Minsait cyber revela seis tendencias de ciberseguridad que definirán la resiliencia empresarial en 2026

- **La geopolítica, la inteligencia artificial, la resiliencia operacional y la protección de datos redefinirán las estrategias de ciberseguridad en México y América Latina**
- **Los ataques a la cadena de suministro de software se han consolidado como uno de los principales vectores de riesgo para las organizaciones**

Ciudad de México, 29 de enero de 2026. – La ciberseguridad se ha convertido en un factor estratégico para la continuidad operacional, la competitividad y la confianza empresarial. De cara a 2026, las organizaciones enfrentarán un entorno de riesgo marcado por tensiones geopolíticas, una adopción acelerada de la inteligencia artificial (IA), cadenas de suministro digitales cada vez más complejas y una superficie de ataque en constante expansión. En este contexto, Minsait Cyber, la unidad especializada en ciberseguridad de Indra Group, identificó seis tendencias clave que marcarán la evolución de la seguridad digital durante los próximos años y que deberán ser consideradas por empresas de todos los tamaños y sectores, especialmente aquellas con operaciones industriales, infraestructura crítica y modelos intensivos en tecnología.

“El reto para 2026 no es solo proteger activos digitales, sino construir resiliencia organizacional frente a un entorno cada vez más volátil, automatizado y distribuido”, señala Erik Moreno, director de Minsait Cyber en México. “La ciberseguridad debe alinearse con el negocio, anticipar riesgos y habilitar una adopción segura de la inteligencia artificial”.

Tendencia #1. Riesgos derivados de los cambios geopolíticos y la adopción de la IA

La creciente volatilidad geopolítica está incrementando la exposición de las organizaciones a ciberataques dirigidos, especialmente, contra grandes corporaciones y proveedores globales de tecnología, con impactos que se extienden a toda la cadena de suministro digital.

De cara a 2026, se prevé un aumento de ataques DDoS y ransomware contra infraestructuras críticas y sectores estratégicos. A este escenario se suma la adopción acelerada de la inteligencia artificial, que amplía la superficie de ataque mediante el uso no controlado de IA, la exposición de datos sensibles y la sofisticación de ataques automatizados, exigiendo una ciberseguridad más resiliente y alineada con el riesgo geopolítico.

Tendencia #2. Patrones arquitectónicos para la seguridad y la resiliencia

La creciente complejidad de los entornos híbridos y multinube está impulsando la adopción de nuevos patrones arquitectónicos de ciberseguridad orientados a la resiliencia.

En 2026, enfoques como Security by Design, Zero Trust Architecture y Cyber Security Mesh Architecture serán clave para integrar la seguridad desde el diseño de los proyectos, reducir la superficie de ataque y limitar el movimiento lateral de los atacantes. Estas arquitecturas permiten unificar controles, mejorar la detección y acelerar la respuesta ante incidentes. A ello se suma la creciente relevancia de Network Detection and Response (NDR), que aporta visibilidad avanzada del tráfico de red y fortalece la capacidad de análisis forense en entornos distribuidos y altamente interconectados.

Tendencia #3. Seguridad en la cadena de suministro de software y Cloud Native Application Protection Platform (CNAPP)

La seguridad de las aplicaciones ha dejado de limitarse a pruebas tradicionales de código y se ha convertido en un pilar crítico para las organizaciones. La dependencia de repositorios públicos, componentes de terceros, modelos de IA y arquitecturas cloud incrementa el riesgo de ataques a la cadena de suministro de software.

Para 2026, se prevé un aumento de incidentes dirigidos a pipelines de desarrollo, contenedores y dependencias de código abierto. Frente a este escenario, prácticas como el uso de Software Bill of Materials (SBOM) y la adopción de Cloud Native Application Protection Platform (CNAPP) permitirán unificar la protección de entornos cloud, priorizar riesgos reales y fortalecer la resiliencia frente a ataques a gran escala.

Tendencia #4. SecOps avanzado: automatización y gestión continua de la exposición

Las operaciones de seguridad enfrentan un entorno marcado por amenazas cada vez más automatizadas y por la presión constante sobre los Centros de Operaciones de Seguridad (SOC).

Para 2026, las organizaciones evolucionarán hacia modelos SecOps más avanzados, con SIEM (Security Information and Event Management) como eje unificador, automatización apoyada en inteligencia artificial y flujos de respuesta orquestados.

En este contexto, la gestión tradicional de vulnerabilidades dará paso a Continuous Threat Exposure Management (CTEM), que permite priorizar riesgos con base en su impacto real en el negocio y validar controles de forma continua. La combinación de automatización, IA y CTEM será clave para reducir la carga de la operación, mejorar la detección y fortalecer la resiliencia frente a amenazas cada vez más sofisticadas. El SOC del futuro será SIEM-céntrico, altamente automatizado y asistido por IA.

