DELTA PROTECT®

ANIA

CIBERSEGURIDAD E INTELIGENCIA ARTIFICIAL

El Blueprint para la Integración de IA y Ciberseguridad en PyMes

Tabla de Contenidos

Alejandra Lagunes
President Alianza Nacional de Inteligencia Artificial (ANIA)

Vivimos un momento de inflexión.

La inteligencia artificial ha dejado de ser el territorio exclusivo de las grandes corporaciones para convertirse en el motor de transformación más democrático de nuestra era. Los números lo confirman: el 94% de los líderes globales la identifica como el motor de cambio más significativo de este año, con un impacto económico proyectado de $15.7 trillones para 2030.

No estamos ante una tendencia emergente — estamos ante una reconfiguración estructural de la economía mundial.

Las PyMes que integran IA en sus procesos core escalan 3.5 veces más rápido que sus competidoras. Pero esa misma aceleración, sin una estrategia de seguridad simétrica, abre puertas que el crimen organizado ya sabe cómo cruzar: las pérdidas anuales por incidentes cibernéticos superan los $19.4 billones de dólares.

Este Blueprint traduce esa tensión en tres vectores de acción concreta: ciberseguridad proactiva, gobernanza de datos y eficiencia estructural.

Lo que tienen en sus manos no es un manual técnico. Es una hoja de ruta estratégica para tomar decisiones informadas en la intersección de dos fuerzas que ya no pueden gestionarse por separado: la inteligencia artificial y la ciberseguridad.

La resiliencia operativa no es un privilegio de los grandes. Es un derecho de quienes construyen, producen e innovan cada día.

Santiago Fuentes
Co-Founder & Co-CEO Delta Protect

En la última década, la ciberseguridad dejó de ser un ítem en el presupuesto de IT para convertirse en la piedra angular de la continuidad de negocio. Hoy enfrentamos un cambio aún más profundo: la convergencia de la Inteligencia Artificial y la ciberdelincuencia profesionalizada.

No existe innovación sostenible sin una defensa inteligente. Este eBook no habla de vulnerabilidades técnicas — habla de riesgo de negocio. Estas páginas analizan cómo las industrias más críticas están siendo desafiadas por atacantes que ya no usan herramientas manuales, sino algoritmos de aprendizaje profundo.

¿Por qué ahora? Porque el silencio es el mejor aliado del atacante. En el C-Suite, la ciberseguridad no puede ser una respuesta reactiva: debe ser una conversación proactiva, estratégica y compartida.

Este documento es una invitación a cuestionar si sus estructuras actuales pueden resistir un ataque que muta en milisegundos — y a entender que la confianza es el activo más difícil de construir y el más fácil de destruir.

Nuestra misión: dotar a quienes toman decisiones de la claridad necesaria para transformar la incertidumbre en resiliencia. El futuro pertenece a las empresas que no solo adoptan la IA para optimizar, sino que la dominan para protegerse.

Bienvenidos a la conversación que definirá el próximo capítulo de su organización.

01. INTRODUCCIÓN

El Nuevo Paradigma de Eficiencia Estructural

En la última década, la digitalización fue vista como una ventaja competitiva. Hoy, en 2026, esa visión ha quedado obsoleta. La digitalización ya no es una ventaja; es el piso mínimo de supervivencia.

El verdadero diferenciador actual es la Eficiencia Estructural: un concepto que trasciende la simple automatización de tareas para enfocarse en el rediseño completo de los flujos de valor mediante la inteligencia artificial profunda y la seguridad proactiva.

Este eBook no es una invitación a la experimentación, sino una hoja de ruta para la consolidación. Para la dirección, el reto ha dejado de ser "*¿cómo implemento IA?*" para convertirse en "*¿cómo protejo y escalo una infraestructura que ya es intrínsecamente inteligente?*"

94%

DE LOS LÍDERES

Ven a la IA como el motor de cambio #1 en seguridad

87%

IDENTIFICA

Vulnerabilidades de IA como riesgo de mayor crecimiento

73%

FUE AFECTADO

Por fraude cibernético en su red durante 2025

$20.9B

PÉRDIDAS

Por cibercrimen al FBI en 2025, primer año sobre $20B

$244B

GASTO GLOBAL

En ciberseguridad 2026 (Gartner, +13.3%)

$2.52T

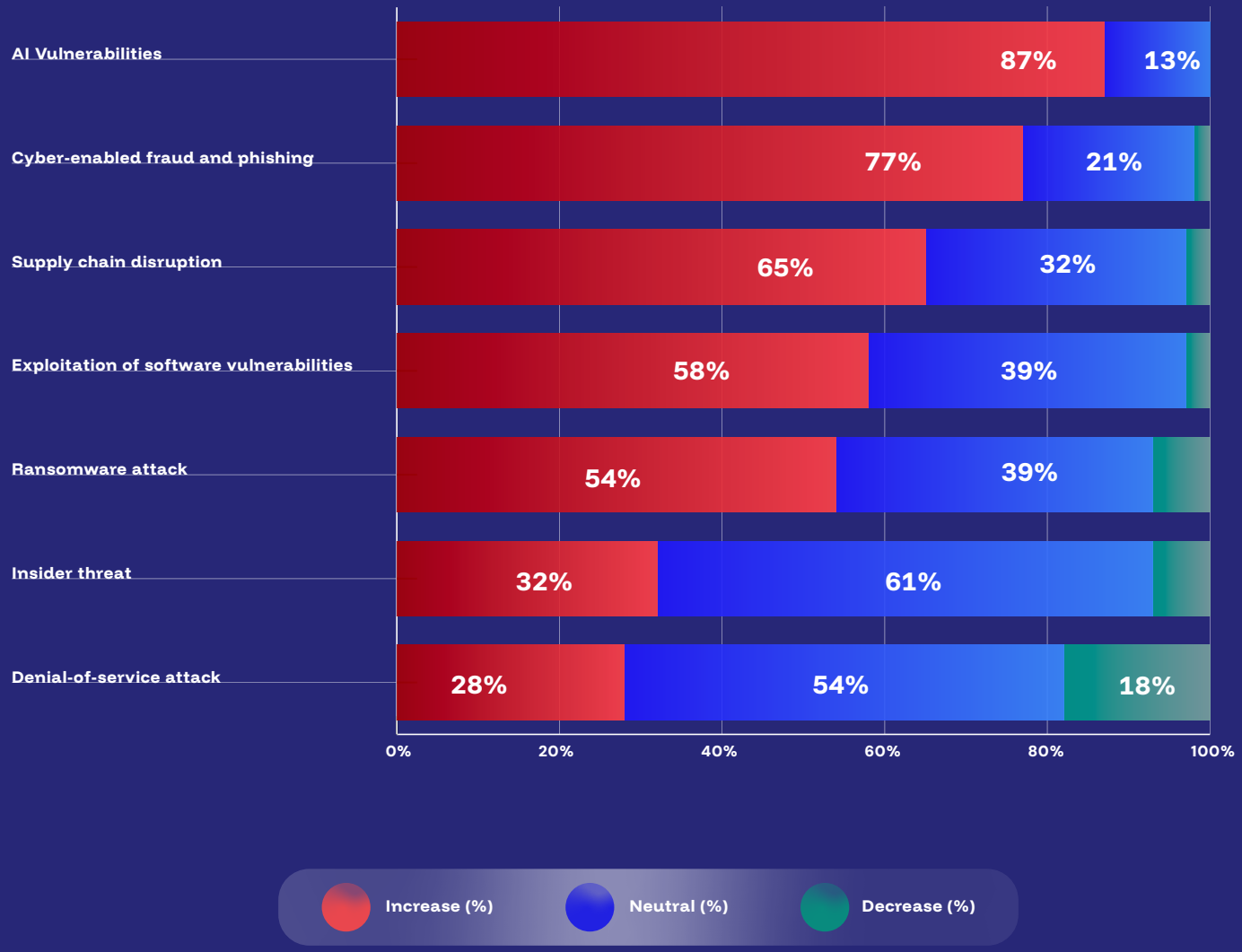
GASTO GLOBAL

En IA en 2026, +44% interanual

Fuentes: WEF + Accenture, GCO 2026 (804 participantes, 92 países, 316 CISOs, 105 CEOs); FBI IC3 2025; Gartner Feb 2026.

Más allá del Hype: La IA como Infraestructura, no como Accesorio

De acuerdo con el Global Cybersecurity Outlook 2026 del World Economic Forum, los riesgos cibernéticos no están creciendo de forma homogénea: algunos se están acelerando de manera estructural. El 87% de los líderes ven las vulnerabilidades de IA como el riesgo de mayor crecimiento.



Fuente: WEF + Accenture. Global Cybersecurity Outlook 2026, Figure 8, p.19.

Más allá del Hype: La IA como Infraestructura, no como Accesorio

Hubo un tiempo en que la IA se trataba como un "proyecto especial" o un laboratorio de innovación aislado del núcleo del negocio. Ese enfoque de "accesorio" ha demostrado ser costoso e ineficiente. La realidad actual exige entender la IA como **infraestructura crítica**, al mismo nivel que la nube o la red eléctrica.

Los mercados de capital lo confirman: desde 2022 se han desplegado **más de $15 mil millones de dólares** en empresas de seguridad para IA. El mercado de AI Security proyecta crecer de **$31B (2025) a $87B para 2030**, con una tasa anual del 23%. En paralelo, el gasto global en IA total asciende a **$2.52 trillones en 2026** (+44% interanual, según Gartner).

De Herramientas a Agentes: Ya no hablamos solo de interfaces de chat o copilotos de productividad. Estamos en la era de los **Agentes Autónomos de Orquestación** que operan directamente sobre ERPs y sistemas core. Gartner predice que el **40% de las aplicaciones empresariales** incluirá agentes de IA específicos para tareas a finales de 2026, contra menos del 5% en enero de este año.

La Deuda Técnica de la IA: Las organizaciones que trataron la IA como un parche ahora enfrentan problemas de escalabilidad. La verdadera adopción implica que la IA sea la capa base sobre la cual se construye el resto de la lógica de negocio.

El Cambio de CAPEX a OPEX Inteligente: La inversión en IA ha dejado de ser un gasto en software para convertirse en una inversión en capacidad cognitiva institucional. Las plataformas AI-native cotizadas en el mercado privado alcanzan múltiplos de **15-20x sobre ingresos**, el doble de lo que vale una solución de ciberseguridad tradicional.

Nota Estratégica 2026

La ventaja no reside en quién tiene el modelo más grande, sino en quién posee la infraestructura de datos más limpia y el despliegue más seguro. La IA está bifurcando el mercado: plataformas nativas (valuaciones premium) vs. herramientas heredadas con IA añadida (múltiplos comprimidos). Lo mismo aplica a las organizaciones que las adoptan.

La Paradoja de la Velocidad: Agilidad vs. Integridad

El mayor dilema para la Alta Dirección hoy es la **Paradoja de la Velocidad:** la presión del mercado exige ciclos de innovación cada vez más cortos, pero la sofisticación de las ciberamenazas demanda una cautela extrema.

Agilidad sin Exposición: La adopción acelerada no puede comprometer la propiedad intelectual. El uso de arquitecturas de **IA Privada** y modelos locales es ahora el estándar para industrias donde el dato es el activo más valioso.

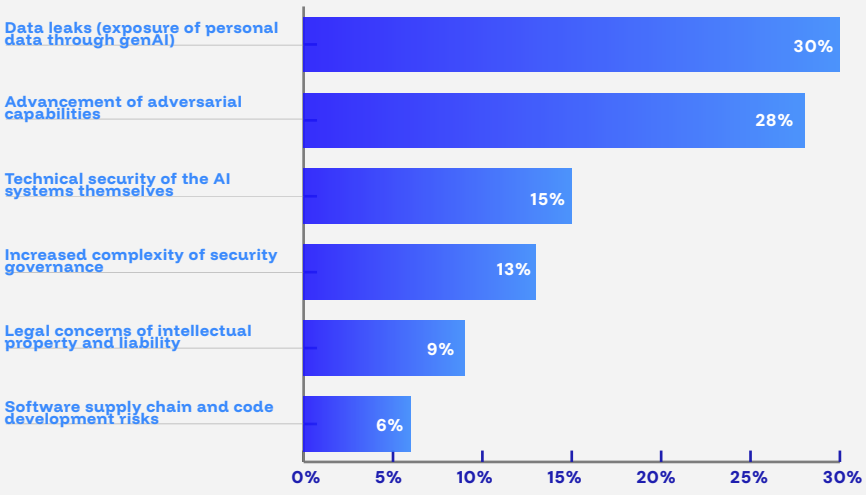
La Integridad como Activo Fiduciario: Para un CEO o CFO, un sesgo en un modelo de riesgo crediticio o una filtración de datos logísticos no es solo un fallo técnico; es una ruptura de la confianza del mercado y una vulnerabilidad legal. La IA ha cambiado incluso la naturaleza de la intrusión: el malware que antes colapsaba sistemas, ahora los estudia. Se fusiona con la operación diaria — escaneando facturas, imitando correos, clonando credenciales.

