Grupo BeIT

NEWSLETTER

Blog CEO

La ciberseguridad
es una inversión
para las organizaciones.

Noticia BeIT

Ciberataques comprometen
embarcaciones iraníes

Edición 44

SmartBits

Partners BeIT

La dualidad de la IA:
impulsando la innovación
y protegiendo el futuro

Edición 44

ELIT
INFRASTRUCTURE
SERVICES

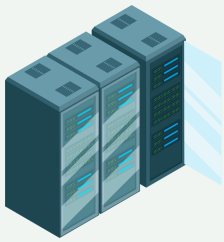
BURÖMC
SEGURIDAD INFORMÁTICA

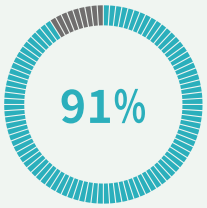
En un entorno cada vez más dinámico y desafiante, en **GrupoBeIT** entendemos la relevancia de contar con soluciones tecnológicas que se adapten a las necesidades específicas de cada industria y cliente.

En esta edición, presentamos desde nuestro equipo de Marketing el lanzamiento de nuevas soluciones integrales que combinan innovación, calidad con nuestras certificaciones en ISO 20000 y 27001 y ciberseguridad, diseñadas para acompañar junto con aliados a nuestros clientes en su camino hacia la transformación estratégica digital.

En 2024, **el 65% de las PyMEs** a nivel mundial **reportaron un aumento en ciberataques**, y para 2025 se espera una mayor adopción de nube híbrida y ciberresiliencia.

Más del 63% de las empresas planean invertir en la construcción o expansión de centros de datos, según un estudio de Datacenter Dynamics.





De las organizaciones industriales mexicanas ha sufrido incidentes cibernéticos en el último año, con pérdidas superiores a $500 mil dólares por evento

- Bundles de Ciberseguridad especialmente diseñados para proteger a las empresas PyMEs, ofreciéndoles diferentes niveles de protección digital, escalable y fácil de implementar. En México el 75% de las Pymes, tuvo al menos un ciberataque en 2024, los cuales pudieron haberse evitado con actualizaciones y medidas preventivas básicas.

- Energía y Enfriamiento para Data Centers, que optimizan el rendimiento y garantizan la continuidad operativa, con enfoque en eficiencia energética y sostenibilidad. México tiene una inversión proyectada de más de 7,000 millones de dólares en centros de datos hasta 2027, buscamos atender sus desafíos para agregar valor durante esta expansión.

- Seguridad para entornos OT (Tecnología Operacional), orientadas a fortalecer la seguridad de infraestructuras críticas industriales frente a amenazas cada vez más sofisticadas. 67.5% de las empresas mexicanas identifica la ciberseguridad como su principal riesgo operativo, especialmente en entornos OT y nube 5.

Estas soluciones han sido diseñadas con un enfoque modular y adaptable, asegurando una sencilla implementación y el mejor retorno sobre la inversión, los invito a conocerlas y prepararse para liderear la evolución tecnológica en sus organizaciones.

Saludos,

GrupoBeIT
Jennifer Morgan | Head of Marketing & Alliances

La ciberseguridad es una inversión para las organizaciones.

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

En la actualidad se ha deja de hablar que la ciberseguridad es un gasto operativo, para convertirse en una inversión estratégica clave. Las organizaciones enfrentan un entorno cada vez más complejo, donde las amenazas cibernéticas evolucionan constantemente y los activos digitales se han vuelto esenciales para la operación y competitividad. En este escenario, invertir en ciberseguridad no solo protege, sino que también genera valor, mejora la resiliencia operativa y fortalece la confianza de clientes, socios e inversionistas.

El mercado global de ciberseguridad está en plena expansión. De acuerdo con Mordor Intelligence, se estima que alcanzará los 350.23 mil millones de dólares en 2029, partiendo de 234.01 mil millones en 2024, con una tasa de crecimiento anual compuesta del 11.44%. Este crecimiento refleja una tendencia clara: las empresas están invirtiendo cada vez más en soluciones de seguridad digital, no solo como respuesta a amenazas, sino como parte integral de su estrategia de negocio. La inversión en ciberseguridad se ha convertido en un indicador de madurez tecnológica y compromiso con la sostenibilidad operativa.

Según Gartner, en este 2025 los líderes de seguridad deben demostrar cómo sus programas de ciberseguridad generan valor empresarial, más allá de la protección técnica. Esto implica una evolución del enfoque tradicional hacia una visión de resiliencia cibernética, donde la seguridad se integra en la transformación digital, la gestión de riesgos colaborativa y la toma de decisiones estratégicas. Las organizaciones que adoptan este enfoque no solo están mejor preparadas para enfrentar incidentes, sino que también pueden aprovechar la seguridad como un diferenciador competitivo.

