Grupo BeIT

NEWSLETTER

Edición 50

ELIT INFRASTRUCTURE SERVICES

BURÖMC SEGURIDAD INFORMÁTICA

Introducción

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

Al acercarnos al cierre de este 2025, quiero tomar un momento para agradecer profundamente el camino que hemos recorrido juntos. Este año ha sido de evolución, consolidación y logros extraordinarios para nuestra organización, y nada de ello habría sido posible sin el compromiso, la visión y la pasión que cada colaborador y cliente aportó día con día. En nombre de quienes conformamos Grupo BeIT, Elit Infrastructure Services y BuróMC Seguridad Informática, les deseo que estas fiestas estén llenas de alegría, descanso y momentos significativos con sus seres queridos.

Este año marcó un punto de inflexión para nuestros servicios y soluciones de ciberseguridad. Fortalecimos nuestra oferta de Field Services 2.0, logrando mayor precisión operativa, tiempos de atención más eficientes y una cobertura que hoy nos posiciona como aliado estratégico en la continuidad de negocio de nuestros clientes. Nuestro equipo demostró, una vez más, que la excelencia tecnológica y personal capacitado, va de la mano de un servicio cercano y confiable.

Con el lanzamiento de Smartbits, logramos pasos firmes hacia una protección integral para mid-market y enterprise del país. Gracias a la innovación conjunta con nuestros partners líderes en ciberseguridad y al talento de nuestros especialistas, logramos implementar arquitecturas más robustas que permitieron una visibilidad integral de los entornos tecnológicos, incrementando la capacidad de reacción y prevención ante amenazas. Este avance no solo impulsó la eficiencia de nuestros clientes, sino que reforzó la seguridad de infraestructuras críticas en múltiples sectores.

Este también fue un año sobresaliente para nuestras iniciativas en OT (Operational Technology). La interconexión entre sistemas industriales y entornos digitales trajo consigo desafíos complejos, pero me enorgullece decir que hemos dado soluciones a gran escala que hoy protegen procesos esenciales. Las prácticas y metodologías desarrolladas por nuestros equipos han elevado el estándar de seguridad en plantas, fábricas y entornos operativos donde la protección no admite margen de error.

Por su parte, nuestra solución de Ethical Hacking contribuyó directamente a crear ecosistemas digitales más seguros y anticiparnos a riesgos emergentes. Este trabajo se vuelve aún más crítico si consideramos que, solo en el primer trimestre de 2025, México enfrentó más de **35,200 millones de intentos de ciberataque,** lo que equivale a **más de 270 mil ataques por minuto,** posicionando al país como **el segundo más atacado de América Latina.**

En este contexto, nuestro equipo ejecutó pruebas de penetración y análisis de vulnerabilidad, los cuales permitieron a nuestros clientes elevar significativamente su postura de seguridad y mitigar riesgos antes de que pudieran materializarse. Nuestro trabajo en esta disciplina seguirá siendo un pilar estratégico sosteniendo la confianza de nuestros clientes.

Mirando hacia el 2026, tengo la certeza de que nos esperan nuevas oportunidades de crecimiento e innovación. Continuaremos robusteciendo nuestros servicios y soluciones, ampliando horizontes y apostando por tecnologías que marquen un verdadero impacto en la seguridad y resiliencia de las organizaciones. Sin duda, este nuevo año será un espacio para construir, mejorar y seguir avanzando juntos.

Gracias por ser parte de esta historia. Les deseo unas felices fiestas y un 2026 lleno de éxito, salud y grandes logros.

Con gratitud y compromiso,
Elías Cedillo
CEO

Ciberseguridad: el mejor cierre para tus metas corporativas

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

Durante 2025, hasta el 8 de diciembre, la **ciberseguridad** se consolidó como el mejor cierre para las metas corporativas, porque dejó de ser un conjunto de herramientas aisladas y pasó a ser una **capacidad estratégica integrada** en la gobernanza, operación y la innovación del negocio. El aumento sostenido del gasto en seguridad reflejó que los directorios y los equipos ejecutivos respondieron a un entorno de amenazas persistentes, a la expansión de la nube híbrida y a la adopción acelerada de IA generativa.