Ciberseguridad como Habilitador: La seguridad ya no puede ser el departamento del "no". El **91% de los ejecutivos de seguridad** confirma que defenderse hoy requiere fusionar arquitectura, operaciones y cultura en un diseño unificado, no son tres funciones separadas.

💡 El argumento del ROI para el CEO

*Las organizaciones con programas de Secure by Design (SbD) maduros proyectan retornos del **22% para 2026, 38% para 2028 y 48% para 2030**. El 87% de líderes tecnológicos vincula SbD directamente con crecimiento de ingresos a largo plazo. La seguridad ya no es un costo, es un multiplicador de valor.*

El 30% de los CEOs identifica las fugas de datos como su mayor preocupación relacionada con IA Generativa, seguido muy de cerca por el avance de las capacidades adversariales (28%). Juntos, estos dos riesgos concentran casi el 60% de la agenda de los CEOs, y tienen algo en común: ambos son consecuencia directa de adoptar IA sin gobernanza. El dato más revelador está al final de la escala: los riesgos de cadena de suministro de software solo preocupan al 6% de los CEOs, a pesar de que los ataques a proveedores casi se duplicaron en 2025. La brecha entre lo que más preocupa y lo que más ocurre define el trabajo estratégico que queda por hacer.



Fuente: WEF + Accenture. Global Cybersecurity Outlook 2026, Figure 1, p.12.

CEO vs. CISO: Dos Agendas de Riesgo que Deben Converger

Uno de los hallazgos más reveladores del WEF 2026 es la divergencia entre lo que preocupa al CEO y lo que preocupa al CISO. No es un desacuerdo de opinión, es una brecha estructural que deja a las organizaciones expuestas en los flancos que nadie está mirando.

En 2025, CEOs y CISOs compartían la misma preocupación #1: ransomware. En 2026, sus agendas divergieron. Los CEOs migraron al fraude cibernético y el phishing como amenaza principal, con las vulnerabilidades de IA subiendo al #2, un riesgo que no aparecía en su top 3 el año anterior. Los CISOs, en cambio, se mantuvieron inamovibles: ransomware #1, disrupción de cadena de suministro #2, igual que en 2025. La tabla lo hace visible de inmediato: el CEO está pensando en pérdida financiera inmediata; el CISO está pensando en resiliencia operativa. Ambas perspectivas son válidas, el problema es cuando no se hablan.

Rank	Chief Executive Officer (CEO)		Chief Information Security Officer (CISO)	
	2025	**2026**	2025	**2026**
1	Ransomware attack	**Cyber-enabled fraud and phishing**	Ransomware attack	**Ransomware attack**
2	Cyber-enabled fraud and phishing	**AI vulnerabilities**	Supply chain disruption	**Supply chain disruption**
3	Supply chain disruption	**Exploitation of software vulnerabilities**	Cyber-enabled fraud and phishing	**Exploitation of software vulnerabilities**

La divergencia es diagnóstica. El dato más revelador no está en las prioridades de 2026, sino en el movimiento de 2025 a 2026: las vulnerabilidades de IA aparecen por primera vez en el top 3 del CEO, pero siguen ausentes en el del CISO. Un CEO que ha interiorizado el riesgo de IA y un CISO que todavía no lo prioriza operativamente generan un vacío de gobernanza exactamente donde la amenaza está creciendo más rápido.

Cifra crítica para el boardroom: **menos del 45% de los CEOs del sector privado** confían en la capacidad de su país para responder a incidentes cibernéticos mayores. En América Latina, esa cifra cae al **13%**, la más baja de todas las regiones.

Fuente: WEF + Accenture. Global Cybersecurity Outlook 2026, Table 2, p.11.

02. GOBERNANZA Y ESTRATEGIA DE DATOS

El Estado Real de la Gobernanza de IA

Los datos del IBM IBV (2025), sobre más de 1,000 ejecutivos C-suite en 20 industrias, revelan una brecha alarmante entre aspiración y ejecución. El contexto económico que hace urgente esta conversación: el WEF estima **$19.4 billones** de dólares en pérdidas anuales por incidentes cibernéticos en mercados líderes, un número que convierte la gobernanza de IA de ejercicio de cumplimiento a imperativo financiero.

CAPACIDAD DE GOBERNANZA DE IA	% QUE LA TIENE
Lineamientos para uso ético y responsable de IA	56%
Estándares de explicabilidad y transparencia	48%
Controles de acceso específicos para IA	38%
Ambiente seguro para desarrollo de modelos	29%
GRC embebido en flujos de trabajo	**Solo 40%**
Monitoreo de inputs/outputs de IA de terceros	**Solo 25%**
Modelos de IA resistentes a ataques adversariales	**Solo 10%**

🚨 **Dato más crítico para la Junta Directiva**

Solo 1 de cada 4 organizaciones monitorea los inputs y outputs de los modelos de IA de terceros que utilizan. Los sistemas que informan las decisiones diarias son, en la práctica, cajas negras no auditadas.

Para contextualizar en el ámbito regional: el BID, OEA y Oxford evaluaron en diciembre 2025 a 30 países de LATAM usando el **Modelo de Madurez de Capacidades de Ciberseguridad (CMM)**. La mayoría de los países de la región se encuentran entre los **niveles 2 (Formativo) y 3 (Establecido)** de un máximo de 5. El factor con menor madurez en toda la región es la **investigación e innovación en ciberseguridad**.

Fuentes: IBM IBV + Microsoft, Q3 2025; BID + OEA + Oxford GCSCC, Dic 2025.

Data Readiness: Evaluación de Calidad y Silos

El éxito o fracaso de cualquier iniciativa de IA se decide mucho antes de que el modelo esté en producción. Se decide en la calidad de los datos que lo alimentan. En organizaciones mexicanas donde la mayoría de los datos críticos existen en silos departamentales, ERP de finanzas, CRM de ventas, WMS de logística, el primer acto de gobierno de datos es cartográfico: saber exactamente qué existe, dónde vive y quién tiene acceso.

Desfragmentación de Silos: Si los datos de logística no "hablan" con los de finanzas, el modelo de IA tomará decisiones incompletas. Un modelo que predice demanda sin ver el inventario en tiempo real produce alucinaciones operativas que pueden costar millones. El primer ejercicio de Data Readiness es forzar la conversación entre los silos: ¿existe un identificador único de cliente que permita cruzar ventas con soporte con finanzas? Si la respuesta es no, esa es la primera brecha.

El Diagnóstico de Calidad: 4 Dimensiones a Medir

1. **Completitud:** ¿Qué porcentaje de los registros críticos tiene todos los campos obligatorios llenos? Un modelo entrenado con el 30% de los campos vacíos producirá predicciones inutilizables.
2. **Exactitud:** ¿Cuántos registros contienen errores conocidos? ¿Existen dos versiones del mismo cliente en diferentes sistemas?
3. **Actualidad:** ¿Con qué frecuencia se actualizan los datos? Un modelo de riesgo crediticio que trabaja con datos de 90 días en un entorno de tasas variables puede generar decisiones catastróficas.
4. **Trazabilidad:** ¿Se puede rastrear el origen de cualquier dato hasta su fuente? La trazabilidad no es un requisito de auditoría, es la defensa contra el Data Poisoning: si un atacante introduce datos sesgados, la trazabilidad permite identificar el punto exacto de contaminación.

Vectorización de Datos: En 2026, la preparación incluye transformar información no estructurada (PDFs, grabaciones de llamadas, correos, notas de campo) en bases de datos vectoriales que permiten a la IA entender el contexto semántico del negocio.

Smart Data sobre Big Data: La calidad ha reemplazado a la cantidad como métrica de madurez. El principio Garbage In, Garbage Out cobra mayor relevancia que nunca en entornos de IA agéntica donde los errores se propagan a través de todos los sistemas con los que el agente interactúa.

💡 Pregunta de diagnóstico para el CEO

"¿Si hoy le pedimos a la IA una predicción de demanda para el siguiente trimestre, cuántos de nuestros sistemas tendría que consultar, y hay al menos uno al que no tendría acceso?" La respuesta define la urgencia del trabajo de Data Readiness.

Arquitectura RAG (Retrieval-Augmented Generation)

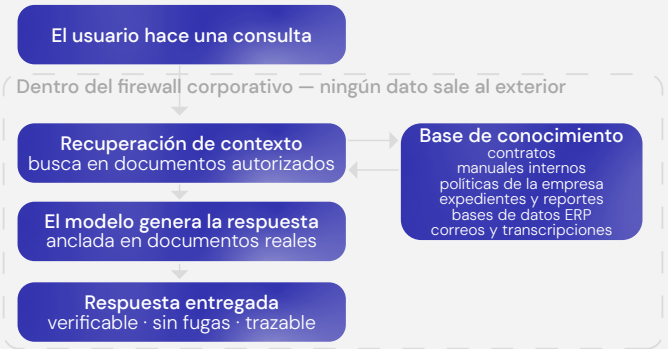
RAG es hoy la solución estándar para que las organizaciones utilicen sus datos privados con modelos de IA de forma segura, sin exponerlos a sistemas públicos ni arriesgar su propiedad intelectual.

¿Cómo funciona en términos ejecutivos? Imagina contratar a un analista que solo puede responder preguntas consultando los archivos internos de la empresa, no puede inventar, no puede filtrar hacia afuera, y tiene acceso solo a lo que tú le autorizas. El resultado: sin alucinaciones (cada respuesta está anclada en documentos reales), sin fugas (la información nunca sale del entorno seguro), y sin entrenamiento (no se usa para mejorar modelos públicos).

Casos de Uso Críticos en Organizaciones Mexicanas

- **Legal y contratos:** El equipo jurídico consulta instantáneamente 5,000 contratos históricos para identificar cláusulas relevantes ante un litigio, sin enviar documentos confidenciales a herramientas externas.
- **Soporte de clientes:** El agente de IA responde con base en los manuales y políticas reales de la empresa, no inventa políticas de garantía que no existen.
- **Finanzas:** El CFO puede hacer preguntas en lenguaje natural sobre el estado financiero consolidado, sin que ninguno de esos datos salga del firewall corporativo.
- **Cumplimiento regulatorio:** El equipo de compliance consulta en segundos toda la normatividad aplicable con referencias precisas a las fuentes.

RAG vs. Fine-tuning: El fine-tuning es costoso, requiere actualización constante y en muchos casos expone los datos a terceros durante el proceso. RAG permite actualizar el conocimiento del sistema simplemente actualizando los documentos fuente, sin re-entrenar nada, sin costos adicionales, con trazabilidad total.



🚨 Señal de alerta para el CTO

Si tu equipo está enviando documentos internos a ChatGPT u otras herramientas públicas para obtener análisis, es posible que esos documentos estén siendo usados para entrenar modelos públicos. RAG es la arquitectura que elimina ese riesgo.

Fuente: Elaboración propia, Delta Protect (2026), basado en IBM IBV Secure by Design, Smarter with AI (2025) y WEF Global Cybersecurity Outlook 2026.

Marcos Éticos y Cumplimiento Regulatorio

Uno de los hallazgos más críticos para la Junta Directiva: el **63% de las organizaciones no tiene políticas de gobernanza de IA**, o aún las está desarrollando. Solo el **34%** de quienes sí las tienen realiza auditorías regulares del uso de IA no sancionado (Shadow AI). La ausencia de gobernanza ya no es solo un riesgo regulatorio, es un riesgo directo de brecha. A pesar de ello, hay señales de avance: el **64% ya tiene procesos formales de evaluación de seguridad de sus herramientas de IA** antes de desplegarlas, y el **74% percibe que las regulaciones vigentes son efectivas para mejorar su postura.** El marco normativo está ganando tracción, la brecha está en la ejecución operativa, no en la voluntad.

El dato que cambia la conversación: el **13% de las organizaciones** reportó brechas directamente sobre modelos o aplicaciones de IA y el **97%** de esas organizaciones carecía de controles de acceso adecuados. La secuencia es clara: IA sin gobernanza = blanco de alta prioridad.

El EU AI Act (vigente agosto 2026 en sus disposiciones clave) clasifica los sistemas de IA en cuatro categorías de riesgo e impone obligaciones de transparencia, auditoría y reporte de incidentes. Para empresas mexicanas que exportan a Europa o trabajan con socios europeos, el cumplimiento no es opcional, es condición de contrato.

La LFPDPPP en el contexto de IA: La Ley Federal de Protección de Datos Personales establece obligaciones de consentimiento, finalidad y proporcionalidad que aplican directamente a los modelos de IA que procesan datos de clientes mexicanos. El uso de datos personales para entrenar modelos sin consentimiento explícito es una violación con multas de hasta 320,000 días de salario mínimo.

💡 Para el CISO ante la Junta

El 58% de los responsables de seguridad usa las regulaciones como palanca para elevar la conciencia en el Consejo. El EU AI Act es hoy la herramienta más efectiva para convertir la ciberseguridad en un tema de agenda de Junta, no solo de TI.

Fuentes: IBM Cost of a Data Breach Report 2025; WEF Global Cybersecurity Outlook 2026.

