itseller.mx

EDICION ANUAL

CIBERSEGURIDAD

Un examen profundo sobre los imperativos de seguridad y la resiliencia de la infraestructura digital crítica en las organizaciones de México; una radiografía actualizada de las amenazas emergentes y las estrategias de defensa que están definiendo el ecosistema TI nacional.

PARTICIPAN DEL INFORME

SUMARIO

4 | CIBERSEGURIDAD:EL GRAN REINICIO DE LA CIBERDEFENSA BAJO LA LUPA DE LA IA

Oscar Suárez
Director Ejecutivo
osuarez@mediaware.org

Matias Perazzo
Director ITseller México
mperazzo@mediaware.org

Andrea Sánchez
Marketing & Content Estrategy - México
asanchez@mediaware.org

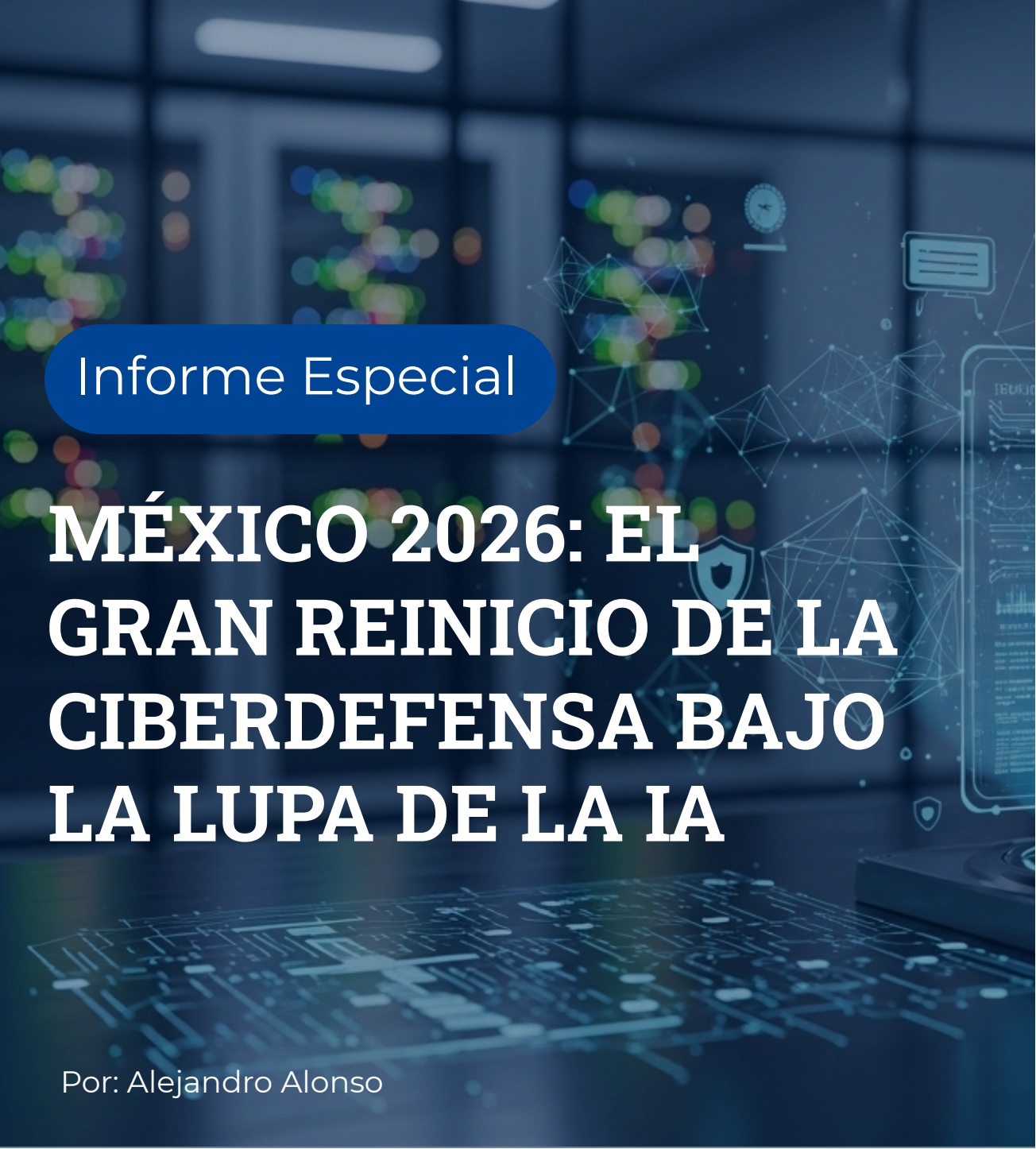
Para publicar en este medio:
www.itseller.mx/publique-aqui-2/

Edita, comercializa y distribuye:

mediaware

AVENIDA PRES ROQUE SAENZ PEÑA 1145.
C1035AAG Edificio Diagonal Plaza . Piso 2
Buenos Aires - Argentina.

enfasys itseller ITWARE LATAM.COM enretail HOGAR & ELECTRO



Informe Especial

MÉXICO 2026: EL GRAN REINICIO DE LA CIBERDEFENSA BAJO LA LUPA DE LA IA

Por: Alejandro Alonso

Con un mercado que roza los US$ 3,900 millones y las empresas destinando el 38.5% de su presupuesto de innovación a protegerse, la ciberseguridad deja de ser un nicho para convertirse en el motor principal del canal. Analizamos cómo el déficit de talento y la urgencia de servicios administrados (MSSP) en el sector público abren una ventana de oportunidad histórica para los integradores en 2026.

Del auge de la IA autónoma a la protección crítica de plantas industriales por el nearshoring: el mapa de la ciberdefensa en México se redibuja. Mientras el sector privado acelera hacia marcos de Zero Trust, la consolidación de la nueva Ley General de Ciberseguridad y el gasto gubernamental en servicios administrados definen las reglas de un juego donde el canal es el árbitro indispensable.

El asedio digital: México frente a sus pares regionales

El panorama regional muestra una competencia feroz por la resiliencia. Según el informe **Annual Threat Report 2026 de Darktrace**, aunque Colombia se ha posicionado recientemente como el país más impactado de la región, Ecuador, Chile y México mantienen una posición crítica como los siguientes blancos favoritos de los ataques de ransomware en Latinoamérica.

Este protagonismo no es para presumir: entre 2019 y 2025, el país acumuló 155 víctimas documentadas en foros de la dark web, una cifra superada únicamente por las 320 víctimas registradas en Brasil (DGCiber, 2025). La diferencia radica en la madurez; mientras Brasil ha avanzado en legislaciones de protección de datos robustas, México apenas está consolidando su arquitectura legal bajo la recién creada Agencia de Transformación Digital y Telecomunicaciones (ATDT).

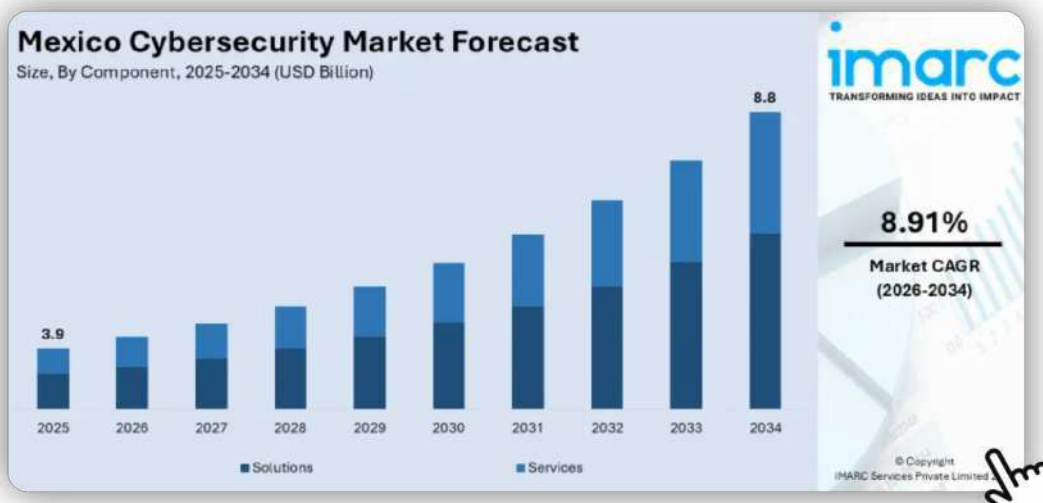
El mercado mexicano: inversión vs. realidad

De acuerdo con las estimaciones más recientes de **IMARC Group (2026)**, el mercado de ciberseguridad en México ha alcanzado una valoración de aproximadamente US$ 3.9 mil millones en 2025. Se proyecta que esta industria mantenga un ritmo de expansión sostenido, con una tasa de crecimiento anual compuesta (CAGR) del 8,9% hacia la próxima década, consolidando al país como uno de los polos de inversión tecnológica más dinámicos de Latinoamérica.

Este crecimiento está impulsado principalmente

por la acelerada migración a servicios en la nube y la proliferación de dispositivos IoT en los sectores industrial y de servicios. La creciente frecuencia de las filtraciones de datos ha generado una presión sin precedentes sobre las empresas mexicanas para que refuercen sus infraestructuras, transformando la ciberseguridad de un componente técnico periférico a un pilar estratégico indispensable para la continuidad del negocio.

Mirando hacia el futuro, el análisis de IMARC destaca que la demanda se concentrará en soluciones de seguridad basadas en la nube y marcos de trabajo de "Zero Trust". A medida que las organizaciones locales enfrentan amenazas cada vez más

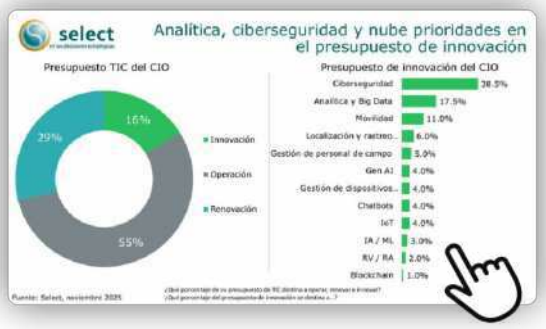


más automatizadas, la inversión se desplazará hacia tecnologías preventivas capaces de neutralizar ataques en tiempo real, protegiendo así la integridad de los datos financieros y personales de millones de ciudadanos.

