Grupo BeIT

NEWSLETTER

grupobeit.com

BLOG DEL CEO

El inicio de 2026 exige que la ciberseguridad se trate como una capacidad estratégica del negocio, no como un gasto operativo aislado...

EDICIÓN 51

Qué esperar en ciberseguridad para 2026 y cómo prepararte

El 2026 estará definido por tres grandes tendencias: ataques más inteligentes, defensas más automatizadas y mayor presión regulatoria...

¡NOS CONVERTIMOS EN SOPHOS FIREWALL PARTNER!

Nos complace anunciar que hemos obtenido la acreditación Sophos Firewall Partner, un reconocimiento que refleja nuestro esfuerzo por mantenernos a la vanguardia en ciberseguridad...

Edición 51

Introducción

Arrancar un nuevo año nunca es solo un cambio de calendario. En ciberseguridad, 2026 se perfila como un punto de inflexión estratégico para las organizaciones en México. El crecimiento exponencial de ataques impulsados por inteligencia artificial, la expansión de la superficie digital y la presión regulatoria obligan a dejar atrás enfoques reactivos y fragmentados.

El inicio de 2026 representa una oportunidad clave para redefinir prioridades, alinear la ciberseguridad con los objetivos de negocio y fortalecer la resiliencia operativa desde la planeación estratégica. Las empresas que comiencen el año con una hoja de ruta clara estarán mejor preparadas para competir, crecer y proteger la confianza de sus clientes.

¡Brindemos por un 2026 más fuerte, seguro y lleno de oportunidades!

¡Feliz año!

Elías Cedillo
CEO & Fundador de GrupoBeIT

Cómo arrancar 2026 de la mejor manera estratégica en ciberseguridad

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

El inicio de 2026 exige que la ciberseguridad se trate como una capacidad estratégica del negocio, no como un gasto operativo aislado. Los datos confirman la urgencia: México cerró 2025 como uno de los países más atacados de América Latina, con más de 35 mil millones de intentos de ciberataque durante el primer trimestre del año, equivalente a más de 270 mil ataques por minuto, según reportes de Fortinet y Cloudflare.
Para comenzar 2026 con una postura sólida, las organizaciones deben concentrarse en cinco ejes estratégicos:

1. Identidad como nuevo perímetro

El abuso de credenciales sigue siendo el principal vector de ataque. Informes de IBM X-Force y Microsoft indican que más del 60 % de los incidentes exitosos inician con identidades comprometidas. Así pues, arrancar el año con MFA resistente al phishing (FIDO2), gestión de privilegios y acceso condicional ya no es opcional: es el estándar mínimo.

2. De Zero Trust como concepto a Zero Trust operativo

En 2026, Zero Trust deja de ser una visión aspiracional. Las organizaciones más maduras ya operan con segmentación dinámica, verificación continua y mínimos privilegios aplicados a usuarios, dispositivos, cargas de trabajo y entornos OT. Iniciar el año con un roadmap claro de Zero Trust permitirá reducir de forma inmediata el impacto de intrusiones.

3. SOC impulsado por datos e IA

La fragmentación de herramientas sigue siendo uno de los mayores obstáculos. IDC estima que las organizaciones con plataformas XDR/SIEM unificadas reducen hasta en 70 % el tiempo de detección y respuesta. Para 2026, el SOC debe evolucionar hacia operaciones asistidas por IA, automatización de contención y correlación avanzada de telemetría.

4. Priorizar vulnerabilidades por riesgo explotable

El volumen de vulnerabilidades ya supera la capacidad humana. IBM y Fortinet coinciden en que menos del 10 % de las vulnerabilidades son explotadas activamente, pero concentran la mayoría de los incidentes. Arrancar 2026 con priorización basada en riesgo real permitirá enfocar recursos donde realmente importa.

5. Gobernanza y resiliencia como ventaja competitiva

La ciberseguridad en 2026 estará estrechamente ligada a ESG, continuidad de negocio y reputación. Simulacros de crisis, pruebas de recuperación y métricas ejecutivas claras (MTTD, MTTR, cobertura de MFA, tiempos de parcheo) deben formar parte del tablero directivo desde el primer trimestre del año.

Empezar 2026 con estos pilares no solo reduce el riesgo, sino que convierte la ciberseguridad en un habilitador para el crecimiento, la innovación y la confianza digital. En definitiva, 2026 será el año en que la ciberseguridad pase a convertirse en un diferenciador competitivo. Las organizaciones que integren estas prácticas desde el inicio no solo estarán mejor preparadas frente a amenazas, sino que también ganarán agilidad para innovar y responder a un mercado cada vez más inestable. La clave está en pasar de la intención a la ejecución: convertir la estrategia en acciones medibles y sostenibles.

Fuentes:

- IBM — X-Force Threat Intelligence Index 2025: IBM X-Force 2025 Threat Intelligence Index | IBM
- Fortinet — Threat Landscape Report 2025: threat-landscape-report-2025.pdf
- Cloudflare — DDoS & Application Security Reports 2024–2025: Cloudflare's 2025 Q3 DDoS threat report -- including Aisuru, the apex of botnets
- Microsoft — Digital Defense Report: **Microsoft Digital Defense Report 2025 - MySecurity Marketplace**

México y la ciberseguridad rumbo a 2026

NOTICIA BeIT

El gobierno de la presidenta Claudia Sheinbaum, a través de la Dirección General de Ciberseguridad, presentó el Plan Nacional de Ciberseguridad 2025-2030, con el que se busca que México sea un país ciberresiliente, así como una referencia a nivel regional en materia de ciberseguridad. El Plan Nacional de Ciberseguridad considera una estructura comandada por un Consejo Nacional de Ciberseguridad, integrado por el gobierno, la academia y la industria; la ATDT como ente a nivel federal; la Dirección General de Ciberseguridad, como ente normativo y operativo. El contexto que impulsa esta estrategia es contundente.