03. LA DEFENSA

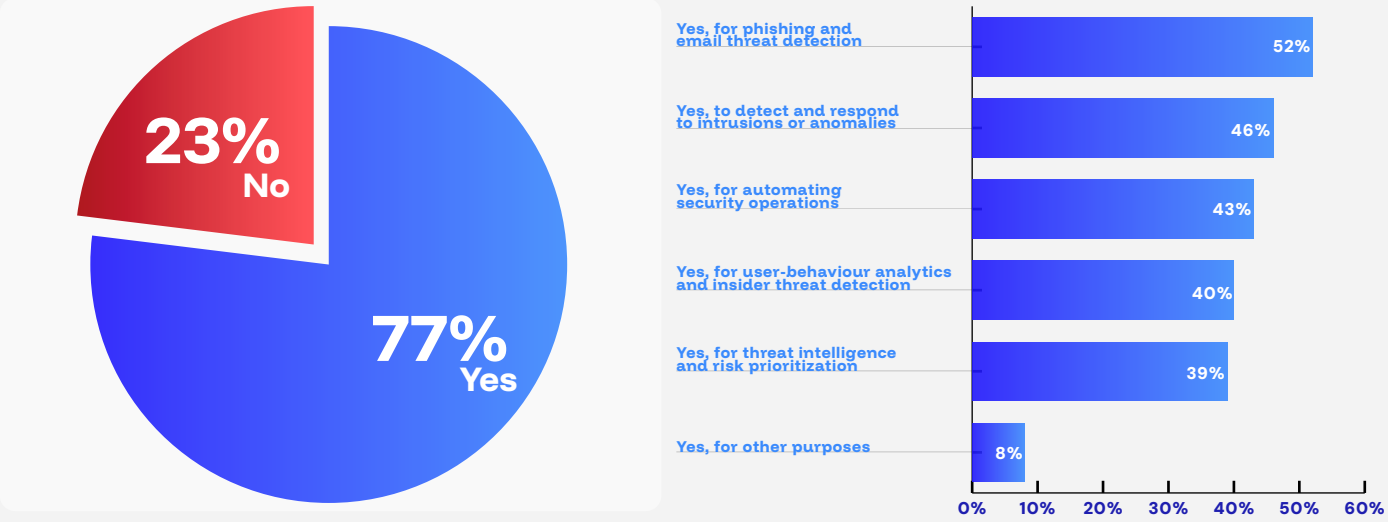
Ciberseguridad en la Era de la IA

Si la IA es el motor, la ciberseguridad son los frenos cerámicos. La ciberseguridad ha dejado de ser una función técnica para convertirse en una prioridad económica central.

En 2025, IBM X-Force rastreó casi **40,000 vulnerabilidades** y el **56% no requerían autenticación** para ser explotadas. La explotación de aplicaciones públicas aumentó un **44%**. Más de **300,000 credenciales de ChatGPT** se encontraron a la venta en la dark web ese año.

Pero el mayor riesgo no viene de afuera. El IBM IBV (2025) encontró que el **42% de los ejecutivos clasifica sus propias deficiencias operacionales entre sus principales amenazas**, superando a actores de estados-nación (31%). Y **dos tercios de los ejecutivos** reconocen que sus equipos de seguridad, tecnología y operaciones aún trabajan en silos.

Cómo las organizaciones implementan la IA en ciberseguridad



El **77%** de las organizaciones ya utiliza herramientas de IA para cumplir sus objetivos de ciberseguridad, en apenas dos años pasó de ser una apuesta de vanguardia a ser práctica estándar. El desglose de usos revela las tres prioridades de la industria: detección de phishing y amenazas por email **(52%)**, respuesta a intrusiones y anomalías **(46%)** y automatización de operaciones de seguridad **(43%)**. Dos datos que no deben pasar desapercibidos: **el análisis de comportamiento de usuarios, que detecta amenazas internas, ya alcanza el 40%; y la inteligencia de amenazas con priorización de riesgos llega al 39%**, confirma que la IA está dejando de ser reactiva para volverse predictiva. El 23% que todavía no ha adoptado IA defensiva opera con una desventaja estructural creciente: sus adversarios sí la usan.

Fuente: WEF + Accenture, Global Cybersecurity Outlook 2026, Figure 12, p.22.

Blindando el "AI Stack": Protección en Capas

Las organizaciones que utilizan IA extensivamente en operaciones de seguridad ahorraron en promedio $1.9 millones de dólares por brecha comparado con las que no la usan (IBM 2025). La protección del AI Stack opera en cuatro capas interdependientes:

- **Capa 1 — Datos:** Protección contra acceso no autorizado a datasets de entrenamiento e inferencia. El 97% de las organizaciones con incidentes de IA carecían de controles de acceso adecuados. Controles clave: clasificación de datos, mínimo privilegio, cifrado en reposo y en tránsito, monitoreo de inputs/outputs.
- **Capa 2 — Modelo:** Integridad algorítmica y detección de deriva (model drift). Un modelo que "deriva" puede estar siendo envenenado intencionalmente (Data Poisoning) o simplemente deteriorarse porque el mundo cambió y los datos de entrenamiento ya no lo reflejan.
- **Capa 3 —** Aplicación: Filtrado de entradas, control de prompts y monitoreo de outputs. La capa más activamente atacada en 2026: Prompt Injection, Model Jailbreak y la manipulación de agentes autónomos para ejecutar acciones fuera de sus parámetros.
- **Capa 4 — El Harness del Agente (nueva en 2026):** El conjunto de prompts, definiciones de herramientas, pipelines de recuperación y lógica de escalación. Debe auditarse con el mismo rigor que los permisos del agente. Antes de desplegar cualquier agente en producción, definir: límites de blast-radius, lógica de escalación y mecanismo de override humano.

Fuente: IBM Cost of a Data Breach Report 2025; CSA CISO Community / SANS, Mythos-ready, abr 2026.

El Colapso del Tiempo de Explotación

El tiempo entre el descubrimiento de una vulnerabilidad y su explotación activa se ha colapsado de 2.3 años (2018) a menos de 20 horas (2026). No es una tendencia gradual, es una ruptura estructural acelerada por la IA.

Tiempo promedio entre descubrimiento de vulnerabilidad y explotación activa

Mínimo documentado: **8 minutos**
Sysdig, febrero 2026, acceso de nivel administrador

Aceleración: **x150,000**

Las barras no se acortan de forma gradual, colapsan. De 2.3 años de margen en 2018, la industria pasó a semanas en 2024 y a días en junio de 2025. La barra de 2026 es casi invisible porque el tiempo disponible es casi cero.

El dato más disruptivo está en el callout rojo: el mínimo documentado es de 8 minutos el tiempo que tardó un sistema con IA en alcanzar acceso de nivel administrador en un entorno real (Sysdig, febrero 2026). La aceleración total: ×150,000 en 8 años. Cualquier modelo de gestión de riesgo que asuma ventanas de parche de semanas es, en 2026, históricamente incorrecto.

La Evolución de las Capacidades Ofensivas de IA

- **Jun 2025:** XBOW se convirtió en el sistema autónomo #1 en HackerOne, superando a todos los hackers humanos.
- **Ago 2025:** Google Big Sleep descubrió 20 vulnerabilidades zero-day reales en proyectos open source de forma autónoma.
- **Ago 2025:** DARPA AIxCC encontró 54 vulnerabilidades en 4 horas de cómputo sobre 54M líneas de código.
- **Nov 2025:** Anthropic reveló que un grupo chino usó Claude Code para ejecutar cadenas de ataque completas, desde reconocimiento hasta exfiltración, contra ~30 objetivos globales.
- **Feb 2026:** Sysdig documentó un ataque con IA que alcanzó acceso de administrador en **8 minutos**.
- **Feb 2026:** Gambit publicó reporte sobre **compromiso de infraestructura gubernamental mexicana mediante IA**.
- **Abr 2026:** Claude Mythos Preview 72% tasa de éxito en generación de exploits. Bug de 27 años descubierto en OpenBSD.
- **May 2026:** El **Google Threat Intelligence Group (GTIG)** confirmó el primer exploit zero-day desarrollado con IA por un actor criminal, planificado para una campaña de explotación masiva. El descubrimiento proactivo de Google puede haber prevenido su uso. El mismo reporte documenta el malware autónomo **PROMPTSPY**, capaz de interpretar el estado del sistema y generar comandos de ataque en tiempo real sin intervención humana.

🚨 Implicación directa para el CEO

Los modelos de riesgo construidos antes de 2025 asumen ventanas de parche de semanas. Esa ventana ya no existe. El tiempo entre "vulnerabilidad descubierta" y "organización comprometida" es ahora de horas.

Project Glasswing y Claude Mythos: El Punto de Inflexión Documentado

El 7 de abril de 2026, Anthropic anunció Project Glasswing, la respuesta más importante de la industria tecnológica al colapso del tiempo de explotación. La razón de su existencia es tan simple como inquietante: Anthropic desarrolló un modelo de IA tan capaz de encontrar y explotar vulnerabilidades que consideró inseguro liberarlo al público. En cambio, decidió dárselo a los defensores primero.

Claude Mythos Preview - Lo que puede hacer

- 72.4% de tasa de éxito convirtiendo vulnerabilidades en exploits funcionales (vs. 14.4% para Claude Opus 4.6, el modelo anterior).
- 181 exploits funcionales en un benchmark de Firefox donde el modelo anterior logró solo 2, 90× más efectivo.
- 23,019 vulnerabilidades candidatas identificadas en 1,000+ proyectos open-source críticos; 1,726 confirmadas como válidas (90.8% tasa de verdaderos positivos).
- Vulnerabilidades encontradas: 27 años en OpenBSD, 16 años en FFmpeg, 17 años en el servidor NFS de FreeBSD.
- CVE-2026-5194 (CVSS 9.3): Falla en la librería criptográfica wolfSSL que permite falsificar certificados digitales y suplantar identidades.
- 73% de éxito en capture-the-flag de nivel experto, primer modelo de IA en alcanzar este threshold (confirmado por el UK AI Security Institute).
- Primer modelo en completar un ataque simulado de 32 pasos end-to-end en red corporativa de forma autónoma.
- Más del 99% de las vulnerabilidades descubiertas permanecen sin parchear — el ritmo de descubrimiento ya superó la capacidad humana de remediación.

Project Glasswing — La respuesta de la industria

12 socios de lanzamiento: Amazon Web Services, Apple, Broadcom, Cisco, CrowdStrike, Google, JPMorganChase, Linux Foundation, Microsoft, NVIDIA y Palo Alto Networks. Más ~40 organizaciones adicionales responsables de infraestructura de software crítica. El principio rector: antes de que las capacidades de Mythos proliferen hacia actores que no están comprometidos con usarlas de forma responsable, los defensores deben tener acceso primero. Es la primera vez que una empresa de IA crea un programa formal para dar ventaja estructural a los defensores sobre los atacantes.

Implicación directa para el CEO

Los modelos de riesgo construidos antes de 2025 asumen ventanas de parche de semanas. Esa ventana ya no existe. El tiempo entre "vulnerabilidad descubierta" y "organización comprometida" es ahora de horas.

Fuentes: Anthropic, Project Glasswing announcement, 7 abr 2026 · Fortune · ZeroFox · UK AISI · Cyberpress · SC Media · CSA Labs

Ejercicio Ejecutivo — Aplicar en la Próxima Reunión de Junta

El Test de los 8 Minutos: ¿Qué ya comprometió un atacante?

En febrero de 2026, Sysdig documentó un ataque asistido por IA que alcanzó acceso de nivel administrador en **8 minutos**. Basado en esa evidencia, este ejercicio de pensamiento está diseñado para que cualquier C-Level entienda su exposición real, sin necesitar ser experto técnico.

El escenario: Un atacante con herramientas de IA entró a tu red hace 8 minutos. Empieza a moverse lateralmente. ¿Qué puede comprometer en ese tiempo?

MINUTO	QUÉ PUEDE HACER EL ATACANTE CON IA	¿TIENES DEFENSA PARA ESTO?
0–2 min	Mapea toda la red, identifica sistemas críticos, detecta credenciales en caché. La IA correlaciona en segundos lo que un humano tardaría horas.	¿Tienes micro-segmentación activa? ¿Monitoreo de comportamiento en tiempo real?
2–4 min	Escala privilegios. Si hay un servicio con acceso de administrador mal configurado (frecuente en el 97% de los entornos), ya tiene las llaves del reino.	¿Aplicaste mínimo privilegio? ¿Tienes MFA en todos los sistemas críticos?
4–6 min	Comienza la exfiltración silenciosa de datos. Objetivos prioritarios: credenciales, contratos, datos financieros, propiedad intelectual compartida con clientes.	¿Tienes DLP activo? ¿Monitoreo de tráfico anómalo saliente?
6–8 min	Prepara la carga útil de ransomware o planta un backdoor para acceso futuro. En muchos casos, permanece dormido semanas antes de activarse.	¿Tienes EDR con detección comportamental? ¿Backups offline inmutables?

⚠️ La pregunta que importa

¿Tu SOC puede detectar una anomalía de este tipo en menos de 8 minutos? El promedio global de detección es de 194 días. En LATAM, el 35% de las organizaciones ni siquiera tiene planificación de respuesta. El tiempo no está del lado de la defensa, a menos que hayas construido los sistemas correctos.