Inversiones privadas y públicas

Según Select, a pesar de las amenazas, el mercado mexicano de ciberseguridad está en un momento de efervescencia. Para los líderes tecnológicos (CIOs), la seguridad ya no es un "gasto", sino la prioridad absoluta, calificada con una importancia de 9.0 sobre 10 (Select, 2026). De acuerdo con su reporte **Panorama del mercado de ciberseguridad 2025,** las empresas están destinando el 38,5% de su presupuesto de innovación exclusivamente a ciberseguridad, dejando atrás rubros como la Analítica (17,5%) o la Nube (16%).

Sin embargo, el Sector Público vive una realidad distinta. La inversión per cápita en ciberseguridad en México es menor a US$ 1,00, un abismo comparado con los US$ 30,00 que invierten países de ingresos altos como Estados Unidos (DGCiber, 2025). Esta brecha presupuestaria es, quizá, la mayor vulnerabilidad del Estado mexicano.



Ciberseguridad como Servicio: El auge de los MSSP

Ante la falta de talento especializado —un déficit global de 4 millones de profesionales que México sufre con rigor—, las organizaciones han volcado su confianza hacia la Ciberseguridad como Servicio.

El gasto en servicios administrados de seguridad alcanzará los $6,539 millones de pesos (MDP) para finales de 2026, lo que representa un crecimiento anual del 10,8% (Select, 2026). Curiosamente, es el Gobierno el mayor motor de este mercado, acaparando el 33% del gasto total, impulsado por la necesidad de modernizar sus 68 centros de respuesta a incidentes (CERTs/CSIRTs) identificados en el país (Select, 2026; DGCiber, 2025).

Sector	Cantidad	Porcentaje
Servicios de ciberseguridad	9	13.2%
Académico	8	11.8%
Consultoría	7	10.3%
Gubernamental Federal	4	5.9%
Telecomunicaciones	4	5.9%
Servicios Empresariales de TI	6	8.8%
Sistema Financiero	5	7.4%
Seguridad Pública Estatal	15	22.1%
Energía	3	4.4%
Sectores Especializados	5	7.4%
Tecnología y Software	2	2.9%
TOTAL	68	100%

Cantidad de CERTs y CSIRTs de México. Fuente: Agencia de Transformación Digital y Telñecomunicaciones, 2025.

Tecnologías de vanguardia: La IA como escudo y espada

La adopción tecnológica en 2026 está marcada por tres pilares fundamentales:

1- IA Generativa y Autonomía:

Según Darktrace (2026), los atacantes ya usan IA para crear deepfakes y automatizar el robo de credenciales. En respuesta, las empresas mexicanas están integrando soluciones de Detección y Respuesta Autónoma que aprenden del comportamiento del negocio en tiempo real.

2- Seguridad en OT (Tecnología Operacional):

Con el auge del nearshoring, sectores como manufactura y energía han comenzado a proteger sus plantas industriales con alianzas estratégicas (Select, 2026).

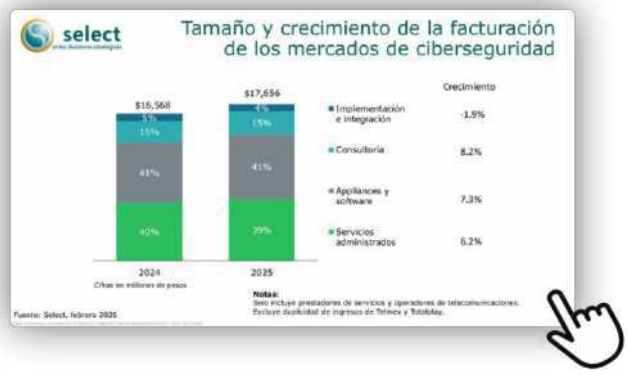
3- Consolidación de SOCs:

La Ciudad de México concentra el 62% de los centros de operación de seguridad del país, buscando una visibilidad unificada de las amenazas (DGCiber, 2025).

El Despertar legislativo: Hacia la Ley General

El mayor desafío no es técnico, sino legal. México ha operado durante años con vacíos normativos que la **Estrategia Nacional de Ciberseguridad 2025-2030** busca subsanar.

La creación de la Dirección General de Ciberseguridad (DGCiber) dentro de la ATDT es el primer paso hacia una Ley General de Ciberseguridad que se espera se materialice en este 2026.



Esta ley busca armonizar la protección de datos en bases públicas y privadas y establecer requisitos de seguridad obligatorios para infraestructuras críticas, un movimiento esencial para que México mantenga su competitividad frente a economías como la chilena o la brasileña, que ya cuentan con marcos legales avanzados (Darktrace, 2026; DGCiber, 2025).

México está en una encrucijada. Por un lado, una industria privada dispuesta a invertir y adoptar IA de vanguardia; por el otro, un sector público que lucha contra presupuestos limitados y un marco legal en construcción. La carrera hacia el Mundial de Fútbol 2026 será la prueba de fuego: un evento que pondrá a prueba la capacidad de coordinación de los 68 CSIRTs frente a la mirada de todo el mundo.

Referencias bibliográficas

itseller.mx

MEDIO DE NOTICIAS PARA EL CANAL TECNOLÓGICO DE MÉXICO.

- EVENTOS
- SERVICIOS DE MARKETING
- INFORMES ESPECIALES
- BOLETÍN DIGITAL

TODO LO QUE NECESITA EL CANAL PARA DESARROLLAR SU NEGOCIO.

HD LATINOAMÉRICA

"El fraude digital ya no es evidente y por eso la ciberseguridad debe replantearse en México"

HD Latinoamérica impulsa una estrategia que combina soluciones especializadas, plataformas digitales como Soga Cloud y programas de capacitación para fortalecer la ciberseguridad en México. El crecimiento de amenazas como phishing, robo de identidad y fraudes financieros, que ya representan hasta el 70% de los incidentes, obliga a empresas y canales a adoptar modelos más integrales para proteger a las pymes y asegurar la continuidad de sus operaciones.

La acelerada evolución de las amenazas digitales está redefiniendo las prioridades de protección para las empresas en México, particularmente en el segmento pyme, que representa más del 80% del tejido empresarial. Fausto Escobar, Director General de HD Latinoamérica, advirtió que los ataques han dejado de ser genéricos para convertirse en esquemas altamente dirigidos, apoyados por inteligencia artificial y técnicas avanzadas de ingeniería social. “El fraude digital ya no es evidente y por eso la ciberseguridad

FAUSTO ESCOBAR,
DIRECTOR GENERAL DE
HD LATINOAMÉRICA.

“Nuestra estrategia está enfocada en que los socios evolucionen hacia un rol consultivo, apoyados por plataformas como Soga Cloud y un portafolio robusto, para que puedan anticiparse a los riesgos y generar valor real en cada proyecto de ciberseguridad”.

debe replantearse en México", afirmó, al tiempo que subrayó que "hoy más que nunca, el canal tiene la responsabilidad de ir más allá de la venta e impulsar una cultura de prevención en sus clientes".

Ante este panorama, la compañía ha reforzado su portafolio con soluciones orientadas a proteger tanto la infraestructura como la identidad digital de las organizaciones. La incorporación de herramientas especializadas permite atender necesidades específicas de las pymes, que históricamente han destinado menos recursos a su seguridad, pero que hoy enfrentan un entorno de mayor riesgo. Este enfoque también se complementa con un programa continuo de capacitación, certificaciones e incentivos para los socios de negocio, con el objetivo de elevar su nivel de especialización y acompañarlos en la evolución hacia modelos más consultivos.

Uno de los pilares de esta estrategia es la habilitación digital del canal. A través de Soga Cloud, HD Latinoamérica ofrece a sus distribuidores la posibilidad de contar con un e-commerce propio sin costo, operativo en cuestión de minutos. Este modelo permite integrar soluciones de ciberseguridad de forma inmediata, facilitando la comercialización de licencias y servicios bajo esquemas automatizados, lo que reduce tiempos de implementación y acelera el cierre de ventas en un mercado que demanda inmediatez.

"En 2026 vamos a consolidar un ecosistema donde el canal tenga acceso a herramientas digitales, capacitación continua y soluciones especializadas, con el objetivo de crecer de forma rentable mientras protege a sus clientes ante amenazas cada vez más sofisticadas".

Además de optimizar la operación comercial, esta plataforma amplía el alcance hacia el mercado pyme y fortalece la experiencia del usuario final con procesos de compra ágiles y seguros. La disponibilidad en línea de soluciones como antivirus, protección de endpoints y herramientas de monitoreo responde a la necesidad de contar con esquemas flexibles, donde la tecnología pueda implementarse de forma rápida y escalable sin comprometer la eficiencia del canal.

Sin embargo, el crecimiento de estas capacidades también viene acompañado de riesgos más complejos. En México, siete de cada diez fraudes digitales están relacionados con phishing, que hoy se

se presenta en múltiples formatos como correos electrónicos, llamadas, mensajes y aplicaciones falsas. A esto se suman esquemas de robo de identidad y fraudes financieros, donde incluso se utilizan deepfakes para suplantar ejecutivos y generar transferencias fraudulentas. “El fraude ya no es como antes; hoy tiene un componente de ingeniería social muy avanzado y, con el apoyo de la inteligencia artificial, se vuelve mucho más efectivo”, explicó Escobar.

El impacto de estas amenazas no solo se limita a pérdidas económicas, sino que también afecta la reputación de las organizaciones y la confianza de los usuarios. Datos del sector señalan que más del 60% de los casos de robo de identidad están vinculados con productos financieros, lo que incrementa la urgencia de adoptar soluciones integrales que combinen tecnología, procesos y educación digital. Bajo esta realidad, el papel del canal se vuelve determinante para guiar a los clientes en la prevención y respuesta ante incidentes.