Durante 2024, México registró 324 mil millones de intentos de ciberataque, cifra confirmada por Fortinet y publicada por medios como El Economista y El Universal. En 2025, la tendencia no solo se mantuvo, sino que se aceleró con ataques más automatizados y sofisticados, impulsados por IA generativa. Bajo este contexto, el Plan Nacional de Ciberseguridad busca alinear instituciones, talento y marcos regulatorios para pasar de una defensa fragmentada a una estrategia integral que cubra todo el ecosistema digital del país.

El plan también prevé el impulso de una **Ley General de Ciberseguridad** enfocada en la gestión de riesgos, la prevención y la respuesta coordinada a incidentes, más que en la persecución penal de los ciberdelitos. La idea es crear un marco que privilegie la profesionalización de los servidores públicos, defina con claridad la infraestructura crítica, establezca un sistema de reporte obligatorio de incidentes y articule sanciones que incentiven buenas prácticas sin caer en la criminalización de la falla humana.

Dicho plan reconoce explícitamente a sectores críticos como energía, telecomunicaciones, servicios financieros, manufactura y logística, y busca fortalecer la cooperación entre gobierno, iniciativa privada y academia. Para las empresas, este movimiento marca un antes y un después, pues la ciberseguridad dejará de ser un tema tecnológico, convirtiéndose en una obligación estratégica y regulatoria, especialmente rumbo a eventos de alto impacto como el Mundial de 2026.

Fuentes:

- Gobierno de Sheinbaum presenta el Plan Nacional de Ciberseguridad 2025-2030

Qué esperar en ciberseguridad para 2026 y cómo prepararte

El 2026 estará definido por tres grandes tendencias: ataques más inteligentes, defensas más automatizadas y mayor presión regulatoria. Cloudflare estima que el tráfico malicioso automatizado seguirá creciendo a doble dígito, mientras que Microsoft advierte que la IA reducirá la barrera de entrada para atacantes con menos experiencia técnica.

Frente a este escenario, prepararse para 2026 implica acciones concretas desde hoy:

- **Elevar el estándar mínimo de seguridad:** MFA en el 100 % de cuentas humanas y de servicio, reducción de aplicaciones obsoletas y control estricto de identidades.
- **Unificar visibilidad y respuesta:** consolidar endpoints, red, nube, correo e identidades en plataformas XDR/SIEM con automatización.
- **Asegurar OT e infraestructura crítica:** la convergencia IT/OT seguirá siendo un objetivo prioritario para atacantes. Fortinet reporta que más del 30% de las organizaciones industriales ya han sufrido incidentes en OT.
- **Prepararse para el cumplimiento y la auditoría:** el marco nacional y las regulaciones internacionales exigirán evidencia, métricas y trazabilidad.
- **Invertir en cultura y simulación:** el factor humano sigue siendo clave. Programas de concientización, ejercicios de phishing y simulacros ejecutivos reducen drásticamente el impacto de incidentes reales.

Las organizaciones que entren a 2026 con disciplina, automatización posición y métricas claras no solo resistirán mejor los ataques, sino que fortalecerán su competitiva en un entorno donde la confianza digital será un diferenciador clave.

En definitiva, la resiliencia digital no será opcional, sino un requisito estratégico. Las organizaciones que integren seguridad en su ADN estarán mejor posicionadas para innovar sin comprometer la confianza de sus clientes y reputación. 2026 no será solo un año de retos, sino también una oportunidad para que quienes actúen con anticipación transformen la ciberseguridad en una ventaja competitiva sostenible.

Fuentes:

- Cloudflare — DDoS & Application Security Reports 2024–2025: Cloudflare's 2025 Q3 DDoS threat report -- including Aisuru, the apex of botnets
- Microsoft — Digital Defense Report: Microsoft Digital Defense Report 2025 - MySecurity Marketplace

BURÓMC SEGURIDAD INFORMÁTICA

Grupo BeIT

ELIT INFRASTRUCTURE SERVICES

COMUNICADO

SOPHOS FIREWALL PARTNER

¡Nos convertimos en Sophos Firewall Partner! Un logro que fortalece nuestras soluciones para nuestros clientes

En GrupoBeIT, creemos que la excelencia se construye con conocimiento y compromiso. Cada capacitación, cada certificación y cada hora dedicada a aprender tiene un impacto directo en la calidad de los servicios que brindamos a nuestros clientes.

Hoy nos complace anunciar que hemos obtenido la acreditación **Sophos Firewall Partner**, un reconocimiento que refleja nuestro esfuerzo por mantenernos a la vanguardia en ciberseguridad. Este logro nos permite ofrecerte soluciones más robustas, seguras y alineadas con las mejores prácticas del mercado.

Nuestro objetivo sigue siendo claro: ayudarte a proteger tu infraestructura, garantizar la continuidad de tu negocio y brindarte la confianza que necesitas para crecer en un entorno digital cada vez más desafiante.

Gracias por confiar en nosotros. Seguiremos trabajando para que tu ciberseguridad sea nuestra prioridad.

Elías Cedillo
CEO & Fundador

SOPHOS