada en tiempo real y cada decisión de acceso está respaldada por datos y algoritmos. Esta evolución exige una gobernanza sólida, una ética clara en el uso de la IA y una visión estratégica que integre la ciberseguridad como un habilitador del negocio, no solo como una función reactiva.

En definitiva, la convergencia entre inteligencia artificial y ciberseguridad está redefiniendo las bases de la protección empresarial. Para los líderes en las organizaciones, este cambio representa una oportunidad única para la evolución estratégica de sus empresas, fortalecer la confianza digital y posicionarse de manera competitiva en un entorno cada vez más complejo y amenazante.

Es por eso, que, en este nuevo escenario de ciberseguridad, donde las amenazas evolucionan más rápido que nunca, **Smart Bits de GrupoBeIT** se presenta como una respuesta concreta y confiable, para quienes lideran la estrategia tecnológica de sus organizaciones. Únicamente no es solamente tecnología avanzada, sino de una **forma más inteligente y humana de proteger lo que realmente importa:** las personas, datos y la continuidad del negocio.

Con un enfoque modular y escalable, **Smart Bits** permite a las empresas:

- **Vigilar en tiempo real** lo que ocurre en su entorno digital, detectando comportamientos anómalos antes de que se conviertan en incidentes.
- **Validar identidades de forma contextual,** entendiendo el comportamiento del usuario y adaptando los controles de acceso según el riesgo.
- **Responder automáticamente a amenazas,** reduciendo tiempos críticos y minimizando errores humanos.
- **Proteger entornos híbridos y multicloud** con una arquitectura flexible y coherente.
- **Cumplir con normativas y políticas internas,** alineando la seguridad con los objetivos estratégicos del negocio.

Más allá de la tecnología, Smart Bits es un socio estratégico para los líderes que tienen claro que la ciberseguridad además de ser un tema técnico, es una pieza clave en la confianza digital, la reputación corporativa y la competitividad a largo plazo.

Referencias

IBM – Inteligencia artificial en ciberseguridad
https://www.ibm.com/mx-es/solutions/ai-cybersecurity

Fortinet – IA en ciberseguridad
https://www.fortinet.com/lat/resources/cyberglossary/artificial-intelligence-in-cybersecurity

Palo Alto Networks – Predicciones sobre IA y ciberseguridad
https://www.paloaltonetworks.com/why-paloaltonetworks/cyber-predictions

Panorama Global

La brecha de ciberseguridad en el tiempo de actividad: por qué las empresas deben cerrarla antes de que sea demasiado tarde.

NOTICIA BeIT

En muchas industrias, detener la operación por unos minutos puede significar pérdidas millonarias. Por eso, el concepto de "uptime" —mantener todo funcionando sin interrupciones— se ha convertido en una obsesión. Pero esa misma urgencia está dejando a muchas empresas vulnerables frente a ataques cibernéticos. Los hackers lo saben: si logran comprometer sistemas críticos, las compañías preferirán pagar antes que detener la producción. Así, la continuidad operativa se transforma en una debilidad que los atacantes explotan con precisión.

Gran parte del problema está en la tecnología que aún se usa en fábricas, hospitales y plantas de energía. Muchos de estos sistemas fueron diseñados hace décadas, sin pensar en amenazas digitales. Protocolos como Modbus o Profinet, por ejemplo, no tienen mecanismos de seguridad modernos. Esto permite que alguien con conocimientos técnicos pueda interceptar o modificar datos sin levantar sospechas. Y como estos sistemas están conectados a redes más amplias, el riesgo se multiplica.

Otro factor que complica la situación es la falta de comunicación entre los equipos de tecnología (IT) y los de operación (OT). Mientras unos se enfocan en proteger redes y datos, los otros solo quieren que las máquinas no se detengan. Esta desconexión crea vacíos que los atacantes aprovechan. Sin una visión compartida, es difícil detectar comportamientos extraños o responder a tiempo. La convergencia entre IT y OT es necesaria, pero requiere más que tecnología: hace falta colaboración real.