El informe global de Fortinet sobre tecnología operacional muestra una correlación directa entre la madurez en ciberseguridad y la reducción de incidentes. Las organizaciones que alcanzaron el nivel más alto de madurez reportaron 65% menos intrusiones en 2025, en comparación con el 46% en niveles bajos. Este dato evidencia que invertir en procesos, tecnologías y talento especializado en ciberseguridad reduce el riesgo operativo, mejora la continuidad del negocio y permite una respuesta más eficiente ante amenazas.

El informe Cost of a Data Breach 2025 de IBM revela que el costo promedio global de una filtración de datos fue de 4.4 millones de dólares. Sin embargo, las organizaciones que implementaron inteligencia artificial en sus sistemas de seguridad lograron ahorros de hasta 1.9 millones. Esto demuestra que invertir en tecnologías avanzadas no solo mejora la capacidad de detección y respuesta, sino que también reduce significativamente los costos derivados de incidentes, incluyendo pérdida de reputación, sanciones regulatorias y pérdida de clientes.

Con base al estudio de forrester sobre el impacto económico total (Total Economic Impact™) de Akamai Guardicore Segmentation sobre microsegmentación muestra que se puede generar un retorno de inversión de hasta 152%, al reducir esfuerzos de gestión de incidentes, optimizar recursos y mejorar la visibilidad de red. Además, se estima un ahorro de 2.9 millones de dólares al eliminar sistemas heredados y una reducción del 33% en personal necesario para operaciones de ciberseguridad. Estos datos confirman que la inversión en seguridad digital puede ser cuantificable y rentable, especialmente cuando se implementan soluciones escalables y automatizadas.

La evidencia es contundente: la ciberseguridad no es solo una medida defensiva, sino una inversión estratégica que permite a las organizaciones reducir riesgos financieros y operativos, mejorar la reputación y confianza del cliente, optimizar recursos humanos y tecnológicos, facilitar la transformación digital segura y aumentar el retorno sobre inversión. Las empresas que priorizan la ciberseguridad están mejor posicionadas para enfrentar los desafíos del futuro, proteger sus activos más valiosos y capitalizar nuevas oportunidades en un entorno digital cada vez más competitivo. En este sentido, la seguridad deja de ser un costo y se convierte en un activo estratégico, capaz de impulsar el crecimiento, la innovación y la sostenibilidad empresarial.

BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

Panorama Global

Ciberataques comprometen embarcaciones iraníes mediante la manipulación de terminales de comunicación marítima conectadas a bases de datos MySQL

NOTICIA BeIT

Una ofensiva cibernética cuidadosamente ejecutada ha dejado fuera de servicio las comunicaciones satelitales de varias embarcaciones iraníes, afectando gravemente su capacidad de navegación y coordinación. El blanco del ataque fue Fanava Group, proveedor de servicios tecnológicos para la flota marítima sancionada de Irán, lo que sugiere una acción dirigida con fines estratégicos.

Los responsables del sabotaje lograron acceder a los sistemas mediante vulnerabilidades en los terminales satelitales iDirect Falcon, dispositivos que operaban con versiones antiguas de Linux y sin medidas de seguridad adecuadas. Una vez dentro, extrajeron información crítica almacenada en una base de datos sin cifrado, incluyendo configuraciones de red, claves de acceso y datos de telefonía IP.

Con esta información, los atacantes coordinaron un apagón masivo el 18 de agosto, interrumpiendo servicios esenciales como correo electrónico, reportes meteorológicos y comunicaciones portuarias. El ataque no solo fue destructivo, sino también meticuloso: se programó para ejecutarse en el momento más vulnerable, borrando por completo las particiones de los módems y dejando a los barcos sin posibilidad de reconexión remota.
Investigadores atribuyen la operación al grupo “Lab-Dookhtegan”, conocido por campañas anteriores contra infraestructura iraní. Desde mayo, el grupo habría estado realizando pruebas encubiertas antes de lanzar el ataque definitivo.

Este incidente pone en evidencia la fragilidad de los sistemas tecnológicos utilizados por embarcaciones sancionadas, y plantea serias dudas sobre la capacidad de Irán para mantener sus operaciones marítimas sin apoyo satelital. En un contexto de tensiones geopolíticas y comercio petrolero encubierto, la pérdida de comunicación representa un golpe significativo.

Referencia:
Cybersecuritynews

BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

Ciberseguridad: del riesgo a la resiliencia

Hoy en día, hablar de ciberseguridad ya no es solo cosa de expertos en tecnología. Las amenazas digitales se han vuelto parte del día a día de cualquier organización, sin importar su tamaño o sector. Desde ataques de ransomware hasta filtraciones de datos, los riesgos son reales y constantes. Por eso, más que blindarse, las empresas necesitan aprender a resistir, adaptarse y recuperarse. Es ahí donde entra en juego la resiliencia cibernética: una estrategia que busca mantener la operación incluso en medio de una crisis digital.