Las empresas que trataron la seguridad como **ventaja competitiva** alinearon inversiones para proteger datos e identidades, modernizar operaciones de seguridad y reforzar la continuidad, y observaron una mejora tangible en la confianza del mercado y en la resiliencia operativa. El **marco de cinco pasos promovido por IBM para asegurar la IA** —proteger datos, modelos, uso, infraestructura y gobernanza— se convirtió en una referencia práctica, al tiempo que IDC señaló el doble filo de la IA: simplificará procesos defensivos y, a la vez, potenciará ataques cada vez más sofisticados, lo que exige plataformas unificadas y controles sólidos sobre riesgos de GenAI y privacidad.

En paralelo, Microsoft reforzó la disciplina de **seguridad por defecto** y las operaciones seguras en Latinoamérica con su Secure Future Initiative, subrayando que elevar el estándar mínimo (MFA, reducción de aplicaciones obsoletas y protección de identidades) aporta beneficios inmediatos cuando la seguridad se integra desde el diseño.

La fotografía operativa de 2025 mostró con claridad los frentes prioritarios. El **abuso de cuentas válidas** se mantuvo como el punto de entrada preferido por los atacantes, y el phishing se consolidó como vector dominante, con un aumento de correos que entregan infostealers y con una presión constante sobre los programas de higiene de identidad y la gestión de credenciales.

En los sectores críticos, las **vulnerabilidades no parcheadas** impulsaron más de una cuarta parte de los incidentes, un indicador que evidenció la necesidad de acelerar el ciclo de parcheo y mejorar la visibilidad de la exposición. Estas observaciones, derivadas del X-Force Threat Intelligence Index 2025, se vieron reforzadas por la experiencia regional que reportó Microsoft en su defensa digital, con ransomware y phishing creciendo en Latinoamérica, confirmando que la identidad y las vulnerabilidades son los ejes donde el cierre de año debía ser más firme.

La respuesta de la industria en 2025 estuvo marcada por **automatización y consolidación.** Las organizaciones que unificaron su centro de operaciones con telemetría de endpoints, identidades, correo, datos y nube bajo **XDR/SIEM** con IA lograron reducir los tiempos de detección y contención, y elevaron la consistencia de sus decisiones a través de lagos de datos de seguridad y de una inteligencia de amenazas más dinámica.

Fortinet planteó para CEOs, CIOs y CISOs imperativos de liderazgo que se observaron durante el año: **transformar la seguridad en ventaja competitiva,** incorporar la gestión de riesgos en el corazón de la gobernanza, invertir en Zero Trust y análisis predictivo, promover una cultura de seguridad transversal y construir resiliencia con continuidad y recuperación planificadas.

Un hito complementario fue la creciente responsabilidad ejecutiva sobre la seguridad de entornos **OT**; el traslado de la responsabilidad hacia el CISO/CSO y la alta dirección se asoció con mayor madurez y menor impacto de intrusiones cuando OT se priorizó, lo que encaja con la visión de convergencia IT/OT bajo modelos de segmentación y control.

Durante 2025 también se registraron lecciones concretas en **gestión de vulnerabilidades y cadena de suministro**. Dell publicó múltiples avisos de seguridad sobre firmware y BIOS en el segundo semestre, recordando que la superficie de riesgo incluye microcódigo, componentes de terceros y dependencias de hardware, y que el ciclo de actualización debe ser parte del plan de continuidad.

La telemetría de plataformas de administración remota (iDRAC, RACADM) y la disciplina de parcheo alineada a criticidad y contexto fueron clave para sostener la disponibilidad. En esa línea, IBM demostró internamente que la **priorización de vulnerabilidades guiada por IA**, reduciendo alertas, identificando riesgos reales que quedaron invisibles bajo enfoques puramente CVSS y acelerando la remediación hacia lo que los adversarios explotan de forma activa, es indispensable.

Este tipo de capacidades, combinadas con **pruebas de restauración de copias y simulacros de incidente,** se convirtieron en prácticas de cierre esenciales: auditar accesos y permisos, elevar MFA resistente al phishing, aplicar parches críticos en 30 días como estándar y entrenar la respuesta operativa.