Basado en: Sysdig, incidente documentado feb 2026; IBM Cost of a Data Breach 2025 (tiempo promedio de detección); WEF LATAM 2026.

La IA en el Cibercrimen: Ya No Es Teoría

El FBI cuantificó en 2025 lo que hasta ese momento era mayormente anecdotal. El IC3 recibió más de **22,000** denuncias vinculadas al uso de IA, con **pérdidas superiores a $893 millones**, solo en casos donde las víctimas identificaron la participación de IA.

Gartner lo confirma: las empresas gastan **17 veces más en herramientas de IA que en asegurar la propia IA** sobre la que esas herramientas corren. Forrester predice que **una brecha pública causada por un agente de IA ocurrirá en 2026**.

BEC potenciado con IA: Generadores de chat imitan con precisión el estilo del CEO; el *voice cloning* se usa para solicitar transferencias de fondos vía llamada. Las empresas reportaron **más de $30 millones** en BEC con nexo de IA. El BEC total alcanzó **$3.046 billones** en 2025.

Fraude de identidad e inversión con IA: Pérdidas reportadas: más de **$632 millones** pero el fraude total de inversión superó **$8 billones**, confirmando que la mayoría de las víctimas no identifican la participación de IA.

Deepfakes en entrevistas laborales: *Voice spoofing* y deepfakes de video para ganar acceso a redes corporativas. Pérdidas: más de **$13 millones**.

⚠️ Alerta para el CFO

El voice cloning de ejecutivos es el vector de mayor crecimiento en BEC. Todo proceso de autorización de pagos que use una llamada telefónica como verificación debe considerarse obsoleto sin una segunda capa de autenticación independiente.

Fuentes: FBI IC3, Internet Crime Report 2025; Gartner, Top Cybersecurity Trends 2026; Forrester, 2026 Cybersecurity Predictions.

GTIG AI Threat Tracker: Los actores estatales ya usan IA para explotar vulnerabilidades

El **Google Threat Intelligence Group (GTIG)**, en su reporte publicado en mayo de 2026, documenta por primera vez casos concretos donde actores adversarios han integrado IA en toda la cadena de ataque:

- **Primer zero-day desarrollado con IA:** GTIG identificó un actor criminal usando un exploit zero-day que se cree fue generado con IA, planeado para una campaña de explotación masiva. El descubrimiento proactivo de Google puede haber prevenido su uso. Esta es la primera vez documentada públicamente de este tipo de capacidad ofensiva.
- **PROMPTSPY — Malware Autónomo:** Nuevo malware capaz de interpretar el estado del sistema comprometido y generar comandos de ataque dinámicamente, sin intervención humana. Señala una transición hacia la orquestación autónoma de ataques donde el modelo adapta su comportamiento en tiempo real a las defensas del entorno.
- **Actores PRC y DPRK:** China y Corea del Norte han demostrado interés significativo en capitalizar la IA para descubrimiento de vulnerabilidades a escala industrial.
- **Actores Russia-nexus:** Grupos vinculados a Rusia están usando IA para acelerar el desarrollo de malware polimórfico y redes de ofuscación que evaden defensas tradicionales basadas en firmas.

La conclusión del GTIG es directa: la IA ya no es un experimento en manos de actores avanzados. Es infraestructura de ataque operativa.

Ransomware 2025: 63 Variantes Nuevas en Un Año

En 2025, el IC3 identificó **63 nuevas variantes** de ransomware, un promedio de 5.25 por mes. Las 10 más activas: **Akira, Qilin, INC./Lynx, BianLian, Play, Ransomhub, LockBit, Dragonforce, SAFEPAY y Medusa**.

SECTOR	INCIDENTES RANSOMWARE	INCIDENTES DATA BREACH
Salud Pública y Hospitales	460	182
Manufactura Crítica	355	52
Servicios Financieros	258	189
Instalaciones Gubernamentales	233	174

Fuentes: Google Threat Intelligence Group (GTIG), "GTIG AI Threat Tracker: Adversaries Leverage AI for Vulnerability Exploitation, Augmented Operations, and Initial Access", 11 mayo 2026.
FBI IC3, Internet Crime Report 2025.

Los 6 Trends de Gartner 2026 para CISOs

1. **IA Agéntica Supervisión Obligatoria:** Tendencia #1. Requiere marcos de identidad, credenciales gestionadas y políticas de autorización específicas para actores no humanos.
2. **Gestión de Riesgo y Gobernanza:** El reporte de riesgos al Consejo debe actualizarse para reflejar nuevos supuestos de tiempos de explotación.
3. **Criptografía Post-Cuántica:** Los avances cuánticos rendirán la criptografía asimétrica insegura antes de 2030. Los ataques "harvest now, decrypt later" ya están ocurriendo.
4. **IAM para Agentes de IA:** La gestión de identidades para actores no humanos es un gap crítico que Gartner predice generará "incidentes de acceso significativos" en 2026.
5. **SOC Impulsado por IA:** Los SOC con IA reducen el tiempo de detección de semanas a minutos, pero introducen nuevas presiones de staffing y upskilling.
6. **Seguridad Centrada en Personas:** El 86% de los ataques exitosos en México tienen un vector humano. La tecnología sola no es suficiente.

Project Glasswing

El Modelo de Defensa Proactiva más Importante de 2026

La adopción de IA para ciberseguridad pasó del 77% como estadística a convertirse en arquitectura de industria el 7 de abril de 2026, cuando Anthropic lanzó Project Glasswing, la primera iniciativa a escala industrial de IA defensiva coordinada. Doce de las compañías tecnológicas más importantes del mundo usan Claude Mythos Preview específicamente para encontrar vulnerabilidades en sus sistemas antes de que lo hagan los atacantes.

Lo que hace diferente a Project Glasswing de cualquier herramienta de seguridad anterior:

- **No es un producto:** es un programa de acceso controlado a una capacidad que Anthropic consideró demasiado poderosa para liberar públicamente. El modelo no está disponible comercialmente.
- **No busca amenazas conocidas:** descubre vulnerabilidades que nadie sabía que existían (zero-days), incluyendo bugs que sobrevivieron décadas de auditorías manuales y herramientas automatizadas.

Fuente: Gartner, Top Trends in Cybersecurity for 2026, febrero 2026.

- **No requiere dirección humana:** Mythos opera de forma autónoma, combinando múltiples vulnerabilidades independientes para construir exploit chains completos sin intervención.

La implicación para cualquier organización: si las empresas más avanzadas del mundo necesitan un programa de este tipo para mantenerse adelante de los atacantes, el modelo de seguridad reactivo no solo es insuficiente, es estructuralmente obsoleto. La pregunta ya no es si adoptar IA defensiva: es con qué urgencia.

El Ecosistema como Nueva Superficie de Ataque

El perímetro tradicional ya no existe. El **40% de las organizaciones** ha sufrido una brecha involucrando a un partner clave en los últimos tres años. El **53%** ya usa MSSPs, pero solo el **40%** extiende el mismo rigor de seguridad a proveedores externos.

El punto ciego más crítico: solo **1 de cada 4 organizaciones** monitorea los inputs y outputs de modelos de IA de terceros. Con la creciente dependencia de servicios externos de IA para decisiones de negocio, los sistemas que informan las decisiones diarias operan como cajas negras no auditadas.

🚨 Alerta para el C-Suite

Un proveedor con IA mal gobernada no es solo su problema, es tu problema. La próxima fase de madurez es la Confianza Federada: tratar al ecosistema completo como una superficie de seguridad colectiva con controles que se extienden a toda la cadena.

Fuentes: Anthropic, Project Glasswing, abr 2026 · Arctic Wolf · HPCwire · Cybersecurity Insiders
IBM IBV + Microsoft, "Secure by Design, Smarter with AI", Q3 2025.

Zero Trust y Privacidad Diferencial

El estándar de seguridad para infraestructuras de IA es "nunca confiar, siempre verificar" (Zero Trust). Todo acceso, humano o de un agente de IA, se verifica continuamente antes de ser otorgado.

Los 5 Pilares de Zero Trust para el Contexto Mexicano

1. Identidad verificada permanentemente. MFA resistente a phishing en el 100% de los sistemas críticos, incluyendo las identidades de aplicaciones y agentes de IA. Gartner identifica la gestión de identidades para agentes como la tendencia #4 más crítica en ciberseguridad 2026.

2. Dispositivos evaluados en tiempo real. El estado de salud del dispositivo se valida en cada intento de acceso, no solo en el primer login del día.

3. Acceso de mínimo privilegio. En LATAM, el 51% no evalúa las herramientas de IA antes de desplegarlas, muchas otorgan a los agentes acceso de administrador por simplificar la configuración. Ese es el error más peligroso.

4. Red micro-segmentada. Para la industria manufacturera en México, implica separar redes IT de redes OT, actualmente convergidas en la mayoría de las plantas del país.

5. Monitoreo continuo y respuesta automática. Todo acceso se registra, analiza y correlaciona en tiempo real. Las anomalías disparan respuestas antes de que un humano pueda reaccionar.

Privacidad Diferencial es una técnica matemática que permite aprender patrones de grandes conjuntos de datos sin "ver" ningún dato individual. Especialmente relevante para salud, finanzas y gobierno en México, donde la LFPDPPP establece obligaciones estrictas sobre datos personales.

Para el CFO y Legal

La transición a Zero Trust requiere 12-24 meses y entre el 15-25% del presupuesto anual de seguridad (CISA). Es una inversión estratégica, no un gasto operativo.

Fuentes: Gartner, Top Cybersecurity Trends 2026; WEF LATAM 2026; CISA Zero Trust Maturity Model.

04. DEEP DIVES SECTORIALES

Contexto LATAM: El Diagnóstico Definitivo

América Latina ocupa una posición única y preocupante en el panorama global de ciberseguridad 2026: **alta conciencia, alta adopción de IA, y la brecha de capacidad más grande del mundo.**

13%

CONFÍA

En la capacidad de su país para responder a incidentes mayores (vs. 37% global)

51%

NO EVALÚA

Seguridad de herramientas de IA antes de usarlas (vs. 29% global)

65%

CARECE DE

Personas y habilidades críticas para sus objetivos de ciberseguridad

12%

CALIFICA SU

Resiliencia como superior a los requerimientos (vs. 19% global)

35%

SIN PLANIFICACIÓN

Suficiente de respuesta a incidentes — la tasa más alta del mundo

92%

JUNTAS DIRECTIVAS

Comprometidas activamente con ciberseguridad

La brecha institucional a nivel país: solo **13 países en LATAM** tienen una estrategia nacional de ciberseguridad. **Solo 9 países** tienen planes para proteger infraestructura crítica — a pesar de que los ataques ya están disrumpiendo administraciones tributarias, puertos y hospitales.

El caso más emblemático: el ataque del grupo ruso **Conti al Ministerio de Finanzas de Costa Rica en 2022** paralizó los servicios del Estado, forzando al país a declarar **estado de emergencia nacional**, el primero causado por un ciberataque. Casos similares ocurrieron en Barbados, Chile, Colombia, Guatemala, Jamaica, México y Perú.

El número que hace que la cadena de suministro sea riesgo colectivo: el **98% de las organizaciones** en LATAM está conectada con al menos un tercero que ha experimentado un ciberataque en los últimos dos años. La resiliencia cibernética no es específica de una organización, es una responsabilidad de toda la sociedad.

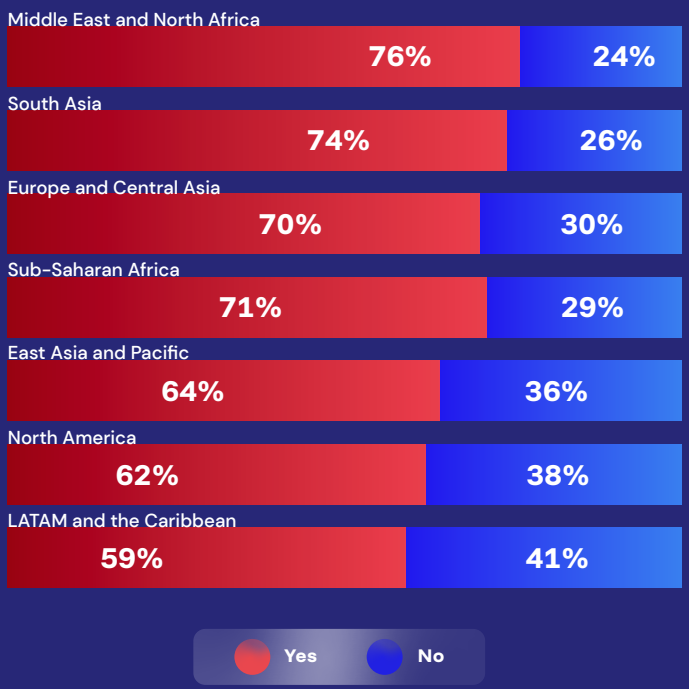
Fuentes: WEF + Accenture, GCO 2026 LATAM; BID + OEA + Oxford GCSCC, Dic 2025.