La resiliencia no significa que no habrá ataques, sino que estaremos preparados para enfrentarlos. Se trata de anticiparse, de tener planes claros, de saber cómo actuar cuando algo falla. Las empresas que entienden esto no solo invierten en firewalls o antivirus, sino que integran la seguridad en sus procesos, en su cultura y en su forma de pensar. Es un enfoque más amplio, más humano, que reconoce que los errores ocurren, pero que también se pueden superar.

Uno de los pilares de esta resiliencia es el liderazgo. No basta con que el área de TI se encargue de todo. Los directivos deben involucrarse, entender los riesgos y tomar decisiones informadas. Además, es clave que todos los colaboradores estén conscientes de su rol en la seguridad digital. Un clic en un enlace malicioso puede abrir la puerta a un ataque, pero también puede evitarse con capacitación y cultura organizacional.

El Foro Económico Mundial propone una brújula para guiar a las organizaciones en este camino. Incluye aspectos como gobernanza, procesos, tecnología, gestión de crisis y relaciones externas. No es una receta única, sino una guía flexible que cada empresa puede adaptar según sus necesidades. Lo importante es tener una visión clara y un compromiso real con la seguridad, más allá de lo técnico.

También es fundamental colaborar. La ciberseguridad no se construye en solitario. Compartir información, aprender de otros, participar en redes de cooperación puede marcar la diferencia. Iniciativas globales como la Partnership Against Cybercrime buscan justamente eso: unir esfuerzos para enfrentar amenazas que no respetan fronteras ni industrias.

En resumen, pasar del riesgo a la resiliencia es un cambio de mentalidad. Es dejar de pensar en la seguridad como un gasto y verla como una inversión en continuidad, confianza y reputación. Las organizaciones que lo entienden no solo sobreviven a los ataques, sino que salen fortalecidas. Porque en el mundo digital, la verdadera ventaja no está en evitar el problema, sino en saber cómo enfrentarlo.

En este escenario actual de constante acción por parte de los ciberatacantes, y donde los riesgos evolucionan a diario, lo que realmente marca la diferencia no es solo la tecnología, sino cómo la usamos y cómo nos preparamos. **SmartBits de GrupoBeIT** nace con esa visión: ser un aliado inteligente que acompaña a las organizaciones en su camino hacia la **resiliencia**, no solo con soluciones técnicas, sino con herramientas que se adaptan, aprenden **y** ayudan a las personas a tomar **decisiones más seguras.**

Porque al final del día, la ciberseguridad no es solo cuestión de firewalls o protocolos. Es cultura, es liderazgo, es colaboración. Es entender que detrás de cada sistema debe se existir una estructura robusta y alineada a los intereses estratégicos de nuestros clientes.

Con **SmartBits** y sus bundles, nos enfocamos en no reaccionar ante una amenaza, sino de anticiparnos, de construir confianza y de asegurar que, pase lo que pase, la operación sigue adelante. Es una **inversión más que económica**, es una inversión en tranquilidad, en reputación y en futuro. Ya no es opcional, contar **con** aliados como **GrupoBeIT** es dar un paso firme hacia una seguridad más consciente, más estratégica y sostenible.

Referencia:

World Economic Forum
IBM

SmartBits

Ciberataques y robo de información: Los despachos manejan datos sensibles que pueden ser objeto de ataques.

Pérdida de datos: Errores humanos o fallos técnicos pueden comprometer la información crítica.

Cumplimiento normativo: Las regulaciones, como la Ley Federal de Protección de Datos Personales, exigen medidas de seguridad estrictas.

Tiempo de inactividad: Fallos en la infraestructura pueden interrumpir las operaciones y generar pérdidas económicas y de reputación de marca.

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

La dualidad de la IA:

impulsando la innovación y protegiendo el futuro

Jueves, 18 de septiembre
11 am MX / 12 pm CO / 2 pm AR

Inscríbase ahora

La inteligencia artificial ofrece un enorme potencial, pero también riesgos significativos. En esta sesión, exploraremos cómo aprovechar la IA de forma segura y responsable, abordando estrategias para:

Proteger los datos dentro de los modelos de IA
Asegurar el uso de la IA generativa
Utilizar la IA para fortalecer su postura de seguridad.

Descubra cómo las organizaciones están construyendo sistemas listos para la innovación con la gobernanza integrada.

Jueves, 18 de septiembre
11 am MX / 12 pm CO / 2 pm AR

Inscríbase ahora

¿No puede asistir en esta fecha?
Regístrese y le enviaremos el enlace para ver la grabación después.

Speakers

Euriel Gómez
Senior Solutions Engineer
Netskope

Vicente Monarque
Solutions Engineer
Netskope