De cara a 2026, las organizaciones deben consolidar la seguridad como **plataforma unificada** y extender su alcance a los objetivos ESG (Environmental, Social and Governance), la privacidad y la sostenibilidad, conectando las métricas de ciberresiliencia con la agenda de confianza digital del negocio.

La IA simplificará tareas de seguridad y permitirá que más equipos participen en protección con asistencia inteligente, pero también elevará el listón: se requerirá **gobernanza específica de GenAI,** controles sobre el uso de PII, mejor gestión de terceros y auditoría integral.

La arquitectura **Zero Trust** se afianzará como estándar operativo de acceso, con segmentación dinámica, privilegios mínimos y señales de riesgo en tiempo real para autorizar o bloquear, y los SOC evolucionarán hacia operaciones impulsadas por IA con datos de seguridad, reglas analíticas más ricas y automatización de contención que reduzca el tiempo medio de respuesta a minutos.

Microsoft seguirá ampliando capacidades en Defender y Sentinel para un SecOps unificado, mientras Fortinet profundizará la automatización y el análisis predictivo; las compañías adoptarán MFA resistente al phishing, gestión de privilegios en endpoints y cobertura de exposición externa como requisitos mínimos.

La **gestión de vulnerabilidades** en 2026 migrará definitivamente de la clasificación por severidad a la **priorización por riesgo explotable,** apoyándose en IA para correlacionar telemetría, enriquecer contexto y automatizar la aplicación de parches y mitigaciones, incluida la capa de firmware y microcódigo.

Fabricantes como Dell mantendrán ciclos de actualización periódicos, y el gobierno corporativo tendrá que sostener la coprotagonía de **OT** con exigencias de visibilidad y segmentación IT/OT, responsables ejecutivos claros y métricas de impacto.

Para que la seguridad sea un trampolín hacia los objetivos de 2026, será necesario ejecutar una **hoja de ruta en dos trimestres:** consolidar Zero Trust e IAM con inventario de identidades, acceso condicional y privilegios mínimos; unificar telemetría y analítica en **XDR/SIEM** con un lago de datos y procesos de borrado seguro y auditoría vinculados a ESG; y adoptar priorización de vulnerabilidades por riesgo con flujos de parcheo automatizados y con indicadores de tiempo a remediación.

Medir será crítico para sostener la coherencia ejecutiva. Cerrar 2025 con tiempos medios de detección y contención por debajo de cuatro horas y aspirar en 2026 a menos de 60 minutos con automatización y XDR es coherente con el nivel de madurez observado en organizaciones líderes.

La cobertura de MFA sobre cuentas humanas y de servicio debe superar el 95 % al terminar 2025 y alcanzar el 100 % con FIDO2 en 2026 para neutralizar el abuso de credenciales. El cumplimiento de parches críticos en 30 días por encima del 90 % al cierre de 2025 deberá mejorar hacia más del 95 % en 14 días durante 2026, cuando la priorización sea guiada por riesgo y la automatización reduzca la fricción.

En entornos OT, el impacto de intrusiones se reducirá año con año si la responsabilidad ejecutiva se mantiene y la segmentación limita el movimiento lateral, con un objetivo razonable de reducción acumulada del 40 % para 2026.

Estos indicadores, acompañados de ejercicios regulares de continuidad y simulaciones de ataque, permitirán que la seguridad siga siendo un **habilitador de ingresos, reputación y expansión con IA,** en lugar de un costo defensivo.

El cierre de 2025 demuestra que la **ciberseguridad funciona como ventaja competitiva** cuando se integra en la gobernanza, se centra en identidades y vulnerabilidades y se apoya en automatización y datos para decidir más rápido y mejor.

La proyección para 2026 exige sostener esa disciplina con plataformas unificadas, Zero Trust operativo, SOC con IA y métricas conectadas a ESG y privacidad. Las organizaciones que mantengan el foco en estos pilares no solo cerrarán con seguridad sus metas corporativas, sino que abrirán con solidez el ciclo siguiente, con la seguridad al servicio del crecimiento y de la confianza digital.