Tendencia #5. Seguridad centrada en los datos

La información se ha consolidado como el activo más crítico para las organizaciones, pero su proliferación en entornos híbridos, multinube y SaaS ha generado grandes volúmenes de dark data sin visibilidad ni control.

Hacia 2026, la seguridad centrada en los datos (Data Centric Security) será clave para identificar, clasificar y proteger la información a lo largo de todo su ciclo de vida, especialmente en escenarios impulsados por inteligencia artificial. Tecnologías como Data Security Posture Management (DSPM), Data Loss Prevention (DLP) y Cloud Access Security Broker (CASB) permitirán reducir riesgos, cumplir con regulaciones y evitar la exposición accidental de datos sensibles, fortaleciendo la resiliencia digital en entornos cada vez más distribuidos.

Tendencia #6. Reducción de la superficie de ataque

La reducción de la superficie de ataque se consolida como un pilar de la defensa en profundidad ante la creciente exposición de endpoints, el uso de esquemas BYOD y la dependencia de la nube.

Una parte significativa de los incidentes de ciberseguridad sigue originándose en deficiencias de higiene digital, como configuraciones inseguras, parches tardíos y controles de acceso débiles. Hacia 2026, las organizaciones priorizarán el robustecimiento de sistemas, la gestión unificada de endpoints y la protección de dispositivos móviles mediante Mobile Threat Defense, así como la extensión de Continuous Threat Exposure Management (CTEM) a configuraciones y parches. Este enfoque permitirá reducir puntos de entrada explotables y fortalecer la resiliencia frente a ataques avanzados.

Ciberseguridad como eje estratégico del negocio

Para Minsait Cyber, estas seis tendencias confirman que la ciberseguridad ha dejado de ser un tema exclusivamente técnico para convertirse en un habilitador estratégico del negocio. “La ciberseguridad de cara a 2026 exige una visión integral que vaya más allá de la protección puntual. Las organizaciones deben construir resiliencia desde el diseño, proteger sus datos, automatizar sus operaciones de seguridad y gestionar de forma continua su exposición al riesgo, en un entorno marcado por la inteligencia artificial y la inestabilidad geopolítica”, señaló Erik Moreno.

La planificación de la ciberseguridad exigirá integrar resiliencia organizacional, seguridad de la inteligencia artificial desde el diseño, protección de datos, automatización inteligente de los SOC y una reducción sostenida de la superficie de ataque. En un entorno donde los modelos híbridos seguirán expandiéndose y los ciberdelincuentes continuarán explotando la IA para potenciar sus ofensivas, solo las organizaciones con arquitecturas sólidas, datos debidamente protegidos y una cultura madura de ciberresiliencia estarán en condiciones de sostener sus operaciones y liderar con confianza durante la próxima década.

Acerca de Minsait

Comunicación y Relaciones con los Medios

Minsait (www.minsait.com) es la compañía del Grupo Indra líder en nuevos entornos digitales y tecnologías disruptivas. Presenta un alto grado de especialización, amplia experiencia en el negocio tecnológico avanzado, conocimiento sectorial y un talento multidisciplinar formado por miles de profesionales en todo el mundo. Minsait está a la vanguardia de la nueva digitalización con capacidades punteras en inteligencia artificial, cloud, ciberseguridad y otras tecnologías transformadoras. Con ello, impulsa los negocios y genera grandes impactos en la sociedad, gracias a una oferta digital de servicios de alto valor añadido, soluciones conectadas a medida para todos los ámbitos de actividad y acuerdos con los socios más relevantes del mercado.

Acerca de Indra Group

Indra Group (https://www.indragroup.com/) es la multinacional española de referencia y una de las principales compañías de Europa de defensa y digitalización avanzada. Tiene una posición de liderazgo en los negocios de defensa, espacio, gestión del tráfico aéreo, movilidad y tecnologías transformadoras, a través de Minsait, e integra en IndraMind sus capacidades de IA soberana, ciberseguridad y ciberdefensa. Indra Group impulsa un futuro más seguro y conectado a través de soluciones innovadoras, relaciones de confianza y el mejor talento. La sostenibilidad forma parte de su estrategia y de su cultura, para dar respuesta a los retos sociales y ambientales presentes y futuros. A cierre del ejercicio 2024, Indra Group tuvo unos ingresos de 4.843 millones de euros, presencia local en 46 países y operaciones comerciales en más de 140 países.

Contacto de Comunicación

Karla Zepeda
kzepeda@minsait.com
+52 55 5072 8304