Algunas empresas ya están tomando medidas. Están segmentando sus redes, monitoreando el comportamiento de cada dispositivo y adoptando modelos de "confianza cero", donde nada ni nadie se da por seguro. También están integrando paneles que muestran tanto métricas de producción como alertas de seguridad, para que todos hablen el mismo idioma. En un caso reciente, una empresa detectó tráfico sospechoso en un protocolo antiguo y evitó un ataque que habría paralizado su operación por días.

La lección es clara: proteger la continuidad no significa ignorar la seguridad. Al contrario, integrar la ciberseguridad en cada parte del proceso es lo que realmente garantiza que todo siga funcionando. Las empresas deben dejar de ver la seguridad como un freno y empezar a verla como una inversión, porque en el mundo digital, cada segundo cuenta, y cada brecha puede convertirse en una oportunidad para quienes no tienen buenas intenciones.

Leer noticia completa: La brecha de ciberseguridad en el tiempo de actividad: por qué las empresas deben cerrarla antes de que sea demasiado tarde | Incorporado

Edición 45

NEWSLETTER BeIT

Smart Bits, lo que necesitas para mantener seguro tu negocio.

La ciberseguridad IT/OT en México ha dejado de ser una función técnica para convertirse en un habilitador estratégico para la protección empresarial. En lo que va de 2025, según **informe ¨Panorama Global de Amenazas 2025¨** elaborado por **FortiGuard Labs**, registraron más de 35 billones de intentos maliciosos en el país durante el primer trimestre, posicionándolo como uno de los más atacados en América Latina, sólo detrás de Brasil. Esta realidad exige que los líderes empresariales adopten un enfoque proactivo, donde la protección digital no solo resguarde activos, sino que habilite la continuidad operativa, la confianza del cliente y el cumplimiento normativo.

Es importante tener en cuenta que la brecha de talento en ciberseguridad se estima en 4.8 millones de profesionales a nivel global, de los cuales 1.3 millones corresponden a América Latina y el Caribe. Lo que nos dice, que, aunque existen muchas empresas que pueden brindar el servicio de ciberseguridad, no todas podrían tener el personal calificado para asistir las cuentas. Y aunque el mercado mexicano de ciberseguridad alcanzaría los 4.85 mil millones de dólares en 2029 con base a al dato brindado por Mordor Intelligence en 2024, es importante tener un aliado estratégico de ciberseguridad calificado y con certificaciones internacionales que lo respalden.

Uno de los principales desafíos es la falta de cultura organizacional en torno a la ciberseguridad. Fortinet reveló que el 73% de las organizaciones de tecnología operacional (OT) han sufrido intrusiones, y que solo el 5% tiene visibilidad completa de sus sistemas OT. IBM, por su parte, destaca que el 30% de los incidentes se originan por abuso de cuentas válidas, y que el 84% del phishing se dirige a robar credenciales mediante técnicas cada vez más sofisticadas. La solución no está solo en la tecnología, sino en construir una fuerza laboral ciber-resiliente, capaz de identificar amenazas y actuar con criterio.

Dell Technologies propone un enfoque integral que combina detección, respuesta y recuperación, utilizando inteligencia artificial para analizar telemetría y eventos de múltiples vectores de ataque. Por su parte, Schneider Electric, ofrece capas de protección para sistemas SCADA, DCS y PLC, con cumplimiento de estándares como NERC CIP y servicios de mantenimiento anual para mantener la seguridad industrial actualizada. Estas soluciones permiten a las empresas mexicanas operar con confianza en entornos híbridos y multicloud.

La protección de datos es otro pilar clave. Netskope, reconocido por Gartner como líder en SASE, ofrece una plataforma unificada que integra DLP, ZTNA, CASB y FWaaS, con visibilidad en tiempo real y protección basada en IA para entornos distribuidos. Vicarius, por su parte, automatiza la remediación de vulnerabilidades con parches, scripts y protección sin parches, reduciendo el riesgo en un 80% y el tiempo de actualización en un 60%.