Frente a este escenario, HD Latinoamérica busca consolidar un modelo que integre herramientas tecnológicas, capacitación constante y acompañamiento cercano al canal. La apuesta no solo está en ampliar el portafolio, sino en construir un ecosistema que permita a los socios responder con mayor rapidez y efectividad a un entorno donde los riesgos evolucionan al mismo ritmo que la digitalización.

Haz crecer tu negocio con ciberseguridad de clase mundial.

safetica
ESET
SOPHOS
Avast
kaspersky
WebTitan
SpamTitan
PDQ
norton
SOCRadar
BitRaser
ULTRABAC

Antimalware + Antispam + Filtrado web
+ DLP + Inteligencia de amenazas

Todo lo que necesitas, en un solo aliado:

HD LATINOAMÉRICA

Partner GROWTH

Accede al mejor programa de partners en el que todas tus acciones te harán ganar.

"Hoy hablamos de ecosistemas donde cada capa de seguridad se complementa"

Ante un entorno digital cada vez más exigente, CT Internacional fortalece su estrategia en ciberseguridad con un enfoque integral que combina tecnología, capacitación y especialización del canal. A través de un portafolio estructurado en cinco segmentos y programas como Ruta CT Business and Training, la compañía impulsa la profesionalización de distribuidores e integradores, acercando soluciones que responden a las nuevas necesidades de protección en empresas mexicanas.

El avance de la digitalización en México ha elevado la relevancia de la ciberseguridad dentro de las organizaciones, particularmente por el incremento en la conectividad y la adopción de nuevos tecnológicos. Este escenario ha impulsado a mayoristas como CT Internacional a consolidar propuestas más completas, orientadas a proteger tanto la infraestructura como la operación de las empresas.

MIGUEL FIMBRES,
DIRECTOR DE MARCA EN
CT INTERNACIONAL.

“Estamos enfocando nuestra estrategia en integrar soluciones que permitan al canal construir propuestas completas de ciberseguridad, alineadas a las necesidades reales del mercado”.

En este sentido, la compañía ha organizado su portafolio en cinco segmentos: seguridad de red, aplicaciones, seguridad en la nube, protección de endpoints y gestión de identidad. Esta estructura busca responder a distintos niveles de riesgo, desde la protección de redes físicas mediante firewalls y VPN, hasta la seguridad de datos y accesos en entornos híbridos.

“La estrategia no se limita a colocar soluciones aisladas, sino a construir ecosistemas donde cada capa de seguridad tenga un propósito claro dentro de la operación del lcliente”, explicó Miguel Fimbres, Director de Marca en CT Internacional. Bajo esta ógica, tecnologías como EDR permiten monitorear dispositivos en tiempo real, mientras que los esquemas de gestión de identidad refuerzan el control de accesos y credenciales.

Para habilitar al canal, CT Internacional trabaja con fabricantes a través de programas de certificación estructurados en distintos niveles. Desde esquemas de entrada con formación comercial y técnica básica, hasta niveles avanzados donde

“El fortalecimiento del canal es fundamental; por eso impulsamos certificaciones y capacitación constante que les permita desarrollar proyectos con mayor nivel técnico y valor para sus clientes.”

se requieren perfiles especializados, evaluaciones formales y capacidades para diseñar soluciones complejas. “El desarrollo del canal pasa por elevar su conocimiento, no solo en producto, sino en la capacidad de implementar y acompañar proyectos de seguridad”, añadió Fimbres

Además del componente técnico, la compañía ha reforzado la capacitación continua mediante iniciativas como Ruta CT Business and Training, que acerca contenido actualizado a distribuidores e integradores. Durante 2025, este programa permitió capacitar a 3,463 partners a través de más de 20 talleres realizados en 15 eventos en distintas regiones del país, complementados con webinars que facilitan el acceso remoto al conocimiento.

El enfoque también contempla la necesidad de acompañar al canal en la entrega de servicios, un aspecto fundamental en proyectos de ciberseguridad. Por ello, CT Internacional mantiene alianzas con fabricantes para ofrecer certificaciones y formación especializada que permitan a los partners fortalecer su expertise y responder a los requerimientos del mercado.

De cara a los próximos meses, la compañía observa un crecimiento sostenido en la demanda de soluciones de ciberseguridad, impulsado por la evolución de los procesos empresariales hacia entornos digitales. Esta tendencia abre nuevas oportunidades para el canal, particularmente en proyectos que integren múltiples capas de protección y servicios asociados.

FORTINET

"La ciberseguridad ya no es opcional: es una condición para operar"

Fortinet refuerza su estrategia en México mediante el impulso al canal, el desarrollo de soluciones con inteligencia artificial y la expansión de programas de capacitación. La compañía busca responder al crecimiento de amenazas como ransomware, ataques a la nube y vulnerabilidades humanas, apostando por un modelo consultivo que permita a las organizaciones elevar su madurez en ciberseguridad.

El avance de los ciberataques en México continuará acelerándose en 2026, impulsado por la adopción masiva de tecnologías digitales y el uso cada vez más sofisticado de la inteligencia artificial. De acuerdo con estimaciones del sector, el país se mantiene entre los principales objetivos en América Latina, concentrando hasta 60% de los intentos de ciberataques en la región.

La desaparición del perímetro tradicional y la hiperconectividad han ampliado la superficie de riesgo en empresas de todos los tamaños.

La evolución de las amenazas no solo ha incrementado en volumen, sino también en complejidad. Ataques de ransomware, extorsión digital y explotación de vulnerabilidades en la nube, especialmente en APIs, se posicionan como los

MARÍA JOSÉ ALBARRÁN,
DIRECTORA DE CANALES
DE FORTINET MÉXICO.

“La estrategia de Fortinet en 2026 está enfocada en fortalecer a nuestros partners con especialización continua, integrando inteligencia artificial en nuestras soluciones y acompañándolos en cada etapa para que puedan ofrecer servicios de alto valor en un mercado cada vez más exigente”.

principales vectores. A esto se suma el uso de inteligencia artificial generativa para diseñar ataques dirigidos y el llamado “envenenamiento de datos”, una técnica que busca corromper modelos desde su origen. María José Albarrán, Directora de Canales de Fortinet México, advirtió: “Hoy vemos ataques mucho más personalizados y sofisticados, donde la inteligencia artificial está siendo utilizada por los ciberdelincuentes para aumentar su efectividad”.

Otro elemento crítico es el factor humano. Se estima que más del 80% de los incidentes de seguridad tienen su origen en errores de usuarios, desde hacer clic en enlaces maliciosos hasta la mala gestión de accesos. Ante ello, las organizaciones enfrentan el reto de fortalecer sus estrategias de capacitación interna, al tiempo que adoptan soluciones tecnológicas capaces de mitigar riesgos en tiempo real.

“Estamos evolucionando hacia un modelo donde el canal no solo comercializa tecnología, sino que se convierte en un asesor estratégico; por eso impulsamos esquemas como MSSP y nuevas especializaciones que responden a tendencias como IA, nube y seguridad distribuida”.

Desde la perspectiva de Fortinet, el papel del canal de distribución adquiere mayor relevancia frente a este entorno. La compañía ha reforzado su estrategia de habilitación con programas de entrenamiento continuo, que incluyen sesiones virtuales y presenciales. Tan solo en el último año, más de 300 especialistas fueron capacitados en arquitecturas SASE, una tendencia que responde a la necesidad de proteger entornos distribuidos y usuarios remotos. A nivel de innovación, la firma apuesta por el desarrollo de plataformas integradas con inteligencia artificial. La evolución de su sistema operativo, **FortiOS 8.0** incorpora capacidades avanzadas para la protección en entornos multicloud, visibilidad en tiempo real y prevención de fuga de datos, además de funciones orientadas a la seguridad post-cuántica. “Nuestros partners deben ser un eslabón muy fuerte, porque son quienes están frente al cliente y necesitan contar con herramientas y conocimiento actualizado de manera constante”, señaló Albarrán.

En paralelo, el programa de canales evoluciona con el lanzamiento de una nueva versión de Partner Engage, que contempla especializaciones más alineadas a las demandas actuales del mercado, incluyendo inteligencia artificial y servicios administrados. Este modelo también integra esquemas flexibles para proveedores MSSP, permitiendo ampliar su oferta bajo modelos de servicio.

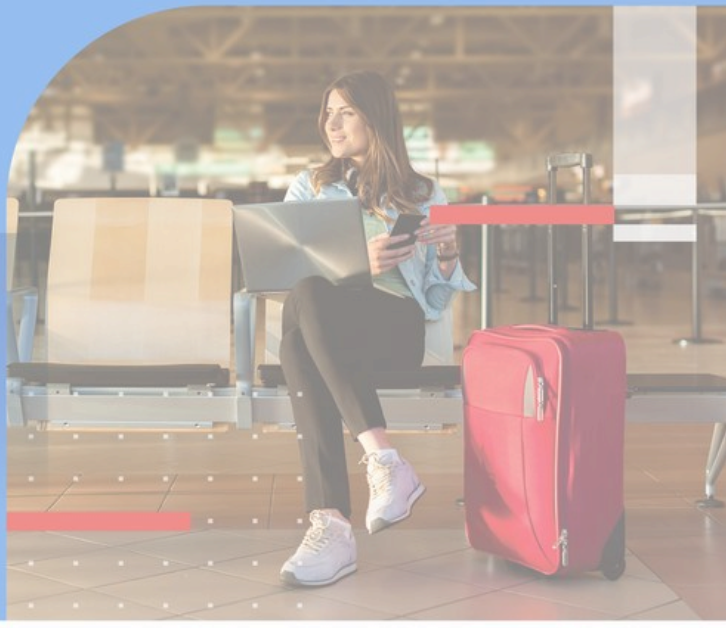
La visión de Fortinet para 2026 apunta al fortalecimiento de la investigación, la colaboración global y la democratización del conocimiento en ciberseguridad. Como parte de este enfoque, la compañía mantiene desde 2020 un esquema de capacitación gratuita orientado a reducir la brecha de talento, que hoy supera los 3.5 millones de especialistas a nivel mundial. Además, los canales pueden registrarse a distintos webinars y sesiones de actualización a través de su **plataforma oficial de eventos** donde se concentran contenidos alineados a las tendencias más recientes del sector.