LATAM frente al mundo: geopolítica y confianza nacional

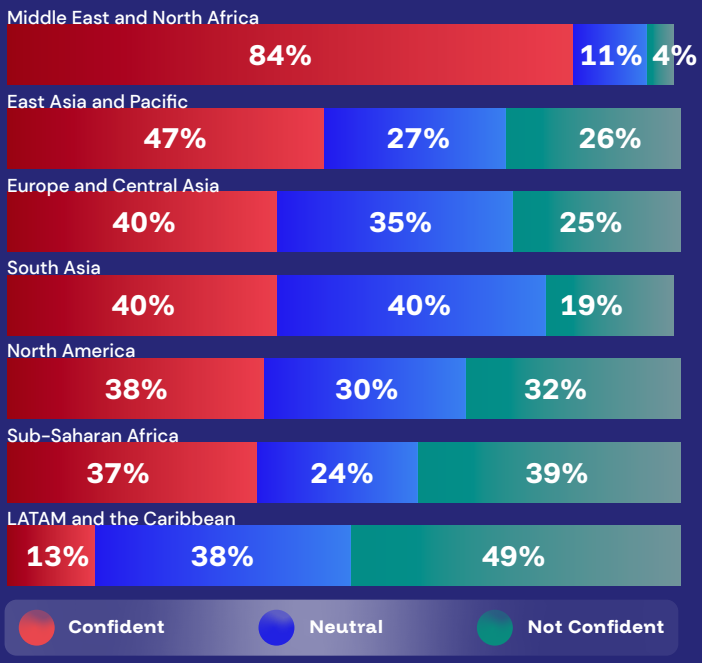
La postura de una región no se mide solo por cuánto invierte en ciberseguridad, se mide por qué tan bien ha calibrado su estrategia frente a las amenazas reales y qué tanto confía en que el sistema institucional la respaldará cuando el ataque llegue.

¿Ha evolucionado la estrategia de ciberseguridad de su organización por la volatilidad geopolítica?

América Latina y el Caribe registra el porcentaje más bajo de todas las regiones encuestadas: solo el 59% de las organizaciones ha ajustado su estrategia de ciberseguridad en respuesta a la volatilidad geopolítica, 17 puntos por debajo de Oriente Medio, la región más atenta a este factor. Esto no es un detalle menor. En un entorno donde los ataques motivados geopolíticamente están aumentando en todo el mundo, y donde México tiene un rol central en las cadenas de suministro de América del Norte, ignorar la dimensión geopolítica del riesgo es una exposición estructural. El 41% de las organizaciones de LATAM que no ha adaptado su estrategia está operando con un mapa de amenazas que ya no refleja el mundo real.



¿Qué tan confiante está en la preparación de su país para responder a incidentes cibernéticos mayores que afecten infraestructura crítica?



Esta gráfica es el diagnóstico más crudo del reporte WEF para la región. Mientras el 84% de las organizaciones en Oriente Medio y Norte de África confía en la capacidad de su país para responder a un incidente cibernético mayor, en América Latina ese número colapsa al 13%, la brecha más amplia entre cualquier par de regiones en todo el estudio. Pero la cifra más inquietante no es el 13%: es el 49% que declara abiertamente no tener confianza. Casi la mitad de las organizaciones en la región opera sabiendo que, si mañana ocurre un incidente de escala nacional, la respuesta institucional será insuficiente. Para cualquier C-Level mexicano, esto tiene una implicación directa: la última línea de defensa no es el Estado es la organización misma.

DELTA PROTECT®

Fuente: WEF + Accenture. Global Cybersecurity Outlook 2026 — Latin America and the Caribbean Regional Analysis. Febrero 2026.

México vs. Benchmark Global por Sector: La Brecha Real

¿Qué tan lejos está México de los líderes globales en ciberseguridad por industria? Esta comparativa cruza los datos del WEF, IBM, FortiGuard y el Plan Nacional para dar una imagen honesta del gap actual y las acciones más urgentes por sector:

Sector	Líder Global Práctica Estándar	Realidad México 2025-2026	Acción Inmediata
Manufactura *#1 más atacado MX*	- *Redes IT/OT segmentadas* - *TPRM como requisito contractual* - *Inventario IoT completo · Backups offline OT*	- *#1 sector más atacado en MX (1,284 casos)* - *Solo 16% reporta incidentes OT a la Junta* - *IT/OT convergida en mayoría de plantas* - *Sin estándares TPRM formales*	- *Separar IT/OT esta semana.* - *Agregar cláusula de TPRM en próximos contratos con clientes EE.UU.*
Servicios Financieros *#2 más atacado MX*	- *Biometría de comportamiento activa* - *Protocolo anti-BEC voice cloning* - *RegTech en tiempo real · DORA compliance*	- *#2 sector más atacado en MX (824 casos)* - *La mayoría aún usa llamada telefónica como único factor de verificación* - *Adopción de RegTech incipiente* - *Sin regulación específica de IA financiera*	- *Actualizar protocolo de autorización de pagos hoy.* - *Briefing a la Junta sobre riesgo BEC.*
Healthcare *12 años el sector más costoso*	- *Segmentación de redes hospitalarias* - *SBOM de dispositivos médicos · EOL sistemático* - *Cifrado de datos de pacientes end-to-end*	- *83% dispositivos imagenología con SO no soportados* - *Sin NOM de ciberseg. (COFEPRIS)* - *279 días para detectar/contener brechas*	- *Inventariar y aislar todos los dispositivos con SO no soportado.* - *Exigir roadmap de reemplazo.*
Gobierno *#2 LATAM más atacado*	- *CSOC nacional 24/7 · CSIRT especializado* - *Notificación obligatoria en 4 horas* - *Presupuesto TI protegido de recortes*	- *#2 más atacado LATAM* - *Presupuesto TI recortado 85% (SICT) tras ser atacada* - *750 vulnerabilidades activas en 2025* - *Plan Nacional 2025-2030 recién publicado*	- *Alinear con Plan Nacional.* - *Priorizar CSOC federal.* - *Nunca recortar TI tras un ataque.*
Logística y Supply Chain *Nearshoring = $37B inversión*	- *TPRM formal: evaluación 4to y 5to nivel* - *Gemelos Digitales para resiliencia operativa* - *Continuidad operativa manual documentada*	- *Nearshoring sin estándares de ciberseg. formalizados* - *Cadena de suministro casi duplicó ataques (154-297 en 2025)* - *Menos del 40% extiende controles a proveedores externos*	- *Incluir evaluación de ciberseg. en próximos RFPs.* - *Documentar plan de continuidad manual.*

DELTA PROTECT®

Fuentes: WEF GCO 2026 LATAM; IBM IBV 2025; FortiGuard Labs 2026; Plan Nacional Ciberseguridad 2025-2030 (ATDT); Check Point Manufacturing Threat Landscape 2025; Delta Protect / IQSEC Healthcare MX 2025.

Caso: Fabricante Automotriz Global

El Ciberataque que Cambió la Conversación de Boardroom

- Producción global paralizada durante **5 semanas**
- Más de **5,000 proveedores** afectados en la cadena de suministro
- Costos directos: **£196 millones ($260M USD)**
- Caída de ingresos: casi **25%**
- Impacto en la economía del Reino Unido: **£1.9 billones ($2.5B USD)** adicionales

Para México, donde el nearshoring integra a empresas mexicanas en cadenas automotrices y manufactureras globales, la exposición es directamente proporcional a esa integración.

Casos de Impacto Real: Cuando los Números se Vuelven Nombres

Los datos son convincentes, pero los nombres lo hacen ineludible. Estas son organizaciones reales, algunas conocidas globalmente, otras del tejido empresarial mexicano, con impactos documentados que ningún C-Level puede ignorar:

56M
Sistema Público de Salud

2025 (3x) - Ransomware + exfiltración

3 ataques en el mismo año. 1.8 TB extraídos. 56 millones de registros de derechohabientes en dark web.

El sector público no está exento. Los datos de salud valen 50x más que los financieros.

6 TB+
Institución de Defensa Nacional

2022 - Intrusión + filtración

Documentos militares clasificados filtrados. El grupo Guacamaya extrajo 6 TB de múltiples gobiernos LATAM.

Ninguna institución es demasiado sensible para no ser atacada.

192.7M
Proveedor de Infraestructura Médica

2024-2025 - Ransomware ALPHV

Personas afectadas. $1.5B+ en costos totales. Parálisis de pagos médicos en EE.UU. durante semanas.

Una brecha en un proveedor de pagos puede paralizar todo un sistema nacional de salud.

1er
Gobierno Nacional

2022 - Ransomware Conti

Primer estado de emergencia nacional causado por un ciberataque. Servicios del Ministerio de Finanzas paralizados.

Un ciberataque puede forzar al Estado a declarar emergencia nacional. Ya ocurrió.

16
Consumo Masivo · Retail · Finanzas

2022-2025 - Plan Nacional ATDT

Los 16 ataques críticos documentados en el Plan Nacional incluyen las marcas más reconocidas del tejido empresarial mexicano.

El tamaño y la reputación no protegen. Las marcas más sólidas de México han sido comprometidas.

En todos estos casos, las organizaciones tenían tecnología de seguridad instalada. Lo que falló fue la combinación de: gobernanza deficiente (políticas sin aplicar), visibilidad incompleta (silos entre seguridad y operaciones), tiempo de detección demasiado largo (promedio: 194 días) y ausencia de playbooks probados (el 73% nunca hizo un simulacro). La tecnología no protege si no hay proceso detrás.

DELTA PROTECT®

Fuentes: WEF GCO 2026; Plan Nacional de Ciberseguridad 2025-2030 (ATDT); Delta Protect Sector Salud, abr 2026; IBM Cost of a Data Breach 2025; múltiples fuentes periodísticas verificadas.

SECTOR FINANCIERO

El sector financiero fue el **segundo sector más atacado en México en 2025** con 824 casos documentados. El BEC con voice cloning es el vector de mayor preocupación: en 2025, las empresas reportaron más de $30M en pérdidas por BEC con nexo de IA.

La defensa que cambia el juego > Biometría de Comportamiento: A diferencia de la biometría física, analiza cómo escribe el usuario, cómo mueve el ratón, su ritmo de tecleo y patrones de navegación. Un deepfake puede imitar la voz. No puede imitar el patrón único de comportamiento digital de una persona.

El impacto de Basilea IV en México: Incrementa los requerimientos de capital para riesgos operacionales, incluyendo explícitamente los riesgos cibernéticos. Para la banca mexicana bajo supervisión de la CNBV, esto se traduce en presión directa para implementar marcos formales de gestión de riesgo cibernético con métricas cuantificables y reportables al regulador.

RegTech como habilitador: La tecnología regulatoria permite auditoría perpetua y en tiempo real del cumplimiento, reemplazando los ciclos de auditoría trimestrales o anuales. En el contexto del T-MEC y la revisión de 2026, las empresas financieras con operaciones binacionales enfrentan obligaciones de cumplimiento tanto con la CNBV como con la SEC y FinCEN en EE.UU.

Los servicios financieros son el sector líder global en análisis de comportamiento de usuarios e insider threat detection — el uso más sofisticado de IA defensiva disponible en 2026. Con el fraude como amenaza #1 del CEO para el sector, las instituciones están adoptando IA donde más importa: detectar comportamientos anómalos antes de que el daño ocurra. La adopción en el sector financiero global supera en casi todas las dimensiones al promedio de otras industrias, incluyendo automatización de operaciones de seguridad (43% global) y threat intelligence (39% global). En México, la brecha no está en intención — está en implementación.

🚨 Alerta para CFOs mexicanos

El C-Suite de 60+ años representó la pérdida promedio más alta de cualquier segmento: **$38,500 USD por incidente**, casi el doble del promedio general ($20,699). Los directivos de mayor rango son el objetivo más valioso para BEC con voice cloning. Todo proceso de autorización de pagos que use una llamada telefónica como verificación debe considerarse obsoleto sin protocolo de segundo factor.

Fuentes: FBI IC3 2025; WEF GCO 2026; IBM IBV Q3 2025.

El sector de materiales e infraestructura (proxy del sector logístico) reporta el **80% de adopción en detección de phishing y amenazas por email**, el valor más alto de cualquier sector en esa dimensión, 28 puntos por encima del promedio global (52%). Esto refleja una realidad operativa: los ataques de ingeniería social son el vector de entrada más frecuente en sectores con cadenas de suministro extensas. El reto para México es que la alta adopción de una herramienta específica no equivale a postura de seguridad robusta si el resto de las dimensiones queda sin cubrir.

Las 3 Prioridades de Seguridad para el Sector Logístico Mexicano

1. TPRM (Gestión de Riesgo de Terceros):

Mapear qué proveedores tienen acceso a sistemas críticos, con qué nivel de privilegio, y cómo se documentan las evaluaciones periódicas.

2. Segmentación IT/OT:

Separar las redes administrativas de las redes operativas. Una infección en la red IT no debe poder saltar a los sistemas de control de producción.

3. Continuidad operativa

¿Cuánto tiempo puede sostenerse la operación en modo manual? Las plantas mexicanas en cadenas JIT tienen una ventana de tolerancia muy pequeña.

LOGÍSTICA Y CADENA DE SUMINISTRO

México vive un momento histórico en logística. El boom del nearshoring lo ha convertido en el principal hub manufacturero de América del Norte, con más de $37 mil millones de dólares en inversión extranjera anunciados entre 2023-2025. Pero cada nueva planta que se instala expande la superficie de ataque.