GrupoBeIT junto a CybrHawk , con un enfoque especializado, ofrecen capacidades de monitoreo continuo, respuesta automatizada y análisis avanzado de amenazas, operando bajo estándares internacionales. Este tipo servicio como el SOC permite a las empresas detectar y neutralizar ataques en tiempo real, reducir el tiempo de respuesta ante incidentes críticos y garantizar la trazabilidad de eventos para auditorías y cumplimiento. Integrar un SOC como el de GrupoBeIT junto a CybrHawk, no solo fortalece las acciones ciberseguridad, sino brinda capas para estar un paso adelante ante cualquier posible evento de vulnerabilidad en los diferentes entornos.

Para este 2025, Gartner, había identificado nueve tendencias claves, entre ellas la gestión de identidades de máquinas, la resiliencia organizacional y la transformación segura impulsada por IA. En México, la falta de un plan nacional de ciberseguridad ha llevado al sector privado a adoptar esquemas de autorregulación, mientras que la rápida urbanización y penetración de internet impulsan la demanda de soluciones flexibles y escalables.

En este contexto, GrupoBeIT presentó su solución Smart Bits. Diseñada para empresas que buscan una protección básica pero efectiva; incluye auditoría de vulnerabilidades, reporte con plan de acción, firewall de próxima generación, antivirus y EDR, protección de correo, filtrado de contenido, IPS y capacitación básica en ciberseguridad. Todo bajo un modelo accesible, ideal para organizaciones que están escalando operaciones sin comprometer su seguridad.

Smart Bits no solo responde a las amenazas actuales, sino que prepara a las empresas para enfrentar los desafíos del futuro. Al combinar tecnología IT/OT con una estrategia de ciberseguridad para mantener la continuidad operativa de la empresa, ya no es una opción. Esto es lo que GrupoBeIT permite a las organizaciones fortalecer su postura de seguridad, cumplir con estándares internacionales y operar con confianza en un entorno cada vez más exigente y vulnerado. Smart Bits se posiciona como el aliado estratégico que transforma la protección en ventaja competitiva.

Referencias utilizadas:

Fortinet – Informe sobre amenazas y seguridad OT
IBM – Cyber Threat Management Services
Dell Technologies – MDR Pro Plus
Schneider Electric – Ciberseguridad industrial
Netskope – Plataforma SASE
Vicarius – Plataforma vRx
Gartner – Tendencias de ciberseguridad 2025
Mordor Intelligence – Mercado de ciberseguridad en México

Casos de ciberataques en sectores industriales

Fuentes: CNN Business (2021). Colonial Pipeline paid $4.4 million to hackers. - https://edition.cnn.com/2021/05/19/politics/colonial-pipeline-hack-payment/index.html - https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists

2010

Stuxnet
Malware altamente sofisticado

Costo de pérdida
Retraso de 2 años en el programa nuclear

Ataque dirigido
Planta nuclear de Natanz – Irán

Objetivo del ataque
Destruir los centrífugas utilizadas para enriquecer uranio, controladas por sistemas SCADA con PLCs Siemens

Repercusiones
- Más de 1,000 centrífugas destruidas
- Primer ataque cibernético conocido que causó daño físico directo

2019

Norsk Hydro - Global
Metals and Mining

Costo de pérdida
$70 millones de dólares

Ataque dirigido
Multinacional noruega de aluminio; afectó tanto IT como procesos industriales OT

Objetivo del ataque
Cifrado de datos y bloqueo de sistemas para extorsión

Repercusiones
- Interrupción en plantas de producción en Europa y América
- Operación forzada en modo manual durante varios días
- Norsk Hydro se negó a pagar el rescate, optando por restauración con respaldos

2021

Colonial Pipeline - USA
Oil and Gas

Costo de pérdida
$4.4 millones dlls en rescate

Ataque dirigido
Oleoducto de transporte de combustible más grande de EE.UU.