FORTINET

Unified SASE

Acceso seguro para su fuerza laboral híbrida y protección para redes, aplicaciones y datos en cualquier nube.

www.fortinet.com/lat



GRUPO DICE® TELECOMUNICACIONES

MAPS DISRUPTIVO

TD SYNNEX

“No se trata solo de respaldar datos, sino de garantizar que estén libres de amenazas”

Adistec consolida su estrategia de ciberseguridad para 2026 al integrar resiliencia operativa, inteligencia artificial y capacitación especializada para canales en México. A través de soluciones que combinan protección de datos, cumplimiento normativo y automatización, la compañía busca reducir tiempos de respuesta ante incidentes y cerrar la brecha de talento en el sector, al tiempo que fortalece el posicionamiento de sus socios frente a un entorno de amenazas cada vez más sofisticado.

En un entorno donde los ataques de ransomware y las brechas de datos siguen creciendo a doble dígito a nivel global, el mayorista Adistec redefine su papel en el ecosistema tecnológico al apostar por una estrategia de ciberseguridad integral para 2026. La compañía enfoca sus esfuerzos en habilitar a los canales con herramientas que combinen respaldo, protección activa y recuperación eficiente, integradas dentro de un **portafolio robusto**, en un contexto donde el tiempo de recuperación (RTO) puede marcar la diferencia entre la continuidad o la interrupción de un negocio.

KARINA DE CASTRO,
PRODUCT SALES
MANAGER EN ADISTEC.

“En 2026 nuestra estrategia está centrada en que los canales evolucionen hacia modelos consultivos, donde no solo comercialicen soluciones, sino que entiendan el riesgo del cliente y lo traduzcan en arquitecturas seguras, resilientes y alineadas a las nuevas amenazas digitales”.

ALEJANDRO HERNÁNDEZ,
ENGINEERING SALES
SPECIALIST EN ADISTEC.

“Estamos enfocando nuestros esfuerzos en integrar tecnologías con inteligencia artificial y automatización, pero también en transferir conocimiento al canal; ahí es donde realmente se genera valor, porque les permite responder con mayor rapidez y precisión ante incidentes complejos”.

Karina de Castro, Product Sales Manager en Adistec, explicó que la compañía ha roto el esquema tradicional que separaba la infraestructura del centro de datos y la operación del SOC, al integrar escaneos de amenazas en cada punto de restauración, así como cifrado y protección de identidades. “Hoy hablamos de resiliencia total: no basta con tener respaldos, debemos asegurar que esos datos estén limpios antes de levantar una operación, incluso ante ataques avanzados”, señaló.

Este enfoque cobra relevancia si se considera que, según estimaciones de la industria, más del 60% de las organizaciones afectadas por ransomware enfrentan

intentos de cifrado en sus respaldos. Ante ello, Adistec impulsa arquitecturas de almacenamiento inmutable que evitan la manipulación o eliminación de la información crítica, reduciendo riesgos y garantizando la continuidad operativa en escenarios adversos, reforzando así su **propuesta de valor para partners.**

Desde el frente tecnológico, Alejandro Hernández, Engineering Sales Specialist en Adistec, destacó la integración de soluciones XDR potenciadas por inteligencia artificial, las cuales permiten reducir hasta en un 40% los falsos positivos en la detección de amenazas. “La automatización y la IA permiten que los analistas se enfoquen en incidentes críticos, acortando significativamente los tiempos de respuesta ante una brecha de seguridad”, afirmó.

La estrategia no se limita a la tecnología. Adistec ha fortalecido su rol como centro de entrenamiento autorizado, ofreciendo programas de capacitación que incluyen webinars, bootcamps y certificaciones especializadas en áreas como Zero Trust,

“No se trata sólo de implementar herramientas, sino de enseñar al canal a entender todo el ciclo de la seguridad: desde la protección de datos hasta el cumplimiento normativo, para que puedan construir propuestas mucho más completas y estratégicas”
Alejandro Hernández

“Estamos impulsando que los socios integren seguridad desde el diseño de sus proyectos, con protección de identidades, cifrado y almacenamiento inmutable, para que puedan garantizar continuidad operativa incluso ante escenarios de ataque complejos”
Karina de Castro

seguridad en la nube y protección de datos, muchas de ellas articuladas desde su **unidad de educación** . Este enfoque busca reducir la brecha de talento en ciberseguridad, que en México continúa siendo uno de los principales retos del sector.

En paralelo, la compañía ha desarrollado laboratorios demo y capacidades de preventa que permiten a los canales traducir regulaciones como la Ley Federal de Protección de Datos o estándares internacionales en soluciones tangibles. Esto facilita la generación de proyectos alineados al cumplimiento normativo, particularmente en sectores donde las licitaciones exigen un alto nivel técnico y documental.

De cara a 2026, Adistec también impulsa campañas de concientización sobre nuevas amenazas impulsadas por inteligencia artificial, un fenómeno que ya comienza a impactar en la superficie de ataque de las organizaciones. La inclusión de nuevas marcas en su portafolio y el acompañamiento estratégico a sus socios refuerzan su visión de consolidarse como un habilitador de valor en el mercado de ciberseguridad.


distec

"La integración entre soluciones es lo que realmente reduce riesgos de TI"

La estrategia de Tecnología Especializada Asociada de México (TEAM) en ciberseguridad para 2026 se centra en la integración de un portafolio robusto que incluye firmas globales como Sophos, CyberArk, Tanium, Tenable, Thales y Netskope, con el objetivo de construir arquitecturas unificadas y no herramientas aisladas. Este enfoque responde a un entorno donde los costos operativos pueden incrementarse hasta en doble dígito cuando las plataformas no se comunican entre sí, impactando directamente en la eficiencia de las organizaciones.

Joaquín Amaya, BU Manager Cybersecurity en TEAM, explicó que la apuesta del mayorista radica en consolidar soluciones mediante conectores e interoperabilidad entre plataformas: “Hoy las marcas ya están diseñadas para integrarse y compartir inteligencia en tiempo real; cuando se logra esa visibilidad unificada, las empresas no solo reducen la complejidad operativa, también optimizan recursos y mejoran su postura de seguridad de forma medible”, detalló. Esta visión busca fortalecer la defensa en profundidad en empresas mexicanas, donde los riesgos de TI mantienen una tendencia al alza.

A la par, TEAM ha fortalecido su estructura de habilitación con equipos especializados por

JOAQUÍN AMAYA, BU MANAGER CYBERSECURITY EN TECNOLOGÍA ESPECIALIZADA ASOCIADA DE MÉXICO (TEAM).

“Buscamos consolidarnos como un mayorista de valor que no sólo distribuya tecnología, sino que integre soluciones, financiamiento y servicios en un mismo ecosistema, permitiendo a nuestros canales desarrollar proyectos más rentables y sostenibles en el tiempo dentro del mercado mexicano”.

marca, incluyendo Product Managers, consultores técnicos y representantes comerciales, con el objetivo de acelerar la adopción de tecnologías avanzadas como SASE o gestión de identidades privilegiadas. Este acompañamiento se complementa con programas de capacitación continua, talleres técnicos, demostraciones y pruebas de concepto que permiten a los canales reducir su curva de aprendizaje en 2026 y adoptar nuevas soluciones con mayor rapidez (https://www.teamnet.com.mx/webinars2026).

Este respaldo resulta relevante si se considera que la especialización en ciberseguridad puede extenderse varios meses sin apoyo adecuado, afectando la velocidad de implementación en proyectos críticos.

Otro de los ejes relevantes es el impulso de modelos financieros flexibles y esquemas de ciberseguridad como servicio, que permiten a los canales cerrar proyectos de mayor volumen. Actualmente, TEAM ofrece esquemas de financiamiento adicionales al crédito tradicional, así como servicios mensualizados desde su nube Stratosphere, facilitando la adopción bajo modelos OPEX “Estamos habilitando a los canales con esquemas financieros más amplios y servicios bajo

“Nuestra meta es crecer de forma exponencial en los próximos años y participar activamente en al menos 5% del desarrollo tecnológico del país, apoyando a las organizaciones a reducir sus riesgos de TI mediante arquitecturas de ciberseguridad integradas, escalables y alineadas a sus necesidades reales de negocio”.

team | THALES

PROTEGE EL BALÓN MÁS VALIOSO:

TUS DATOS.

Control total del dato, sin importar dónde juegue.

JUEGA A LA DEFENSIVA. GANA CON CYPHERTRUST.

AGENDA UNA DEMO

CypherTrust
La solución de
THALES

suscripción para que puedan llevar soluciones avanzadas al mercado sin depender de grandes inversiones iniciales, lo que abre oportunidades en empresas que antes no podían acceder a este tipo de tecnologías", comentó Amaya.

Finalmente, el mayorista también avanza en la integración de proyectos "llave en mano" que combinan hardware, software y servicios, incluyendo despliegues a escala nacional. Esta capacidad permite atender atender iniciativas de hasta cientos de equipos —como integraciones de 500 dispositivos con configuraciones específicas —, consolidando una oferta que responde a sectores críticos como financiero y retail. La compañía proyecta contribuir con el 5% del desarrollo tecnológico en México en los próximos años, respaldada por un crecimiento sostenido y más de 40 años de operación en el país.

mediaware

Servicio 360
MARKETING Y VENTAS

Especializado en Tecnología y Consumo

MEDIOS DE COMUNICACIÓN

DISEÑO INTEGRAL

MARKETING DIRECTO Y SOLUCIONES DIGITALES

Desarrolle su **PLAN** con **NOSOTROS**

mediaware.org

"Nuestro compromiso es con la seguridad, no con una marca"

Con tres décadas de trayectoria, Grupo Propulsor de Soluciones (GPS) fortalece su presencia en el mercado de ciberseguridad con operaciones en más de 30 países y un SOC de alto nivel en México. Su estrategia se centra en habilitar a canales mediante modelos como Cybersecurity as a Service, integrando soluciones avanzadas como SIEM, DLP y automatización. La compañía impulsa la adopción tecnológica en LATAM con innovación proveniente de Europa y Asia, al tiempo que promueve un crecimiento colaborativo entre socios en un entorno donde la protección digital se ha vuelto prioritaria para empresas de todos los tamaños.