Fuentes y enlaces:

- IBM — Tomar decisiones inteligentes de gasto en ciberseguridad en 2025
- IBM — Soluciones de ciberseguridad empresarial
- IBM — X-Force 2025 Threat Intelligence Index
- IBM — Cómo IBM Concert está redefiniendo la ciberseguridad y la operación de TI
- Fortinet — Ciberseguridad en el 2025: seis imperativos de liderazgo para CEOs, CIOs y CISOs:
- Fortinet — Informe OT 2025
- IDC — FutureScape: Security & Trust 2025 (eBook, previsiones a 2026):
- Microsoft — Microsoft Defender: soluciones de ciberseguridad y SOC con IA:
- Microsoft — La creciente importancia de la ciberseguridad en América Latina (SFI)
- Microsoft Learn — Centro de seguridad, Zero Trust y SecOps:
- Dell Technologies — Mes de concienciación de ciberseguridad y evaluación de ciberresiliencia:
- Dell — DSA-2025-211 (avisos de seguridad, IPU/firmware):
- Dell — OpenManage iDRAC Tools (RACADM)

México y los ciberataques en fechas decembrinas

NOTICIA BeIT

Las celebraciones decembrinas, que incluyen Black Friday, Cyber Monday y Navidad, se han convertido en el momento más crítico para la **ciberseguridad en México.** Durante estas fechas, el incremento en las compras en línea y en las transacciones digitales genera un escenario ideal para los ciberdelincuentes, quienes aprovechan la urgencia y el volumen de operaciones para lanzar **ataques masivos.** Según datos recientes, los ciberataques se disparan hasta un **67%** en este periodo, lo que convierte a la temporada en una de las más riesgosas del año.

Los informes de empresas líderes en seguridad, como Fortinet, revelan que las campañas maliciosas se intensifican durante estas semanas, con tácticas que incluyen phishing, ransomware y ataques a dispositivos móviles. El objetivo principal es robar **credenciales bancarias y datos personales,** aprovechando que los usuarios están más dispuestos a interactuar con enlaces y aplicaciones que prometen descuentos y ofertas. Esta dinámica convierte la Navidad y las promociones previas en un terreno fértil para los **fraudes digitales.**

El impacto no se limita a los consumidores. Las **empresas mexicanas,** especialmente aquellas que dependen del comercio electrónico, enfrentan un aumento significativo en intentos de intrusión y secuestro de datos. Sophos advierte que incluso sectores industriales sufren ataques orientados a interrumpir operaciones en plena temporada alta, afectando la disponibilidad de productos y servicios esenciales para las celebraciones. La presión por cumplir con la demanda navideña provoca que muchas organizaciones descuiden medidas básicas de protección, lo que incrementa su vulnerabilidad.

Los delincuentes digitales también apuntan a los **dispositivos móviles,** aprovechando que los usuarios realizan compras rápidas desde sus teléfonos. En países como México y Colombia se reporta una oleada de ataques mediante aplicaciones falsas y enlaces fraudulentos que circulan en redes sociales y servicios de mensajería instantánea. El objetivo es claro: explotar la urgencia y la confianza que caracterizan a las compras navideñas para obtener acceso a cuentas y datos sensibles.

Ante este panorama, **Grupo BeIT**, como socio estratégico en ciberseguridad para grandes empresas mexicanas, recomienda extremar precauciones durante las fiestas decembrinas. Para ello, compartimos **cinco puntos clave** que pueden ayudarte a prevenir incidentes y evitar formar parte de las estadísticas de ciberataques en esta temporada. La época navideña, que debería ser sinónimo de celebración y tranquilidad, se ha convertido en un periodo crítico para la **seguridad digital**.