Objetivo del ataque
Extorsionar a la empresa

Repercusiones
- Paralización del oleoducto durante varios días
- Escasez de combustible.
- Impacto directo en la economía y la seguridad energética nacional

SmartBits

Esencial
(Protección Básica)

Ideal para empresas que buscan seguridad fundamental sin grandes inversiones

- Auditoría y evaluación de vulnerabilidades para determinar el nivel de riesgo y tu postura de ciberseguridad.
- Entrega de reporte con recomendaciones y plan de acción.
- Firewall: Firewall de próxima generación (NGFW) básico.
- Antivirus y EDR: Protección de endpoints con detección y respuesta (EDR).
- VPN Segura: Para acceso remoto cifrado.
- Gestor de contraseñas: Para mejorar la seguridad del acceso.
- Capacitación básica: Sensibilización en ciberseguridad para empleados.

Bundle Avanzado
(Protección Integral)

Para empresas con información sensible y mayor exposición a amenazas

Todo lo del Bundle Esencial, más:

- SIEM básico: monitoreo y detección de amenazas en tiempo real.
- Seguridad en correos: protección contra phishing y malware en emails.
- MFA: autenticación multifactor para accesos críticos.
- Backups seguros: copia de seguridad en la nube con recuperación rápida.
- Escaneo de vulnerabilidades: revisión periódica de seguridad.

Bundle Premium
(Máxima Protección)

Para empresas con altos requerimientos y cumplimiento normativo

Todo lo del Bundle Avanzado, más:

- SOC 24/7: centro de operaciones de seguridad gestionado.
- NOC 24/7: monitoreo de la infraestructura crítica.
- XDR: protección extendida contra amenazas en la infraestructura crítica.
- DLP (Data Loss Prevention): prevención de fuga de datos.
- Pentesting anual: pruebas de penetración para evaluar vulnerabilidades.
- Cumplimiento normativo: herramientas para cumplir regulaciones (ISO 27001, GDPR, etc.).

BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

Excecutive Partner Forum 2025

Panamá, Septiembre 2025

TOP IAM PARTNER 2024

Con mucho orgullo les informamos que **BuróMC Seguridad Informática**, ha sido distinguido por **Thales**, líder global en tecnologías de seguridad y protección de datos, con el reconocimiento al **"Top IAM Partner 2024"** por nuestra especialidad en Gestión de Identidades y Accesos.

Para nosotros, este galardón es el reflejo del compromiso, innovación y confianza que hemos construido con la colaboración estratégica hacia nuestros clientes y aliados tecnológicos como Thales.

ELIT INFRASTRUCTURE SERVICES

Grupo BeIT

Serie de Webinars

Defensa Industrial: La Ciberseguridad en entornos Operational Technology (OT) al descubierto

Te invitamos a descubrir una serie de 3 episodios donde desciframos los retos, riesgos y soluciones del entorno en la seguridad industrial. Cada episodio aborda una etapa clave en el camino hacia un entorno OT seguro, resiliente y alineado con estándares internacionales, aunque puedes unirte al que más se ajuste a tu rol o interés.

Una producción de GrupoBeIT con sus marcas BuróMC Seguridad Informática y Elite Infrastructure Services para distintos niveles de decisión y operación, con un enfoque práctico y basado en escenarios reales.

EPISODIO 1: "Fundamentos de la Defensa OT"
Fecha: Martes, 14 de octubre
Hora: 11:00 hrs.

EPISODIO 2: "Evaluando el Riesgo: Diagnóstico y Madurez"
Fecha: Jueves, 30 de octubre
Hora: 16:00 hrs

EPISODIO 3: "Estrategias de Mitigación: Diseñando la Defensa OT"
Fecha: Jueves, 6 de noviembre
Hora: 11:00 hrs.

QR de registro a todos los episodios

Contacto

+52 56 5100 8613

admmarketing@buromc.com