El riesgo #1: visibilidad cero en la cadena extendida. Las empresas que integran cadenas de suministro para EE.UU. y Canadá están sujetas a estándares contractuales que exigen visibilidad sobre subcontratistas de cuarta y quinta parte. **Un proveedor de manufactura que no puede demostrar gestión de riesgo de terceros pierde contratos.** No es hipotético: ya está pasando en los sectores automotriz, aeroespacial y farmacéutico.

En 2025, los ataques a la cadena de suministro casi se duplicaron: de 154 incidentes en 2024 a **297 en 2025**. Los ciberdelincuentes atacan cada vez más a proveedores pequeños, MSSPs o plataformas SaaS para obtener acceso indirecto a los grandes clientes.

Gemelos Digitales como herramienta de resiliencia: Una réplica virtual en tiempo real de la cadena de suministro física. No solo herramientas de optimización, son instrumentos de respuesta a incidentes. Cuando un ataque compromete un nodo, el Gemelo Digital permite simular en minutos el impacto en toda la red y tomar decisiones de rerouting antes de que la disrupción escale.

DELTA PROTECT®

Fuentes: IDC / Ikusi México, Jul 2025; ITware LATAM / Check Point, Abr 2026; Novasec, May 2026.

MANUFACTURA E INDUSTRIA

La manufactura no solo es el sector más atacado en México, es el más atacado en el mundo. Los incidentes de ransomware contra fabricantes aumentaron un **56% globalmente**, de 937 a 1,466 en 2025. La manufactura fue el **sector más atacado en México en 2025 con 1,284 casos documentados**. Los corredores de Monterrey, Querétaro, San Luis Potosí y el Bajío son geografías de alto riesgo.

La convergencia IT/OT: Las plantas industriales modernas han conectado sus sistemas de tecnología operativa (OT) (máquinas CNC, robots industriales, sistemas SCADA) a las mismas redes que la administración y el correo. Un ataque que empieza como phishing en el email administrativo puede terminar deteniendo una línea de producción completa.

El dato de gobernanza: solo el **16% de las organizaciones industriales** reporta incidentes OT a sus juntas directivas. El 84% opera con una brecha que mantiene a los decisores en la oscuridad sobre sus vulnerabilidades más críticas.

Un punto de inflexión regulatorio: La ciberseguridad está empezando a aparecer en los contratos comerciales entre empresas mexicanas y sus clientes en EE.UU. y Canadá. Proveedores que no puedan demostrar controles mínimos ya están siendo descalificados en procesos de contratación automotriz, aeroespacial y farmacéutico.

El sector manufactura, supply chain y transportación registra el **59% de adopción en automatización de operaciones de seguridad** por encima del promedio global del 43% . Es la buena noticia. La mala: en detección de intrusiones OT, análisis de comportamiento de usuarios y threat intelligence, el sector se ubica por debajo de servicios financieros y salud. La brecha no es de presupuesto, es de madurez operativa. Las plantas que automatizan alertas pero no segmentan redes IT/OT siguen siendo vulnerables al vector de ataque más común del sector.

Las 5 Medidas No Negociables para Plantas Industriales

- Separación física o lógica de redes IT y OT (microsegmentación)
- Inventario actualizado de todos los dispositivos conectados, incluyendo IoT industrial
- MFA en todos los accesos remotos, especialmente VPN
- Backups offline cifrados e inmutables que cubran toda la infraestructura OT
- ¿Cuántos días puede operar la planta en modo manual?

DELTA PROTECT®

Fuentes: Check Point, Manufacturing Threat Landscape 2025; FortiGuard Labs, Global Threat Report 2026; CódigoQro / Fortinet, May 2026.

HEALTHCARE Y FARMACÉUTICO

El sector salud lleva **12 años consecutivos** siendo el más costoso en ciberseguridad. Un expediente médico vale hasta **50 veces más que una tarjeta de crédito** en el mercado negro. Y los hospitales tienen una vulnerabilidad estructural que los hackers conocen perfectamente: no pueden apagar sus sistemas mientras atienden pacientes.

7.42m

COSTO PROMEDIO

De una brecha en salud, casi el doble del global ($4.88M)

279

DÍAS PROMEDIO

Para identificar y contener una brecha en salud

83%

DISPOSITIVOS

De imagenología médica con sistemas no soportados

$331B

MERCADO GLOBAL

De ciberseguridad en salud en 2026 (+20.7%)

La brecha regulatoria

En México no existe una NOM (Norma Oficial Mexicana) que contemple ciberseguridad para dispositivos médicos, ni obligaciones claras. Esto contrasta con la FDA (EE.UU.), la EMA (Europa) y las directrices de la OMS, que ya establecen requisitos explícitos. México tiene una ventana de oportunidad para establecer regulación antes de que sea forzada por incidentes de mayor escala.

Oportunidad: Datos Sintéticos

Para la industria farmacéutica mexicana, una de las más grandes de LATAM, los datos sintéticos representan la solución para acelerar R&D sin comprometer la privacidad del paciente. Un laboratorio puede entrenar modelos de predicción de respuesta a fármacos usando datos sintéticos que preservan los patrones estadísticos reales sin contener información identificable.

DELTA PROTECT®

Fuentes: IBM Cost of a Data Breach 2025; Delta Protect, Abr 2026; IQSEC / Sisnova; MundoFarma / COFEPRIS análisis, Dic 2025.

GOBIERNO
MÉXICO BAJO LUPA

México ya no es un objetivo futuro.
Es un objetivo activo.

México es el segundo país más atacado de América Latina (WEF 2026). Entre 2024 y 2025, los incidentes crecieron un 78%. En abril de 2026 se reportaron más de **50 filtraciones de información y 4 casos documentados de ransomware** solo en ese mes. La cifra que resume la vulnerabilidad estructural: **750 vulnerabilidades** fueron detectadas en instituciones federales en 2025, y la ATDT tuvo que eliminar **25 portales fraudulentos** que suplantaban servicios gubernamentales ese mismo año.

Lo más alarmante: el gobierno federal documentó la brecha, **pero recortó presupuestos**. Al menos 6 dependencias sufrieron incidentes de ciberseguridad entre 2022 y 2025, y 5 de ellas redujeron sus recursos. La SICT, que fue atacada con ransomware, recortó su presupuesto de informática un **85%:** de ~1,800 millones de pesos a ~260 millones.

La peor filtración de datos biométricos de la historia del país: **2.3 terabytes de información confidencial** de más de **25 instituciones** circulando en foros de la dark web. En el ranking internacional: México ocupa el **segundo lugar en LATAM en víctimas publicadas en foros criminales de ransomware** 155 organizaciones comprometidas entre 2019 y 2025.

Publicado el 4 de diciembre de 2025 por la ATDT bajo el gobierno de la Presidenta Sheinbaum. **Obligatorio desde el 18 de diciembre de 2025.** La estrategia nacional anterior data de 2017 — 9 años sin actualización. El Plan establece: Consejo Nacional de Ciberseguridad, CSOC nacional, CSIRT federal, notificación obligatoria de incidentes en 24 horas, y una hoja de ruta a 2030 para convertir a México en referente regional. Aunque el enfoque inicial es la APF, sus ondas de choque alcanzan al sector privado: empresas tecnológicas que proveen a gobierno, sectores regulados y cadenas de suministro con instituciones públicas.

El Mundial FIFA 2026 — La Prueba de Fuego de México

México co-organiza la Copa Mundial con EE.UU. y Canadá. Proyecciones: hasta **30 millones de ciberataques durante el torneo**, con foco en ataques geopolíticos, campañas de desinformación masiva y DDoS potenciados por IA. Para las empresas mexicanas en cadenas de infraestructura turística, financiera y de comunicaciones, el Mundial no es un evento de entretenimiento, es una ventana de ataque abierta.

DELTA PROTECT®

Fuentes: Plan Nacional de Ciberseguridad 2025-2030 (ATDT, dic 2025); Infobae México, abr 2026; IMEF, feb 2026; Etcetera, dic 2025; DigitNow, ene 2026.

Vectores de Amenaza Futura: El Horizonte 2030

Sistemas autónomos y robótica: El 26% ya los identifica como de impacto en 2026, con crecimiento acelerado. La superficie de ataque físico-digital continúa expandiéndose.

Tecnologías cuánticas: El 37% cree que afectarán la ciberseguridad en los próximos 12 meses. Gartner predice que los avances cuánticos rendirán la criptografía asimétrica insegura antes de 2030. Los ataques "harvest now, decrypt later" ya están ocurriendo (datos robados hoy para descifrarlos cuando la cuántica alcance escala comercial).

Tecnologías espaciales y cables submarinos: Solo el 15% los considera en su planificación de riesgo, a pesar de que soportan el 99% del tráfico de datos internacional. Una interrupción deliberada representaría una disrupción económica sin precedentes.

Monedas digitales: Infraestructura crítica emergente con alta vulnerabilidad a ataques sistémicos, especialmente relevante en América Latina donde la adopción de activos digitales crece por encima del promedio global.

Fuente: WEF + Accenture, Global Cybersecurity Outlook 2026; Gartner, Top Cybersecurity Trends 2026.

05. DEL DIAGNÓSTICO A LA ACCIÓN

La Brecha de Talento: La Mayor del Mundo

LATAM tiene la **brecha de talento en ciberseguridad más amplia de todas las regiones:** el 65% de las empresas carece de las habilidades para cumplir sus objetivos. La brecha global asciende a **4.8 millones de profesionales** que simplemente no existen.

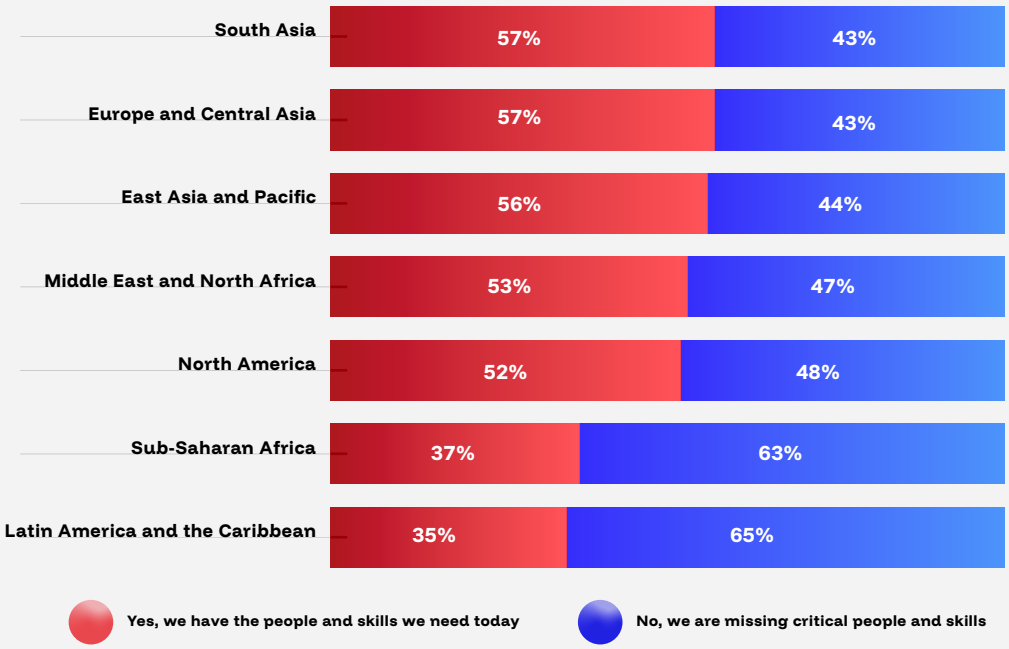
Los tres roles más escasos en LATAM, con el mayor déficit comparado con cualquier otra región del mundo:

- **Analista de inteligencia de amenazas:** anticipación de ataques antes de que ocurran
- **Ingeniero de DevSecOps:** LATAM lidera globalmente en déficit de este perfil
- **Respondedor de incidentes:** LATAM también lidera globalmente en escasez de este rol

El impacto diferencial por tamaño de empresa: las organizaciones con menos de **250 empleados** tienen **3 veces más probabilidad** de carecer de habilidades necesarias. Solo el **21%** de organizaciones pequeñas tiene ciberseguro, frente al **85% de las grandes**.

La paradoja de liderazgo: el **92% de las Juntas Directivas** en LATAM ya está comprometido activamente con ciberseguridad. El problema no es falta de interés en la cima, es la falta de capacidad operativa para ejecutar. El 39% ya está usando IA para compensar esta brecha, confirmando que la IA no es opcional: es la única palanca escalable disponible dado el déficit estructural.

¿Cuenta su organización con el talento necesario para alcanzar sus objetivos actuales de ciberseguridad?



En México, donde manufactura y servicios financieros son los dos sectores más atacados, operar con dos de cada tres posiciones de seguridad sin cubrir no es una proyección de riesgo, es la condición operativa actual. Los tres roles más críticos que faltan: analista de threat intelligence, ingeniero de DevSecOps y respondedor de incidentes — precisamente los perfiles que se necesitan cuando el ataque ya está en curso.