¨La seguridad digital no depende únicamente de las tecnologías implementadas, sino también del factor humano, que debe desarrollar resiliencia y hábitos sólidos para proteger su información personal frente a las crecientes amenazas¨

Fuentes y enlaces:

- https://www.segurilatam.com/seguridad-por-sectores/infraestructuras-criticas/proteccion-de-infraestructuras-criticas-durante-el-mundial-2026-en-mexico_20251111.html
- https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/es_la/threat-landscape-report-2025.pdf
- sophos-state-of-ransomware-in-manufacturing-2025.pdf
- Los ciberataques se disparan un 67% en Black Friday, CyberMonday y Navidad: CyberLideria MGZN
- Oleada de ciberataques sacude la Navidad: delincuentes digitales ponen en la mira cuentas y móviles de usuarios en Colombia | ACIS

Edición 50

NEWSLETTER BeIT

México y ciberataques para diciembre

México cerró 2024 como uno de los países más hostigados por la **actividad cibercriminal en América Latina** y entró a 2025 con señales claras de una escalada sostenida. El **informe global de amenazas** registró **324 mil millones de intentos de ciberataques** en el país durante 2024, cifra alimentada por el uso intensivo de **inteligencia artificial**, automatización y mercados de acceso inicial a redes; a la par, el escaneo activo del ciberespacio alcanzó récords, con cerca de **36 mil sondeos por segundo**, consolidando un entorno de riesgo que desborda las defensas tradicionales tanto en el sector privado como en el público. En el primer trimestre de 2025, el volumen acumulado ya superó los 35.2 mil millones de intentos —casi 272 mil por minuto—, con México como el segundo país con mayor asedio en la región, solo detrás de Brasil; la lectura transversal subraya la combinación de presión operativa, brecha de talento y fragmentación de herramientas como factores que elevan la exposición corporativa.

La dinámica de amenazas en 2025 mantuvo al phishing como **vector dominante**, con reportes que indican un promedio de **59 millones de ciberataques** diarios en el país y señalan a los sectores de **telecomunicaciones y financiero** entre los más afectados. El incremento del tráfico de Internet en México **—23 % en el primer trimestre—** amplificó la superficie de ataque y la frecuencia de campañas de **ingeniería social** capaces de derivar en robo de credenciales y toma de cuentas, con tasas de éxito que siguen descansando en el error humano y la respuesta impulsiva ante mensajes con urgencia o recompensas aparentes. Este patrón se combina con **kits de explotación mercantilizados** y malware de robo de información, cuyo registro de sistemas comprometidos se disparó **500%**, habilitando el comercio subterráneo de credenciales y el acceso lateral a entornos corporativos, incluidos servicios en la nube y **protocolos industriales sensibles.**

La dinámica de amenazas en 2025 mantuvo al phishing como **vector dominante**, con reportes que indican un promedio de **59 millones de ciberataques** diarios en el país y señalan a los sectores de **telecomunicaciones y financiero** entre los más afectados. El incremento del tráfico de Internet en México **—23 % en el primer trimestre—** amplificó la superficie de ataque y la frecuencia de campañas de **ingeniería social** capaces de derivar en robo de credenciales y toma de cuentas, con tasas de éxito que siguen descansando en el error humano y la respuesta impulsiva ante mensajes con urgencia o recompensas aparentes. Este patrón se combina con **kits de explotación mercantilizados** y malware de robo de información, cuyo registro de sistemas comprometidos se disparó 500%, habilitando el comercio subterráneo de credenciales y el acceso lateral a entornos corporativos, incluidos servicios en la nube y **protocolos industriales sensibles.**

Diciembre, por su naturaleza transaccional y emocional, concentra el mayor número de **fraudes digitales** en México. El incremento en las compras en línea, la entrega de aguinaldos y la saturación informativa crean condiciones óptimas para ataques que explotan la urgencia y la confianza automática. Fuentes especializadas y autoridades de protección al usuario documentan la **temporada navideña** como la más crítica del año, con repuntes de estafas de paquetería que crecen a **triple dígito** y campañas de suplantación bancaria orientadas a la "liberación" de depósitos o a la resolución de supuestos cargos no reconocidos; este panorama se traduce en **pérdidas multimillonarias** y compromete tanto las finanzas personales como la **reputación de las marcas involucradas,** en especial aquellas con operaciones de comercio electrónico, logística y atención al cliente. Expertos han advertido que durante la entrega de aguinaldos aumenta la eficacia de los falsos enlaces bancarios y que una proporción relevante de usuarios hace clic y comparte datos sin verificaciones elementales; este comportamiento, aunado a la expansión de técnicas de deepfake de voz y sitios fraudulentos, eleva la tasa de conversión de los atacantes en el último mes del año.