Grupo Propulsor de Soluciones (GPS) ha construido, a lo largo de 30 años, una operación enfocada en ciberseguridad que hoy rebasa fronteras, con presencia en más de 30 países y participación en proyectos de alcance nacional e internacional. Fundada en Cancún Quintana Roo, la compañía nació bajo un modelo “Partner First”, orientado a fortalecer a los distribuidores de valor agregado mediante colaboración directa, acceso a infraestructura especializada y una red de apoyo que permite ejecutar iniciativas tecnológicas de alta complejidad.

FERNANDO DURÁN DE LA SIERRA, COO & CORPORATE ACCOUNTS EN GRUPO PROPULSOR DE SOLUCIONES (GPS).

“La ciberseguridad en 2026 exige visión integral; no se trata solo de tecnología, sino de acompañamiento estratégico para que nuestros socios puedan capitalizar cada oportunidad del mercado con soluciones sólidas y escalables”.

En la actualidad, GPS Informática se posiciona como un actor relevante en el ecosistema de protección digital al operar uno de los principales Centros de Operaciones de Seguridad (SOC) en México y América Latina. Este entorno permite ofrecer monitoreo, detecciónyrespuesta ante amenazas en tiempo real, en un contexto donde los ataques evolucionan al ritmo de tecnologías emergentes como la inteligencia artificial.

La propuesta de valor de la compañía se sustenta en una actualización constante frente a un entorno tecnológico que cambia de manera acelerada. A través de acompañamiento comercial, técnico y logístico, GPS busca fortalecer a sus socios con herramientas que les permitan competir en un mercado donde la especialización y la rapidez de respuesta son determinantes. “Estamos en un entorno donde la innovación no se detiene, y nuestra responsabilidad es

traducir esa evolución en oportunidades reales para nuestros socios de negocio, con respaldo integral en cada proyecto", señaló Fernando Durán de la Sierra, COO & Corporate Accounts de GPS.

Su portafolio abarca soluciones de protección de endpoints (EPP), prevención de pérdida de datos (DLP), plataformas SIEM e iaSIEM de nueva generación,

"En GPS estamos construyendo un ecosistema donde la innovación, la colaboración y el cumplimiento normativo convergen para ofrecer a nuestros partners una ventaja real frente a un entorno cada vez más desafiante".

así como herramientas de orquestación y automatización con capacidades de respuesta inmediata. Estos servicios se integran en esquemas como "Cybersecurity as a Service", que permiten a los canales ofrecer modelos escalables, con costos competitivos y una mayor fidelización de clientes. "Nuestro enfoque es claro: habilitar a nuestros partners con plataformas robustas y esquemas flexibles que les permitan crecer en uno de los mercados más demandados, sin atarse a una sola marca", añadió Durán de la Sierra.

Otro diferenciador importante radica en la capacidad de GPS para introducir tecnologías provenientes de Europa y Asia al mercado latinoamericano, ampliando así el abanico de soluciones disponibles para sus socios. Este enfoque ha contribuido a posicionar diversas marcas en la región,

consolidando un ecosistema donde la innovación tecnológica se convierte en una ventaja competitiva tangible.

A nivel de infraestructura, la compañía también ofrece servidores virtuales de alta seguridad, diseñados tanto para el segmento SMB como para entornos empresariales.

Estos servicios se caracterizan por su personalización y atención prioritaria, lo que permite a los clientes contar con soluciones ajustadas a sus necesidades específicas, en contraste con modelos tradicionales de infraestructura como servicio.

Aunque opera bajo un esquema de canal cerrado, GPS mantiene una estrategia activa de incorporación de nuevos socios en América Latina, con planes de expansión hacia Estados Unidos y Canadá. La compañía apuesta por el crecimiento conjunto, brindando el mismo nivel de atención a proyectos pequeños y grandes, lo que refuerza su enfoque colaborativo en un sector donde la demanda de soluciones de ciberseguridad continúa en aumento.

“La ciberseguridad se construye sobre inteligencia artificial, nube y especialización”

Grupo CVA avanza en la construcción de un ecosistema de ciberseguridad que combina inteligencia artificial, servicios en la nube y especialización técnica, con el objetivo de fortalecer a su canal de distribución frente al crecimiento de amenazas digitales en México. La estrategia incluye la incorporación de nuevas marcas, programas de capacitación escalonados y un modelo de acompañamiento que busca transformar la venta tradicional en proyectos consultivos de alto valor.

La aceleración de los ataques digitales en México, donde más del 60% de las organizaciones ha reportado incidentes en el último año y el ransomware crece a doble dígito, está obligando a los mayoristas a replantear su rol en la cadena de valor, por lo que Grupo CVA, impulsa una estrategia enfocada en la integración de inteligencia artificial, servicios en la nube y ciberseguridad, con el objetivo de preparar al canal para un entorno cada vez más sofisticado y regulado.

“La convergencia entre inteligencia artificial, nube y ciberseguridad no es una tendencia pasajera, es la arquitectura sobre la cual se van a construir las soluciones de los próximos cinco años”, afirmó Adrián Simg, Director de Marcas en Grupo CVA.

ADRIAN SIMG,
DIRECTOR DE MARCAS
EN GRUPO CVA.

“La estrategia de Grupo CVA para 2026 está enfocada en integrar inteligencia artificial en cada capa de la ciberseguridad, permitiendo a nuestros canales ofrecer soluciones más proactivas, con capacidades de detección y respuesta en tiempo real que antes no eran posibles”.

El directivo explicó que el mayorista se encuentra en un proceso de incorporación de nuevas soluciones que integren estas capacidades, con anuncios previstos en los siguientes meses.

El cambio en la dinámica comercial también forma parte del reto. De acuerdo con estimaciones del sector, más del 70% de los proyectos de ciberseguridad en empresas medianas requieren hoy un enfoque consultivo, lo que implica habilidades técnicas más profundas. Ante ello, CVA ha desarrollado esquemas de acompañamiento que incluyen evaluaciones de seguridad, diseño de arquitecturas y desarrollo de playbooks por industria.

“Lo que buscamos es habilitar al canal no solo con producto, sino con conocimiento y acompañamiento real, desde el assessment hasta el cierre de proyectos, para que puedan evolucionar hacia un modelo consultivo”, detalló Simg. Este enfoque contempla incluso pruebas de concepto y soporte especializado en las primeras implementaciones, reduciendo la curva de aprendizaje.

En cuanto a oportunidades, el sector público destaca como uno de los principales focos de inversión, especialmente ante la necesidad de modernizar infraestructuras críticas. A este segmento se suman industrias como la financiera, manufactura, salud y retail, donde la adopción de soluciones de seguridad basadas en inteligencia artificial podría crecer por encima del 20% anual hacia 2026.

“Estamos construyendo un portafolio que no solo responda a las amenazas actuales, sino que anticipe las futuras, apoyando a nuestros socios con capacitación, certificaciones y acompañamiento continuo para que evolucionen hacia modelos de negocio más especializados”.

La hoja de ruta de capacitación de Grupo CVA contempla un proceso escalonado que puede extenderse por más de 12 meses. Este incluye desde fundamentos de ciberseguridad e inteligencia artificial, hasta certificaciones avanzadas y acompañamiento en campo. La meta es que los socios de negocio desarrollen capacidades técnicas y comerciales que les permitan competir en proyectos de mayor valor.

Finalmente, la visión hacia 2026 apunta a una adopción más amplia de tecnologías autónomas de detección y respuesta. Según el directivo, los modelos tradicionales comienzan a mostrar limitaciones frente a amenazas más dinámicas, por lo que la integración de inteligencia artificial será determinante para reducir tiempos de respuesta y mitigar riesgos en tiempo real.

MARRUECOS

CONVENCIÓN CVA 2026

De México para el mundo:
¡Vive la experiencia más top de la industria TI!

Participa por un lugar en la Convención CVA Marruecos y sé parte de un encuentro donde los negocios cruzan fronteras.

Compras acumulables del **1 de enero al 31 de julio.**
¡Compra en CVA!

14 AL 19 DE SEPTIEMBRE 2026

¡ENTRE MÁS COMPRES EN CVA,
TIENES MÁS POSIBILIDADES DE GANAR!

Invitación exclusiva por cuota de venta.
Consulta detalles del viaje con tu ejecutivo.

Gen™

“La ciberseguridad en la era actual exige protección integral, accesible y centrada en el riesgo real del negocio”

En un entorno donde la digitalización crece a doble dígito y las amenazas evolucionan constantemente, la ciberseguridad se posiciona como un elemento estratégico para la continuidad de las empresas en México. Hoy el riesgo ya no es únicamente la presencia de un virus, sino escenarios mucho más sensibles como el robo de información, el uso indebido de la identidad o fraudes digitales que pueden impactar directamente en la operación del negocio. En este contexto, Norton enfoca su propuesta en ofrecer soluciones accesibles y fáciles de implementar para pequeñas empresas, uno de los segmentos más vulnerables ante ataques cada vez más sofisticados.

La acelerada digitalización en México ha abierto nuevas oportunidades para las pequeñas y medianas empresas, pero también ha ampliado significativamente la superficie de ataque. En este entorno, el riesgo ya no se limita a malware tradicional, sino que abarca robo de información, suplantación de identidad y fraudes que pueden impactar directamente la operación, especialmente en organizaciones que no cuentan con áreas especializadas de TI.