Fuente: WEF + Accenture. Global Cybersecurity Outlook 2026 — Latin America and the Caribbean Regional Analysis. Febrero 2026.

Los 5 Imperativos Estratégicos para el Liderazgo (IBM IBV 2025)

El IBM Institute for Business Value, tras encuestar a más de 200 CISOs y 500+ CEOs/CFOs/COOs, identifica cinco imperativos que separan a las organizaciones resilientes de las vulnerables:

1. **Integrar seguridad en cada fase de diseño y construcción.** Usar IA para automatizar gobernanza, detectar anomalías y disparar respuestas en tiempo real. No como capa final, sino como requisito de origen.
2. **Conectar arquitectura y operaciones con visibilidad compartida.** Estandarizar prácticas de código seguro y garantizar que los loops de retroalimentación de incidentes informen mejoras de diseño continuas. Cerrar el silo es condición sine qua non.
3. **Integrar partners y proveedores en un marco de seguridad unificado.** Aplicar principios SbD a proveedores, MSSPs y servicios externos de IA. El ecosistema es tan fuerte como su eslabón más débil.
4. **Vincular el patrocinio ejecutivo con ejecución accountable.** El 67% de las organizaciones señala la falta de patrocinio ejecutivo como su principal barrera para escalar.
5. **Unir IA y Secure by Design para construir sistemas auto-defensivos.** Usar agentes de IA para modelado contextual de amenazas y análisis "what-if". Priorizar transparencia y auditabilidad.

Los 3 Gaps que Frenan el Progreso

Gap 1 - Fricción del practicante: Las capacidades están construidas, pero problemas de usabilidad e integración impiden que los equipos las traduzcan en valor real. Un SIEM que nadie usa es peor que no tenerlo.

Gap 2 - Brecha percepción vs. rendimiento: Las organizaciones sobreestiman o subestiman dramáticamente su postura de seguridad. Los programas SbD funcionan como catalizadores culturales al dar un marco de referencia común y medible.

Gap 3 - Brecha de eficacia: Las organizaciones han construido capacidades que puntúan 5 puntos más alto que sus resultados reales, están dejando ganancias sobre la mesa. Las plataformas avanzadas generan retornos mínimos porque están subutilizadas.

El ROI de hacerlo bien

69% de organizaciones con programas SbD reportan mayor ROI en nuevos productos. 72% reporta mejoras en GRC. Las 3 mejoras de eficiencia más citadas: respuesta a incidentes más rápida (58%), operaciones simplificadas (53%) y mayor visibilidad de riesgos (52%).

Fuente: IBM Institute for Business Value + Microsoft, "Secure by Design, Smarter with AI", Q3 2025.

El Marco Mythos-ready: 11 Acciones Prioritarias para el CISO

El CSA CISO Community, SANS, OWASP y más de 80 CISOs globales publicaron en abril 2026 el primer framework operativo para preparar programas de seguridad ante la nueva era de amenazas autónomas por IA. Se organiza en tres horizontes:

Esta semana (acciones inmediatas)

- **Apuntar agentes de IA hacia el propio código y pipelines**, revisión de seguridad con LLM antes de cada merge.
- **Exigir adopción formal de agentes de coding** en todas las funciones de seguridad (no solo programación, también GRC y respuesta a incidentes).
- **Establecer gobernanza de innovación:** mecanismo cross-funcional para onboarding acelerado de controles defensivos.
- **Prepararse para patching continuo:** Proyecto Glasswing ya liberó acceso anticipado a Mythos a 40 vendors.
- **Actualizar modelos de riesgo:** los supuestos pre-IA sobre ventanas de parche ya no son válidos.

Este mes (45 días)

- **Defender los propios agentes:** definir límites de blast-radius, lógica de escalación y override humano antes de cualquier despliegue en producción.
- **Inventariar y reducir la superficie de ataque:** generar SBOMs reales, eliminar funcionalidades no mantenidas, aislar sistemas de alto riesgo.

90 días — 12 meses (programa estructural)

- **Endurecer el entorno:** segmentación, filtrado de egreso, Zero Trust, MFA resistente a phishing.
- **Construir capacidad de detección temprana** (deception: canaries, honey tokens).
- **Establecer respuesta automatizada:** playbooks que ejecuten a velocidad de máquina.
- **Establecer VulnOps (Vulnerability Operations):** función permanente, como DevOps pero para descubrimiento y remediación autónoma de vulnerabilidades.

💡 VulnOps — El Concepto Operativo Más Relevante de 2026

El pentesting anual ya es insuficiente — se necesita una función continua de descubrimiento de vulnerabilidades, tan automatizada como el pipeline de CI/CD.

Fuente: CSA CISO Community / SANS / OWASP, "The AI Vulnerability Storm: Building a Mythos-ready Security Program", abril 2026. Versión 0.95.

Project Glasswing: VulnOps a Escala Industrial | El Caso Real

Project Glasswing no es solo el ejemplo más relevante de VulnOps en 2026, es la demostración más convincente de por qué el concepto existe. Anthropic usa Claude Mythos Preview para escanear continuamente más de **1,000 repositorios open-source críticos**. En semanas, encontró más vulnerabilidades que años de auditorías manuales combinadas.

El modelo de VulnOps que Project Glasswing ilustra para cualquier organización:

- **Descubrimiento continuo:** No escaneos trimestrales, revisión permanente y autónoma del código. Mythos corre contra el corpus OSS-Fuzz de forma regular, sin intervención humana entre ciclos.
- **Divulgación responsable coordinada:** Anthropic divulgó 1,596 vulnerabilidades directamente a los mantenedores del software antes de hacerlas públicas, el proceso de remediación empieza antes de que el atacante sepa que existe el bug.
- **Comunidad de defensores:** 40+ organizaciones comparten hallazgos para elevar el piso de seguridad de toda la industria, no solo el de sus propias organizaciones.

El dato que cierra el argumento: **más del 99% de las vulnerabilidades que Mythos ha descubierto permanecen sin parchear**. No porque nadie las conozca, sino porque el ritmo de descubrimiento ya superó la capacidad humana de remediación. VulnOps no es una aspiración en este entorno: es la única respuesta estructural posible al colapso del tiempo de explotación. El pentesting anual no cierra esa brecha. Solo una función continua, automatizada y coordinada puede hacerlo.

Fuentes: Anthropic, Project Glasswing, abr 2026 · Cyberpress · ZeroFox · ArmorCode · CSA Labs

Hoja de Ruta Práctica por Horizonte Temporal

El Test de los 8 Minutos: ¿Qué ya comprometió un atacante?

En febrero de 2026, Sysdig documentó un ataque asistido por IA que alcanzó acceso de nivel administrador en 8 minutos. Basado en esa evidencia, este ejercicio de pensamiento está diseñado para que cualquier C-Level entienda su exposición real, sin necesitar ser experto técnico.

El escenario: Un atacante con herramientas de IA entró a tu red hace 8 minutos. Empieza a moverse lateralmente. ¿Qué puede comprometer en ese tiempo?

HORIZONTE	PRIORIDAD	ACCIÓN CONCRETA	RESPONSABLE	INDICADOR DE ÉXITO
0–90 días	Alta	Diagnóstico de madurez (WEF Cyber Compass) — ¿estás entre el 19% que supera requisitos o el 25% con resiliencia insuficiente en LATAM?	CISO / CEO	Score basal documentado vs. benchmark WEF
0–90 días	Alta	Inventario de activos de IA en producción — incluyendo Shadow AI y agentes no autorizados	CTO / CISO	100% activos catalogados
0–90 días	Alta	Actualizar procesos de autorización de pagos: eliminar llamada telefónica como único factor de verificación	CFO / CISO	Protocolo de doble verificación activo
90–180 días	Alta	Implementar Zero Trust en accesos críticos — comenzar con VPN y webmail	CISO	MFA en 100% sistemas core
90–180 días	Alta	Simular un incidente de ransomware completo con playbook de respuesta	CISO / CEO	Playbook probado y validado por Junta
90–180 días	Media	Programa de upskilling en IA + ciberseguridad para equipos	CHRO / CTO	80% equipo capacitado
12 meses	Alta	Establecer VulnOps: función continua de descubrimiento y remediación de vulnerabilidades	CISO	Ciclo mensual de revisión activo
12 meses	Alta	Evaluación de cumplimiento Plan Nacional Ciberseguridad 2025–2030	Legal / CISO	Gap analysis documentado
12 meses	Media	Evaluación de cumplimiento EU AI Act (si exportas a Europa o tienes socios europeos)	Legal / CISO	Clasificación de sistemas de IA completada

06. EL FUTURO DE LA RESILIENCIA OPERATIVA

La ciberseguridad y la IA ya no son funciones técnicas aisladas; son **preocupaciones estratégicas, económicas y sociales** que exigen una acción coordinada. La verdadera resiliencia no reside en nunca ser atacado, sino en haber construido una estructura capaz de absorber el impacto, aprender y recuperarse con velocidad.

Imperativo Económico: En 2025, el cibercrimen superó por primera vez el umbral de los $20 mil millones: **$20.877** billones en pérdidas solo en denuncias al FBI IC3 (+26% vs. 2024). El costo del ciberataque empresarial promedio ya supera los **$250,000 USD**. El Banco Mundial calcula que mejorar la ciberseguridad podría aumentar el PIB per cápita en un **1.5% en economías en desarrollo**, incluyendo México.

El DNA de la Organización Resiliente: Solo el **19% de organizaciones** supera sus requisitos mínimos de resiliencia. El WEF 2026 documenta con precisión qué las diferencia — y el patrón empieza en la percepción del propio CEO.

Which cyber risks concern you most for your organization?	High resilience (rank)	Insufficient resilience (rank)
AI vulnerabilities	1	4
Cyber-enabled fraud and phishing	2	1
Supply chain disruption	3	7
Exploitation of software vulnerabilities	4	3
Ransomware attack	5	2
Insider threat	6	6
Denial-of-service attacks	7	5

Esta tabla muestra cómo cambia la percepción de riesgo de un CEO según el nivel de resiliencia de su organización. Los CEOs de organizaciones altamente resilientes ponen las vulnerabilidades de IA en el #1 y la disrupción de cadena de suministro en el #3. Los CEOs de organizaciones con resiliencia insuficiente aún tienen el ransomware en el #2 y la cadena de suministro en el #7, ni siquiera está en su radar. La agenda del CEO no es una opinión: es un diagnóstico. Lo que un CEO pone en el #1 revela el nivel de madurez de toda su organización.

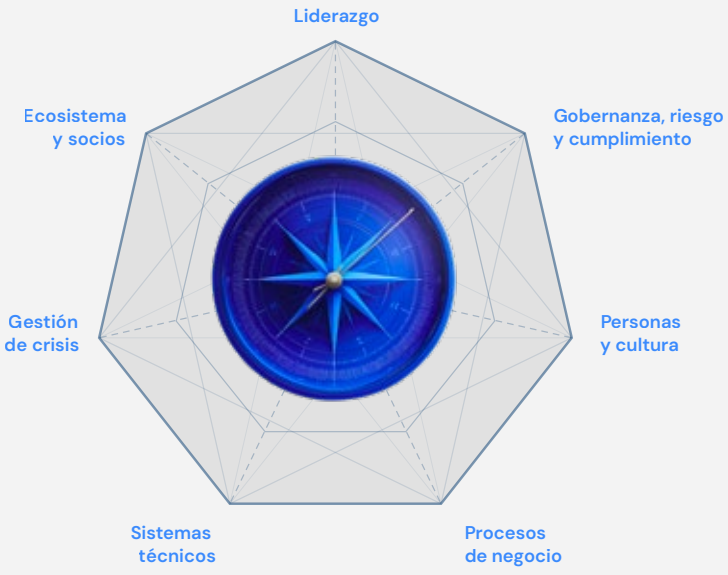
Fuente: WEF + Accenture. Global Cybersecurity Outlook 2026, Table 3, p.11.

Esto confirma lo que la experiencia operativa demuestra en campo: las organizaciones resilientes no son más resilientes porque gastaron más, son más resilientes porque sus líderes tienen el mapa de amenazas correcto. El primer paso para cerrar la brecha no es tecnológico, es de percepción.

Práctica	Altamente Resilientes	Resiliencia Insuficiente
Evalúan seguridad de IA antes de desplegar	83%	39%
Evalúan madurez de seguridad de proveedores	74%	48%
Simulan incidentes con socios del ecosistema	44%	16%
Junta directiva activamente involucrada	99%	-

La brecha no está en el presupuesto ni en la tecnología. Está en los procesos, la gobernanza y la cultura. **Solo el 27% de todas las organizaciones** simula incidentes cibernéticos regularmente. En un entorno donde el tiempo de explotación es de horas, un playbook no probado es un playbook que fallará.

Cultura de Confianza: El 34% de organizaciones ofrece apoyo formal a socios pequeños para elevar la resiliencia de toda la red. El 98% de las organizaciones está conectada con al menos un tercero que fue atacado en 2 años. La ciberseguridad es, en última instancia, un bien público.