La sofisticación de las campañas decembrinas se refleja en **tres modalidades** con impacto directo en organizaciones y clientes. Primero, el **fraude de paquetería "fantasma"**, que simula retenes de entrega mediante SMS y WhatsApp, solicita pagos mínimos o autenticación con datos bancarios y utiliza marcas legítimas para conferir credibilidad; los reportes anuales muestran incrementos de **222%,** con una proporción de víctimas que transfiere pequeñas cantidades y una fracción que supera los **cinco mil pesos por incidente.** Segundo, el **robo de cuentas de WhatsApp,** con un crecimiento de **672%**, habilita la suplantación de identidad y peticiones de dinero a contactos, además de abrir puertas de acceso a cuentas corporativas conectadas por hábitos de uso y sincronización; el vector pivota sobre el descuido en la activación de la verificación en dos pasos y el reuso de contraseñas. Tercero, las tiendas y agencias de viajes falsas operan como plataformas de phishing y fraude transaccional, capitalizando la expectativa de descuentos y promociones; su impacto se multiplica cuando la marca suplantada no cuenta con monitoreo de abuso de dominio, validación de certificados ni mecanismos de derribo coordinados con proveedores.

La respuesta del **Estado Mexicano** comenzó a ordenar un marco de **ciberresiliencia nacional.** En diciembre de 2025 se presentó el Plan Nacional de Ciberseguridad 2025–2030, con la creación de un **Centro Nacional de Operaciones de Ciberseguridad y un CSIRT federal,** sistemas de alerta y notificación de vulnerabilidades, inventario de infraestructura crítica y el diseño de una política general y una futura **Ley General de Ciberseguridad;** el objetivo declarado es homogenizar protocolos, fortalecer capacidades de prevención y respuesta y preparar al país para picos de exposición asociados a eventos de alto impacto, incluyendo el **Mundial del 2026.** La estrategia reconoce que la **inteligencia artificial** es un acelerador del delito digital y, simultáneamente, una herramienta esencial de defensa, y propone una arquitectura de cooperación entre gobierno, academia y sector privado que, bien implementada, puede elevar el umbral mínimo de seguridad en industrias con alta criticidad regulatoria y operativa.

Para el nivel corporativo, la convergencia de tendencias obliga a una **postura proactiva** y medible. La primera línea es reducir la dependencia del factor humano mediante **autenticación multifactor,** verificación en dos pasos y segmentación de accesos con principios de mínimo privilegio; la evidencia sugiere que el phishing y el abuso de credenciales siguen siendo la puerta de entrada predominante, por lo que conviene acompañar la tecnología con simulaciones periódicas de phishing y programas de formación que evalúen y mejoren la tasa de reporte de incidentes en tiempo real. La segunda es integrar la visibilidad y el contexto de amenazas en un tejido operativo que evite la fragmentación: consolidar telemetría de endpoints, red y nube en una plataforma que correlacione eventos y priorice respuestas automatizadas reduce el dwell time y la probabilidad de movimiento lateral en campañas modernas; la literatura reciente muestra que los entornos con herramientas desconectadas sufren más en detección temprana y contención.

La tercera línea es proteger la **confianza del cliente** como activo estratégico. En diciembre, los ataques que afectan la relación marca–usuario requieren capacidades de **defensa de identidad digital:** monitoreo de suplantación de dominio y de marca, verificación de certificados, listas anti-phishing actualizadas y acuerdos de colaboración con plataformas para el derribo ágil de sitios y cuentas fraudulentas; incorporar mensajería preventiva y protocolos de comunicación de incidentes en temporada alta mejora la **resiliencia reputacional** y reduce la tasa de conversión del atacante en campañas que dependen de señales sociales y de urgencia percibida. En paralelo, la adopción **de cifrado extremo** a extremo en canales de atención, doble validación de operaciones sensibles y controles de riesgo transaccional —incluida la detección de anomalías y las listas de dispositivos confiables— apuntalan la seguridad sin sacrificar la experiencia del cliente, condición crítica en mercados de alto volumen navideño.