“Pensar que por ser pequeño no serás atacado es uno de los mayores errores en ciberseguridad; precisamente por tener menor o nula protección digital, las PyMEs se convierten en objetivos rentables rentables para los atacantes.”

EDGAR ORDOÑEZ, DIRECTOR DE VENTAS EN MÉXICO EN NORTON.

ISKANDER SANCHEZ-ROLA, DIRECTOR DE INTELIGENCIA ARTIFICIAL E INNOVACIÓN EN NORTON.

“La inteligencia artificial ha elevado el nivel y la sofisticación a una escala sin precedentes, por lo que la defensa debe ser igualmente avanzada, capaz de anticipar riesgos y proteger al usuario en cada punto de interacción en línea”.

Frente a este panorama, Norton ha fortalecido su estrategia para 2026 con soluciones como Norton Small Business, orientadas a organizaciones que carecen de áreas especializadas de TI. Iskander Sanchez-Rola, Director de Inteligencia Artificial e Innovación en Norton, advirtió que subestimar el riesgo sigue siendo uno de los principales errores: “Pensar que por ser una empresa pequeña no serás atacado es un error crítico; en realidad, al contar con menos protección, te conviertes en un objetivo más accesible y el impacto puede ser total”.

El avance de la inteligencia artificial ha transformado también la naturaleza de las amenazas. Hoy, los ataques son más personalizados, automatizados y difíciles de detectar, evolucionando más allá del virus tradicional hacia esquemas de engaño que apelan directamente al comportamiento del usuario. En este contexto, Norton ha desarrollado herramientas impulsadas con inteligencia artificial, que permiten analizar amenazas en tiempo real y anticipar comportamientos maliciosos antes de que se materialicen.

“La ciberseguridad debe integrarse de forma natural al negocio, sin fricciones, y ahí el canal juega un papel esencial para traducir la tecnología en soluciones prácticas que realmente protejan y generen valor”.

Iskander Sanchez-Rola

“Los ataques ya no ocurren en un solo punto; hoy se distribuyen a través de múltiples canales como mensajes, llamadas, correos electrónicos o códigos QR.

Por eso, la protección debe ser integral y capaz de acompañar al usuario en todo su entorno digital”, explicó Sanchez-Rola, al destacar la necesidad de evolucionar hacia modelos de defensa más amplios y que cubran diversos puntos de ataque.

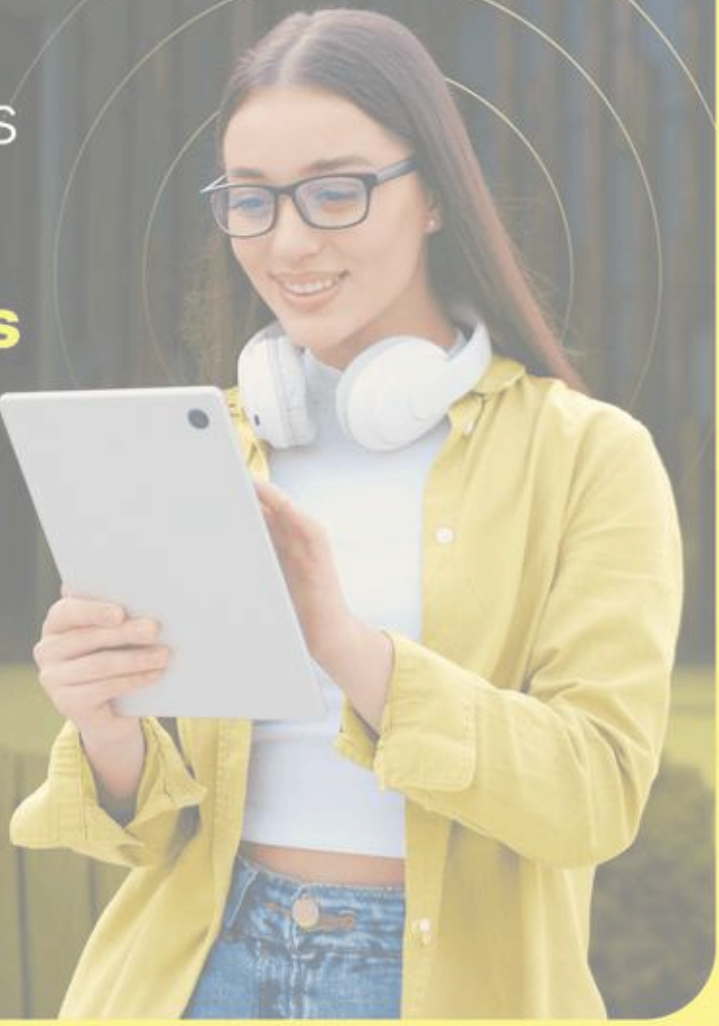
Uno de los pilares de esta estrategia es la simplificación tecnológica. Norton busca que la ciberseguridad deje de ser un proceso complejo y se convierta en una herramienta accesible para cualquier negocio, independientemente de su tamaño. En este proceso, el canal de distribución se posiciona como un actor estratégico para acercar, implementar y adaptar las soluciones a las necesidades reales de cada cliente.

Desde la perspectiva comercial, Edgar Ordoñez, Director de Ventas en México, enfatizó que la evolución del portafolio responde a un cambio de fondo en la forma en que operan los riesgos digitales, especialmente para las PyMEs que carecen de áreas especializadas en ciberseguridad. En este contexto, destacó cómo soluciones como Norton Small Business, Norton Mobile Security y Norton 360 Advanced extienden la protección más allá del dispositivo tradicional, integrando seguridad para identidad, navegación y transacciones en entornos móviles y personales que también impactan al negocio y a los usuarios directamente. “Hoy los ataques ya no buscan solo vulnerar un equipo, sino engañar al usuario y aprovechar cualquier punto de contacto digital; por eso nuestras soluciones están diseñadas para acompañarlo en su día a día, proteger su información y facilitar la seguridad sin exigir conocimientos técnicos, especialmente en empresas donde no existe un equipo de TI”, afirmó.

Asimismo, Ordoñez destacó el papel del ecosistema de partners para llevar estas capacidades a mercados donde la digitalización avanza rápidamente, pero la protección aún es limitada. “La oportunidad está en acercar soluciones que realmente entiendan la realidad de las pequeñas empresas, que no compliquen su operación y que les permitan protegerse sin necesidad de convertirse en expertos; ahí el canal tiene un rol fundamental como asesor y habilitador”.

norton

Las amenazas avanzadas necesitan **herramientas inteligentes**



PC MAG BEST 2025 ANTIVIRUS SOFTWARE

Poderosa Protección con IA

"La ciberseguridad debe ser más efectiva, no más costosa"

ABBA Networks enfoca su estrategia de ciberseguridad en 2026 en la eficiencia operativa, el uso inteligente de IA y la entrega de servicios especializados accesibles. La compañía apuesta por simplificar la protección, reducir la complejidad tecnológica y fortalecer la capacidad de respuesta de las organizaciones mexicanas ante amenazas cada vez más sofisticadas.

La acelerada digitalización en México ha elevado la superficie de ataque para empresas de todos los tamaños. Datos de la industria compartidos por ABBA Networks estiman que más del 60% de las organizaciones en el país han enfrentado al menos un incidente de ciberseguridad en los últimos 12 meses, mientras que el costo promedio de una brecha puede superar los 4 de dólares. Frente a panaroma, ABBA Networks redefine su enfoque al colocar al usuario final en el centro de la estrategia de protección.

Desde la óptica del cliente, las amenazas no solo han incrementado en volumen, sino también en complejidad. El uso de inteligencia artificial por parte de actores maliciosos ha reducido las barreras técnicas para ejecutar ataques, lo que amplifica los riesgos. "Hoy los

RENÉ FUENTES, DIRECTOR DE INNOVACIÓN DE ABBA NETWORKS.

“Estamos construyendo un modelo donde la ciberseguridad no sea un lujo, sino una capacidad accesible, eficiente y escalable, apoyándonos en inteligencia artificial para anticipar riesgos y responder con mayor velocidad sin elevar los costos para el cliente”.

atacantes ya no necesitan un alto nivel técnico; basta con curiosidad y acceso a herramientas avanzadas para generar impactos significativos", explicó René Fuentes, Director de Innovación de ABBA Networks, al referirse a la evolución del ecosistema digital.

El mercado de ciberseguridad también atraviesa una transformación marcada por tres perfiles de fabricantes: aquellos que integran inteligencia artificial como valor agregado, los que nacieron bajo este paradigma y los que han quedado rezagados. Esta segmentación ha provocado una disrupción donde las soluciones más eficientes comienzan a desplazar a modelos tradicionales, especialmente cuando ofrecen costos hasta 20% menores con mejores capacidades de respuesta.

Ante este escenario, las organizaciones demandan soluciones que combinen visibilidad, prevención y capacidad de reacción en una sola plataforma. La consolidación tecnológica se vuelve una prioridad para reducir la complejidad operativa y optimizar presupuestos. En paralelo, el reto de talento persiste: la brecha

"La industria está cambiando rápidamente: quienes no integren inteligencia artificial de forma real en sus soluciones perderán relevancia. En ABBA Networks apostamos por tecnología que simplifique la operación y realmente mejore la protección de nuestros clientes".

global de profesionales en ciberseguridad supera los 3.5 millones de especialistas, lo que impacta directamente en la capacidad de respuesta de las empresas.

ABBA Networks se posiciona como un habilitador de servicios especializados, enfocándose en maximizar la eficiencia operativa de sus clientes. La compañía ha fortalecido su equipo técnico con capacitación continua y adopción de herramientas basadas en IA, lo que le permite escalar servicios y atender a más organizaciones sin comprometer la calidad.
“Nuestro enfoque está en lograr un equilibrio real entre riesgo y protección, con soluciones que sí puedan ser operadas por los clientes”, añadió Fuentes.

Durante los últimos dos años, la firma ha impulsado una estrategia interna orientada a optimizar sus operaciones, especialmente en las áreas que interactúan directamente con el cliente.