La brújula muestra estructura. Las organizaciones resilientes no lo son porque compraron la mejor tecnología: lo son porque tienen las 7 dimensiones alineadas simultáneamente. La mayoría de las organizaciones en México y LATAM invierten en sistemas técnicos y en gestión de crisis cuando el incidente ya está en curso. Las dimensiones que consistentemente se descuidan son las que más determinan el resultado real:

People and culture: la conciencia y comportamiento humano

Ecosistema: la seguridad de la cadena de suministro y socios

Gobernanza, riesgo y cumplimiento: el marco que convierte la seguridad en una decisión de negocio, no de TI.

La distancia entre donde apunta la aguja de la mayoría de las organizaciones y donde apunta la de las más resilientes no es de tecnología: es de cultura, gobernanza y ecosistema.

Fuentes: WEF + Accenture, GCO 2026; FBI IC3 2025; BID + OEA + Oxford, LATAM 2025.

ANEXO A

Guía de Autoevaluación de Madurez

Marco basado en el Cyber Resilience Compass del WEF y el CMM del BID/OEA/Oxford. Diagnostica tu organización frente a los líderes del mercado y el benchmark regional LATAM:

DIMENSIÓN	PREGUNTA DE DIAGNÓSTICO	BENCHMARK LÍDERES (GLOBAL)	BENCHMARK LATAM	TU SCORE
Liderazgo	¿La Junta Directiva recibe actualizaciones regulares y está comprometida activamente?	99% (altamente resilientes)	92% (promedio LATAM)	☐
Gobernanza de IA	¿Evalúan la seguridad de herramientas de IA antes de desplegarlas?	83% (altamente resilientes)	49% (solo la mitad en LATAM)	☐
Talento	¿Cuenta con las personas y habilidades críticas para sus objetivos actuales?	78% (global)	35% (LATAM mayor brecha global)	☐
Procesos	¿Involucra a seguridad desde el inicio del proceso de adquisiciones?	76% (global)	58% (LATAM)	☐
Cadena de Suministro	¿Evalúa la madurez de seguridad de sus proveedores?	74% (altamente resilientes)	52% (LATAM)	☐
Respuesta a Incidentes	¿Tiene planificación documentada y probada de respuesta y recuperación ante incidentes?	44% simula con socios (global)	65% tiene planificación suficiente (LATAM lidera en déficit global)	☐
Resiliencia	¿Su resiliencia cibernética supera los requerimientos mínimos?	19% (global)	Solo 12% en LATAM	☐

ANEXO B

15 Preguntas que Todo CEO debe Hacerle a su CISO

Sobre Gobernanza y Postura

1. ¿Cuál es nuestra postura real de ciberseguridad hoy, no la aspiracional, sino la documentada con datos métricos?
2. ¿Cómo nos comparamos con las 5 dimensiones del WEF Cyber Resilience Compass? ¿En qué somos líderes y dónde están las brechas más grandes?
3. ¿Tenemos un inventario completo de todos los activos digitales, incluyendo herramientas de IA en uso? ¿Sabemos quién tiene acceso a qué?

Sobre IA y Nuevas Amenazas

1. ¿Qué herramientas de IA está usando nuestra gente hoy, con o sin autorización? ¿Tenemos un proceso para evaluarlas antes de usarlas?
2. ¿Cómo autorizo una transferencia bancaria si recibo una llamada de un "directivo" solicitando urgencia? ¿Existe un protocolo de verificación secundaria?
3. ¿Monitoreamos los inputs y outputs de los modelos de IA de terceros que usamos? ¿O son cajas negras?

Sobre Resiliencia y Respuesta

1. ¿Cuánto tiempo tardaríamos en detectar que estamos siendo atacados ahora mismo? ¿Y en contener el ataque?
2. ¿Tenemos un playbook de respuesta a incidentes probado y ejercitado con simulacros reales? ¿Cuándo fue el último simulacro?
3. ¿Qué pasa con nuestra operación si mañana cifraran todos nuestros sistemas con ransomware? ¿Cuántos días tardaríamos en recuperarnos?

Sobre la Cadena de Suministro

1. ¿Sabemos cuál es la postura de seguridad de nuestros 10 proveedores más críticos? ¿Los auditamos?
2. ¿Cuáles de nuestros proveedores tienen acceso a nuestros sistemas? ¿Con qué nivel de privilegio?

Sobre Talento y Presupuesto

1. ¿Tenemos el talento necesario para operar en el entorno actual? ¿Qué roles críticos nos faltan: analista de amenazas, DevSecOps, respondedor de incidentes?
2. ¿Qué porcentaje del presupuesto de TI se destina a ciberseguridad? (Benchmark: 10-15% para organizaciones expuestas)

Sobre Regulación y Cumplimiento

1. ¿Qué regulaciones nos aplican en 2026 que no nos aplicaron en 2024? ¿EU AI Act, Plan Nacional de Ciberseguridad, CNBV?
2. ¿Si mañana tuviéramos un incidente grave, qué dependencias debemos notificar, en qué plazo y con qué información?

ANEXO C

Glosario del C-Suite — Términos Clave de IA y Ciberseguridad

TÉRMINO	DEFINICIÓN EJECUTIVA
Agente de IA / IA Agéntica	Sistema de IA que toma decisiones y ejecuta acciones de forma autónoma. Puede controlar otros sistemas, hacer llamadas a APIs y encadenar acciones sin intervención humana entre pasos.
AI Stack	El conjunto completo de tecnologías que soportan un sistema de IA: datos, modelos, aplicaciones e infraestructura. Cada capa es una superficie de ataque distinta.
BEC (Business Email Compromise)	Fraude donde el atacante se hace pasar por un ejecutivo o proveedor (vía email o voz clonada) para solicitar transferencias bancarias o datos sensibles. Causó $3.046B en pérdidas en 2025.
CISO	Chief Information Security Officer. El máximo responsable de ciberseguridad en la organización. Reporta idealmente al CEO o al Consejo Directivo.
CMM	Cybersecurity Capacity Maturity Model. Marco de Oxford para evaluar la madurez de ciberseguridad nacional en 5 dimensiones y 5 niveles. La mayoría de países LATAM está entre niveles 2 y 3.
Data Poisoning	Ataque donde se introducen datos falsos o sesgados en el dataset de entrenamiento de un modelo de IA, corrompiendo sus decisiones de forma permanente.
Deepfake	Contenido audiovisual falso generado por IA que imita con alta precisión la apariencia o voz de una persona real. Usado para fraudes de identidad, BEC y desinformación.
EDR	Endpoint Detection & Response. Herramienta de seguridad que monitorea comportamiento en dispositivos en tiempo real y responde automáticamente ante actividad sospechosa.
Model Jailbreak	Técnica para hacer que un modelo de IA ignore sus restricciones de seguridad mediante instrucciones ingeniosamente formuladas.
Prompt Injection	Ataque donde instrucciones maliciosas se insertan en los inputs que recibe un modelo de IA, manipulando su comportamiento para revelar información o ejecutar acciones.
RAG (Retrieval-Augmented Generation)	Arquitectura que permite a la IA consultar documentos internos en tiempo real para responder preguntas, sin que la información salga del entorno seguro. La alternativa a conectar IA a modelos públicos con datos confidenciales.
Ransomware	Malware que cifra los sistemas de la víctima y exige un rescate para restaurar el acceso. En 2025 surgieron 63 variantes nuevas, una cada 5 días.
SbD (Secure by Design)	Filosofía de diseño donde la seguridad se integra desde el origen del código, los procesos y los sistemas, en lugar de añadirse como capa posterior.
Shadow AI	Uso de herramientas de IA no autorizadas por TI o seguridad, creadas por empleados sin visión ni control corporativo.
SIEM	Sistema de gestión de información y eventos de seguridad. Correlaciona logs y alertas de múltiples fuentes para detectar anomalías en tiempo real.
SOC (Security Operations Center)	Centro de operaciones de seguridad donde analistas monitorizan en tiempo real las amenazas y coordinan la respuesta a incidentes.
VulnOps	Vulnerability Operations. Función emergente equivalente a DevOps pero para descubrimiento y remediación continua de vulnerabilidades. La respuesta al colapso del tiempo de explotación.
Zero Trust	Modelo de seguridad que elimina la confianza implícita: todo acceso se verifica de forma continua y contextual antes de ser otorgado. Principio: "nunca confiar, siempre verificar".
Zero-Day	Vulnerabilidad desconocida para el fabricante del software. No existe parche cuando es explotada por primera vez, en 2026 la ventana de exposición se mide en horas.

FUENTES Y REFERENCIAS BIBLIOGRÁFICAS

1. World Economic Forum + Accenture. Global Cybersecurity Outlook 2026. Geneva: WEF, enero 2026. 804 participantes, 92 países, 316 CISOs, 105 CEOs.
2. World Economic Forum + Accenture. Global Cybersecurity Outlook 2026 — Análisis Regional LATAM y el Caribe. Febrero 2026.
3. Momentum Cyber. AI Security Capital Markets Report: An Analysis of Financing Acceleration and Premium Valuations. Austin: Momentum Cyber Group, marzo 2026.
4. CSA CISO Community, SANS Institute, OWASP Gen AI Security Project, [un]prompted. The "AI Vulnerability Storm": Building a "Mythos-ready" Security Program. Cloud Security Alliance, 18 abril 2026. Versión 0.95.
5. IBM Institute for Business Value + Microsoft. Secure by Design, Smarter with AI. +1,000 ejecutivos C-suite, 20 industrias, 18 países. Q3 2025.
6. IBM Security / Ponemon Institute. Cost of a Data Breach Report 2025. Julio 2025.
7. IBM Security. X-Force Threat Intelligence Index 2026. Febrero 2026.
8. FBI. Internet Crime Report 2025 (IC3). Washington D.C.: FBI Cyber Division, 2025.
9. Banco Interamericano de Desarrollo (BID) + Organización de Estados Americanos (OEA) + Oxford GCSCC. Cybersecurity Report LATAM & the Caribbean 2025. Diciembre 2025. 30 países, metodología CMM.
10. Gartner. Top Trends in Cybersecurity for 2026. Febrero 2026.
11. Gartner. Forecast: Information Security, Worldwide, 2023–2029. Gasto 2026: $244.2B. Diciembre 2025.
12. Gartner. AI Spending Worldwide: $2.52 trillones en 2026. Enero 2026.
13. Gobierno de México / ATDT-DGCiber. Plan Nacional de Ciberseguridad 2025-2030. Presentado 4 dic 2025. Obligatorio desde 18 dic 2025.
14. IT-Harvest / Richard Stiennon. Guardians of the Machine Age. Citado en Momentum Cyber, 2026.
15. Zero Day Clock (zerodayclock.com) / Sergej Epp. Visualización del colapso del tiempo de explotación. Lanzado marzo 2026.
16. Check Point Software Technologies. Manufacturing Threat Landscape 2025. Abril 2026.
17. FortiGuard Labs. Global Threat Landscape Report 2026. Mayo 2026.
18. Rockwell Automation. Oportunidades y riesgos de ciberseguridad en entornos OT — América Latina. Marzo 2026.
19. IDC / Ikusi México. Ciberseguridad: riesgo clave para la manufactura en México. Julio 2025.
20. Infobae México. Ciberseguridad en México al límite: aumentan los ataques, cae la inversión y falla la estrategia. Abril 2026.
21. IMEF. Plan Nacional de Ciberseguridad y el Mundial 2026: el riesgo que nadie está midiendo. Febrero 2026.
22. Etcetera. México lanza su Plan Nacional de Ciberseguridad, pero llega tarde y con vacíos estratégicos. Diciembre 2025.
23. Gambit. Reporte sobre el compromiso de infraestructura gubernamental mexicana mediante IA. Febrero 2026. (Pendiente obtener PDF completo.)
24. Google Threat Intelligence Group (GTIG). GTIG AI Threat Tracker: Adversaries Leverage AI for Vulnerability Exploitation, Augmented Operations, and Initial Access. Google Cloud Blog, 11 mayo 2026. cloud.google.com/blog/...
25. MundoFarma. Protección digital en salud: hacia una política nacional de ciberseguridad médica. Diciembre 2025.
26. Novasec. Ciberseguridad en México 2026: el GRC ya no es opcional. Mayo 2026.

DELTA PROTECT®

Delta Protect es una empresa mexicana de ciberseguridad que protege a negocios en México y LATAM mediante servicios como pentesting, cumplimiento normativo, certificaciones, evaluaciones de riesgo y monitoreo SOC. Hemos apoyado a más de 300 empresas en 8 países a fortalecer su seguridad y generar confianza. Nuestra misión es hacer la ciberseguridad simple, escalable y efectiva, construyendo un futuro digital más seguro para todos.

Delta Protect | @delta.protect | @DeltaProtect | www.deltaprotect.com

Comienza a proteger tu empresa hoy →

ANIA

La Alianza Nacional de Inteligencia Artificial (ANIA) es un mecanismo líquido, multisectorial, que reconoce y fortalece el ecosistema de inteligencia artificial en México con una perspectiva integral, plural y multidisciplinaria.
En la ANIA creemos que la Inteligencia Artificial debe ser un motor de transformación, bienestar y progreso.

ÚNETE →

ANIA | @ANIAMEXICO | @Alianza Nacional de Inteligencia Artificial