El cierre del año exige, además, **gobernanza clara de incidentes** y pruebas realistas de continuidad de negocio. La coordinación con centros de respuesta nacionales, el alineamiento a marcos regulatorios emergentes y la ejecución de playbooks que integren ciberseguridad con las áreas legal, de compliance y comunicación corporativa determinan la rapidez y eficacia de la contención; a medida que el Plan Nacional de Ciberseguridad madure, las organizaciones que se anticipen a sus obligaciones y estándares tendrán ventajas regulatorias y operativas, especialmente en sectores críticos y entidades reguladas.

En suma, el aprendizaje de 2024 y el arranque de 2025 confirman que el **riesgo ya no es un fenómeno episódico,** sino una condición permanente del entorno digital: diciembre acentúa la exposición, pero también ofrece un espacio para consolidar disciplina, arquitectura y cultura de ciberseguridad orientadas a resultados. Las empresas que sostengan inversiones en protección basada en inteligencia, reduzcan la superficie de ataque y fortalezcan la alfabetización digital de sus equipos estarán mejor posicionadas para resistir la próxima temporada alta del cibercrimen y el ciclo de amenazas que traerá 2026.

Fuentes y enlaces:

- 324 000 millones de intentos de ciberataques en 2024 – Fortinet / El Economista
- https://www.eleconomista.com.mx/tecnologia/mexico-recibio-324-000-millones-intentos-ciberataques-2024-fortinet-20250429-756919.html
- 324 000 millones confirmados – Fortinet / El Universal
- https://www.eluniversal.com.mx/techbit/mexico-sufrio-324-mil-millones-de-ciberataques-en-2024/
- 59 millones de ciberataques diarios en Q1 2025 – Cloudflare / El Universal
- https://www.eluniversal.com.mx/cartera/mexico-registro-59-millones-de-ciberataques-al-dia-en-primer-trimestre-del-2025-cloudfare-phishing-la-amenaza-mas-reportada/
- Incremento de 23 % en tráfico de Internet en Q1 2025 – Cloudflare / Expansión
- https://expansion.mx/tecnologia/2025/06/11/mexico-sufre-tantos-ciberaatques-al-dia-estadio-azteca
- Fraude de paquetería “fantasma” +222 % – El País
- https://elpais.com/mexico/2024-12-11/los-fraudes-por-paqueteria-fantasma-en-ciudad-de-mexico-aumentan-un-222-amazon-y-dhl-entre-las-empresas-mas-suplantadas.html
- Detalles de incremento de paquetería y robo de WhatsApp – Latinus
- https://latinus.us/mexico/2024/12/26/fraude-de-paquete-fantasma-aumenta-222-alertan-sobre-robo-de-cuentas-de-whatsapp-en-mexico-131362.html
- Robo de cuentas de WhatsApp +672 % – AMECI

- Robo de cuentas de WhatsApp +672% – CABECERA
- https://www.cabecera.mx/robo-de-cuentas-de-whatsapp-crece-672-en-mexico/
- Presentación del Plan Nacional de Ciberseguridad 2025-2030 – El Economista
- https://www.eleconomista.com.mx/tecnologia/gobierno-sheinbaum-presenta-plan-nacional-ciberseguridad-2025-20251204-789652.html
- Detalle del plan y centros CNSOC/CSIRT – El Imparcial
- https://www.elimparcial.com/mexico/2025/12/05/plan-nacional-de-ciberseguridad-mexico-crea-centros-de-operaciones-protocolos-obligatorios-y-una-estrategia-contra-amenazas-digitales/
- Alcances estratégicos del plan – DPL News
- https://dplnews.com/mexico-lanza-plan-nacional-de-ciberseguridad-2025-2030/

Alcances institucionales y tecnológicos – TIGMX
https://tigmx.com/2025/12/mexico-presenta-su-primer-plan-nacional-de-ciberseguridad-y-va-por-una-ley-general/