Este modelo busca incrementar la efectividad en la implementación y gestión de soluciones, reduciendo errores de configuración y mejorando los tiempos de respuesta ante incidentes que, en muchos casos, se originan por omisiones involuntarias o falta de recursos especializados.
La combinación de servicios gestionados, automatización e inteligencia aplicada permite a ABBA Networks ofrecer esquemas más accesibles, alineados a las necesidades reales del mercado mexicano. En un entorno donde los ataques pueden escalar en minutos, la capacidad de anticiparse y responder oportunamente se convierte en un diferenciador determinante para las empresas.

"El CISO dejó de ser operativo: hoy define el negocio y el riesgo"

La estrategia de Zscaler en 2026 se centra en simplificar la ciberseguridad mediante plataformas integradas, el uso inteligente de la inteligencia artificial y un enfoque orientado al negocio. En un entorno donde el riesgo digital impacta directamente en los resultados financieros, la compañía apuesta por fortalecer el rol del canal como asesor estratégico y por transformar la manera en que las empresas protegen sus datos.

En 2026, el panorama de ciberseguridad en México se caracteriza por un aumento sostenido en la sofisticación de los ataques, impulsados por el uso de inteligencia artificial tanto por atacantes como por defensores. México se mantiene entre los países más atacados a nivel global, junto con Brasil, al concentrar organizaciones con mayor madurez tecnológica en la región. Bajo este escenario, las empresas enfrentan amenazas automatizadas que evolucionan constantemente, elevando la presión sobre las estrategias de protección.

La adopción de inteligencia artificial dentro de la ciberseguridad ha dejado de ser opcional. De acuerdo con estimaciones del sector, más del

MARIO MORA, SENIOR REGIONAL DIRECTOR DE LATINOAMÉRICA PARA EL SEGMENTO DE CUENTAS ESTRATÉGICAS EN ZSCALER.

“Hoy el CISO ya no es medido por métricas operativas, sino por su impacto en el negocio: cuánto riesgo reduce, qué tan eficiente es la organización y cómo contribuye a crecer de forma segura en un entorno cada vez más complejo”.

60% de los incidentes recientes involucran algún tipo de automatización o componente basado en IA. En paralelo, compañías como Zscaler han invertido en desarrollos propios y adquisiciones para integrar capacidades avanzadas en análisis de riesgo y prevención. “La inteligencia artificial se utiliza en ambos sentidos: para defender y para atacar… quien diga que tiene la bala de plata está mintiendo”, advirtió Mario Mora, al subrayar el carácter evolutivo de esta tecnología.

Los sectores financiero, retail y manufactura encabezan la inversión en ciberseguridad en México, debido a su alta exposición y al valor de los datos que manejan. En estas industrias, el objetivo no solo es prevenir brechas, sino proteger el activo más crítico: la información. A nivel global, se estima que el costo promedio de una filtración de datos supera los 4.5 millones de dólares, lo que refuerza la urgencia de adoptar modelos más eficientes y menos fragmentados.

Uno de los principales retos para las organizaciones ha sido la acumulación de soluciones aisladas que incrementan la complejidad operativa y los costos. Frente a esto, Zscaler impulsa una estrategia basada en la consolidación tecnológica, orientada a reducir tanto el Capex como el Opex. “La recomendación es evitar stacks heterogéneos que no agregan valor y generan complejidad; se necesitan estrategias bien pensadas que prioricen eficiencia y flexibilidad”, explicó Mora, enfatizando la necesidad de simplificar arquitecturas.

En este entorno, el rol del CISO ha cambiado de forma radical. De ser un perfil técnico enfocado en la operación, ahora participa activamente en decisiones de negocio, con métricas centradas en reducción de riesgo, eficiencia y crecimiento seguro. Este cambio también está impulsado por una mayor presión regulatoria y por la necesidad de alinear la ciberseguridad con objetivos estratégicos, donde la gestión del riesgo digital se convierte en un elemento determinante para la continuidad y competitividad de las organizaciones.

Zscaler, ha apostado por una arquitectura de plataforma que ofrece visibilidad integral y protección continua. Este enfoque busca reducir la fatiga de alertas y mejorar la capacidad de respuesta de los equipos de seguridad, un problema que afecta a más del 70% de los CISOs según diversos estudios del sector.

“El canal tiene frente a sí una decisión importante: mantenerse en un modelo tradicional o evolucionar hacia soluciones que realmente generen valor. Ahí es donde tecnologías como las de Zscaler abren la puerta a nuevos ingresos y mejor posicionamiento.”

Para el canal de distribución, el contexto también ha cambiado. La ciberseguridad ha dejado de depender exclusivamente de servicios de red, abriendo nuevas oportunidades para integradores y socios especializados. La escasez de talento en el mercado, que supera los 3.5 millones de profesionales a nivel global, ha convertido al canal en un asesor estratégico para las organizaciones, con la posibilidad de generar ingresos a través de servicios profesionales y consultoría.

tm | tasmicro
EL MAYORISTA LÍDER EN CIBERSEGURIDAD

"El valor en ciberseguridad se construye con servicios que evolucionan en el tiempo"

Tasmicro ha destacado por su enfoque en software (95% de su operación), servicios administrados e inteligencia artificial, junto con una fuerte inversión en capacitación del canal —con más de 1,200 ejecutivos formados— y modelos financieros flexibles, estos elementos buscan impulsar propuestas de mayor valor, proteger entornos híbridos y fortalecer la rentabilidad de sus socios.

En un mercado mexicano donde la demanda de protección digital no deja de crecer, Tasmicro ha definido una ruta clara: priorizar software, innovación y especialización. Actualmente, 95% de su operación se basa en soluciones de software, alejándose del modelo tradicional de hardware. Este enfoque responde a un entorno donde el mercado global de ciberseguridad ya supera los 311 mil millones de dólares, con un 66% concentrado en servicios, lo que marca la pauta de evolución para fabricantes y canales.

Bajo esta lógica, la selección de fabricantes dentro de su portafolio no es casual. La compañía evalúa criterios como innovación constante, modelos de distribución definidos y programas de canal maduros.

“Nuestra estrategia está enfocada en que el canal evolucione hacia servicios administrados de valor, donde la ciberseguridad deje de ser una transacción y se convierta en un proceso continuo, capaz de adaptarse a los cambios del negocio y generar una relación de largo plazo con el cliente”.

SERGIO HERNÁNDEZ, SOCIO DIRECTOR GENERAL DE TASMICRO.

“Si un fabricante no está innovando, en un año se vuelve obsoleto; por eso buscamos marcas que integren inteligencia artificial desde su base tecnológica y que permitan al canal construir propuestas realmente diferenciadas en el mercado”, explicó Sergio Hernández.

El crecimiento de infraestructuras híbridas —entre nube y on-premise— también ha abierto nuevas oportunidades. En este terreno, la protección de APIs y aplicaciones se vuelve crítica, especialmente en sectores como fintech, donde una interrupción puede detener toda la operación. A ello se suma el desafío de la superficie de ataque dinámica, donde cada usuario y dispositivo representa un riesgo distinto. Frente a esto, la empresa impulsa soluciones basadas en inteligencia artificial capaces de analizar comportamientos y reducir vulnerabilidades en tiempo real.

La estrategia hacia el canal también se sustenta en capacitación intensiva. Tan solo en el último año, la compañía capacitó a más de 1,200 ejecutivos y certificó a 280 ingenieros en México, con programas alineados a marcos como NIST y MITRE ATT&CK. “La inversión más importante que hacemos, incluso por encima de muchas otras iniciativas estratégicas, es la que destinamos al habilitamiento; creemos firmemente que un canal bien preparado puede transformar una solución tecnológica en una propuesta de valor real para el cliente y sostenerla en el tiempo”.

En paralelo, el modelo financiero y de renovaciones se ha convertido en un diferenciador. La firma asegura visibilidad anticipada de contratos y procesos de “health check” que permiten incrementar el valor de cada renovación. Gracias a este enfoque, logran elevar hasta 120% el valor anual de sus oportunidades, combinando renovación con crecimiento del negocio. Además, esquemas flexibles como la mensualización de licencias facilitan la adopción tecnológica en empresas con distintos perfiles financieros.

“Estamos integrando tecnología innovadora, modelos financieros flexibles y una fuerte inversión en capacitación para que nuestros socios puedan capitalizar la inteligencia artificial, diferenciarse en el mercado y construir ofertas de ciberseguridad sostenibles y rentables hacia 2026”.

tm | tasmicro

EL MAYORISTA LÍDER EN CIBERSEGURIDAD

La Ciberseguridad:
Nuestro compromiso estratégico

En Tasmicro entendemos que la Ciberseguridad ya no es una opción, sino un pilar estratégico para la continuidad y crecimiento de las organizaciones.

Acompañámos a nuestros socios y clientes en la adopción de soluciones avanzadas que les permitan anticipar, detectar y responder a las amenazas actuales.

"Impulsamos el desarrollo de capacidades en nuestros socios de negocio para que puedan incrementar su competitividad generando nuevos servicios y oportunidades de negocio en un mercado de transformación"

CAPACIDADES DE INGENIERÍA

Servicio preventa integral y habilitamiento técnico y comercial

MODELOS DE FINANCIAMIENTO

Línea de crédito estandar y proyectos de financiamiento a la medida

COINVERSIÓN EN DESARROLLO DE NEGOCIO

Fondos dedicados para la ejecución de actividades de Geneación de Demanda

SLA 365°

Nuestro compromiso es que el canal tenga respuesta y solución a cualquier tipo de requierimiento en tiempo y forma

WWW.TASMICRO.COM marketing@tasmicro.com +52 56 3811 0593

PORTENNTUM

"La infraestructura ya es la primera línea de defensa digital"

“Nuestro objetivo es claro: ayudar a dejar de instalar dispositivos aislados y comenzar a implementar infraestructura convergente donde videovigilancia y voz IP se convierten en la primera línea de defensa digital de las empresas”.

La forma en que las empresas entienden su infraestructura tecnológica está cambiando. Sistemas como la videovigilancia y la voz sobre IP, tradicionalmente considerados operativos, hoy forman parte activa de la superficie de ataque. Ante este panorama, Portenntum impulsa una visión donde cada dispositivo conectado debe diseñarse con ciberseguridad desde su origen. “Hoy cualquier cámara IP o conmutador de voz es un endpoint conectado, y por lo tanto debe diseñarse con ciberseguridad desde el origen”, afirmó Pedro Gerón, Director Comercial en Portenntum, al explicar que la compañía trabaja para que estos elementos dejen de ser puntos vulnerables y se conviertan en componentes de protección.

Uno de los desarrollos más relevantes se presenta en el ámbito de la videovigilancia. A través de soluciones con Provision ISR en conjunto con Check Point, la firma incorpora

“Zero Trust debe construirse desde la infraestructura física hasta la operación en la nube; solo así se logra una arquitectura real que proteja entornos industriales y críticos sin comprometer su operación”.

PEDRO GERÓN, DIRECTOR COMERCIAL EN PORTENNTUM.

firewalls directamente en las cámaras, lo que permite proteger los sistemas desde el edge y evolucionar hacia un modelo preventivo apoyado en analítica e inteligencia artificial para la toma de decisiones.

En paralelo, la voz empresarial también se transforma. Desde 2025, la compañía impulsa la Familia GCC de Grandstream Networks, un conmutador 4-en-1 que integra telefonía IP, switching, routing con VPN y firewall de nueva generación en una sola plataforma, eliminando vulnerabilidades derivadas de implementaciones fragmentadas y facilitando un enfoque Secure-by-Design.

La estrategia se complementa con la adopción de arquitecturas de Confianza Cero, especialmente en entornos industriales y de infraestructura crítica. A través de tecnologías de HPE Aruba Networks y Juniper Networks, se habilitan modelos

donde ningún usuario o dispositivo es confiable por defecto, integrando autenticación continua, segmentación dinámica y detección de anomalías mediante inteligencia artificial.

Adicionalmente, soluciones de fabricantes como Hillstone Networks permiten la inspección profunda del tráfico y la prevención avanzada de amenazas, mientras que Micro aporta visibilidad, analítica y monitoreo centralizado. Este enfoque se refuerza desde la infraestructura física con aliados como Leviton y Corning, asegurando conectividad confiable y resiliente.

A la par, Portenntum fortalece la evolución de sus socios mediante programas de especialización y certificación, acompañándolos desde la preventa hasta la operación. Este modelo se complementa con plataformas en la nube que permiten administrar redes, seguridad y comunicaciones de forma remota, habilitando servicios gestionados y esquemas de soporte continuo.

" La ciberseguridad en México evoluciona hacia un modelo donde la protección ya no se limita a soluciones aisladas, sino que se integra desde la base de la infraestructura tecnológica. Portenntum impulsa este cambio al incorporar seguridad en videovigilancia, voz IP, redes y entornos industriales, combinando inteligencia artificial, monitoreo continuo y arquitecturas de Confianza Cero para responder a los nuevos vectores de ataque".

PORTENNTUM®

EL MEJOR EQUIPO SE ARMA CON LAS MEJORES MARCAS DEL MERCADO

CONOCE NUESTRAS SOLUCIONES

hp · GRANDSTREAM · DTEN · Panasonic · OneScreen · HPE aruba networking · Instant On · Newland AIDC · Hillstone Networks · R Ridge Security · opentext™ · PROVISION ISR · ANVIZ · WAM · LEVITON · CONDUMEX · CORNING · north · prysmian · CyberPower

Las jugadas inteligentes comienzan con la tecnología correcta.

Ser socio PORTENNTUM

CompuSoluciones

“La ciberseguridad ya no reacciona: gobierna sistemas que toman decisiones”.

CompuSoluciones refuerza su estrategia en ciberseguridad mediante un enfoque centrado en prevención, gobernanza de inteligencia artificial y protección de identidades digitales. A través de capacitación especializada y acompañamiento a canales, impulsa la adopción de soluciones que fortalecen la resiliencia operativa, reducen tiempos de respuesta ante incidentes y permiten a las organizaciones asegurar la continuidad de sus operaciones frente a amenazas avanzadas.

El año 2026 marca un punto de inflexión en la ciberseguridad, donde el modelo reactivo ha quedado atrás frente a una visión centrada en la gobernanza de sistemas inteligentes. De acuerdo con estimaciones del sector, más del 65% de las organizaciones en América Latina ya integran algún tipo de inteligencia artificial en sus procesos de seguridad, mientras que los incidentes vinculados a automatización mal gestionada han crecido cerca de 40% en el último año. En este contexto, la protección digital evoluciona hacia entornos donde humanos y algoritmos operan simultáneamente.

Uno de los cambios más significativos radica en la

“Nuestra estrategia en 2026 está enfocada en evolucionar junto con los canales hacia servicios gestionados de ciberseguridad, con visibilidad integral, control sobre entornos impulsados por IA y un enfoque preventivo que permita a las organizaciones anticiparse a los riesgos y operar con mayor confianza”.
DIANA RIOS, GERENTE COMERCIAL DE CIBERSEGURIDAD EN COMPUSOLUCIONES

adopción de IA agente, capaz de ejecutar decisiones sin intervención humana directa. Este avance, aunque potencia la eficiencia operativa hasta en 30%, también introduce nuevos riesgos asociados a la falta de control sobre los algoritmos, lo que obliga a las organizaciones a establecer esquemas formales de supervisión, auditoría y trazabilidad.

A la par, el concepto de perímetro tradicional ha perdido relevancia. En su lugar, la identidad digital se consolida como el principal punto de defensa, especialmente ante el crecimiento de ataques sofisticados como los deepfakes, que han aumentado más de 50% en intentos de fraude corporativo. La autenticación basada en biometría y patrones de comportamiento se posiciona como una herramienta indispensable para mitigar estos riesgos en entornos distribuidos y altamente dinámicos.

En este escenario, CompuSoluciones compartió que las organizaciones están migrando hacia modelos de resiliencia operativa, donde la capacidad de mantener la continuidad del negocio resulta tan importante como prevenir ataques. Datos recientes indican que las empresas con estrategias de visibilidad integral reducen hasta en 45% el tiempo de detección de amenazas, lo que se traduce en menores impactos financieros y reputacionales.

Asimismo, la ciberseguridad comienza a consolidarse como un habilitador estratégico más que como un gasto operativo, por lo que, el mayorista estima que la inversión en este rubro crecerá alrededor de 18% anual hacia 2027, impulsada por la necesidad de proteger ecosistemas digitales cada vez más complejos Esta transformación también redefine el rol de los canales de distribución, quienes ahora deben integrar capacidades de consultoría, monitoreo y acompañamiento continuo para sus clientes.

Finalmente, el reto para 2026 no solo consiste en adoptar nuevas tecnologías, sino en gestionar de manera efectiva la interacción entre personas, procesos y sistemas autónomos. La madurez en ciberseguridad dependerá de la capacidad de las organizaciones para anticipar riesgos, establecer controles sobre la inteligencia artificial y fortalecer la confianza en entornos hiperconectados.

“Hoy no solo protegemos sistemas, sino decisiones automatizadas que impactan directamente en la operación; eso exige establecer reglas claras de supervisión, trazabilidad y responsabilidad sobre cada acción que ejecuta la inteligencia artificial”.

NOTICIAS DEL SECTOR IT EN LATINOAMÉRICA

ITWARE
LATAM.COM

- INFORMACION ACTUALIZADA PARA CIOs
- ENTREVISTAS EXCLUSIVAS.
- COBERTURA INTERNACIONAL DE EVENTOS

Manténgase informado suscribiendo a nuestros newsletter

@ITwareLatam
@ITwareLatam
ITware Latam
ITware Latam
ITware Latam

10 AÑOS

"En 2026, la ciberseguridad deja de ser un tema técnico para convertirse en una decisión de negocio: ya no basta con proteger, hay que anticipar. La identidad, los datos y la inteligencia aplicada marcan el rumbo, permitiendo a las organizaciones operar con confianza, adaptarse al cambio y sostener su crecimiento en entornos dinámicos y digitales".

Jesús Sánchez, Director de Limbergy

"La IA autónoma redefine la amenaza en 2026 con ataques que mutan en tiempo real y deepfakes estructurales que vulneran la cadena de mando. La tendencia exige blindar la identidad ante un phishing diseñado a medida y establecer una gobernanza de datos sensibles en consultas de IA; sin este control, el riesgo de exfiltración o mal uso de información crece".

Jonathan Rodriguez, Presales Team Leader en MAPS Disruptivo

NETSCOUT

"En 2026, la ciberresiliencia dependerá de eliminar los puntos ciegos. A medida que los atacantes usan IA para lanzar ataques hiperdirigidos a gran escala, las empresas deben pasar de defensas reactivas a una visibilidad de red profunda y proactiva. El futuro de la seguridad es automatizado, inteligente y en tiempo real."
Jorge Tsuchiya, Country Manager de NETSCOUT System México

"La ciberseguridad se convirtió en una necesidad concreta dentro de la agenda de cualquier empresa que dependa de su operación digital. Sin embargo, la adopción sigue estando limitada por barreras de acceso, complejidad y gestión. Las propuestas que logren simplificar la implementación, reducir la fricción comercial y acompañar al cliente en la operación serán las que realmente ganen espacio".
Hernán Pollini, Director Help Manager de México

help-manager

SitioSimple

Crear tu página web es tan rápido como leer esta publicidad

Hoy podés tener tu página web o tienda online ¡sin programar y en menos de una hora!

- Más de 200 plantillas pre-diseñadas
- 0% comisiones por venta
- Lista para celulares
- Optimizada para Google
- Múltiples opciones de pago y envíos
- En pesos argentinos

ESCANEÁ
Y EMPEZÁ GRATIS

DonWeb.com