OlimpIA | Sentry

Tendencias en ciberseguridad para el 2026:

Preparando a las organizaciones para los **nuevos riesgos digitales**

CIFRA DESTACADA

Durante 2025, Colombia registró más de **8.400 incidentes de ciberseguridad** reportados por entidades públicas y privadas, un **incremento del 47%** frente al año anterior.

Fuentes: CSIRT Colombia y MinTIC, 2025.

El próximo año traerá avances tecnológicos que cambiarán la manera en que operan las organizaciones, pero también abrirá nuevas puertas a las amenazas digitales. Los ciberataques serán más inteligentes, las regulaciones más estrictas y los usuarios más exigentes. Por este motivo, prepararse con anticipación será la mejor defensa.

En este eBook, te presentamos las tendencias clave que marcarán la ciberseguridad en 2026 y cómo las organizaciones pueden anticiparse a los riesgos para fortalecer su confIAnza digital y proteger cada interacción.

Radiografía del entorno digital 2025 - 2026

El panorama global muestra un crecimiento acelerado en la frecuencia, sofisticación y costo de los ataques. Algunos datos reflejan el escenario que las organizaciones enfrentarán el próximo año:

El costo global del cibercrimen alcanzará los **USD 13,8 billones** en 2026.

Fuente: Cybersecurity Ventures, 2025.

Más del 80% de las brechas se originan en credenciales comprometidas o accesos indebidos.

Fuente: Verizon Data Breach Report, 2025.

Los sectores financiero, energético y de transporte serán los más atacados en América Latina, con un **incremento del 61%** en ransomware y phishing corporativo.

Fuente: Kaspersky LATAM, 2025.

En Colombia, los ataques con deepfakes y manipulación de voz **crecieron un 430%** durante 2025.

Fuente: Informe de investigaciones de OlimpIA, 2025.

El **70% de las empresas** colombianas planean invertir en IA para monitoreo y detección de amenazas.

Fuente: IDC Colombia, 2025.

Estos indicadores demuestran que la ciberseguridad debe ser una **prioridad estratégica** para garantizar continuidad, reputación y cumplimiento.

Tendencias que marcarán la **ciberseguridad en 2026**

Inteligencia artificial generativa: aliada y amenaza al mismo tiempo

La IA generativa será una de las tecnologías más influyentes, y también más desafiantes, del nuevo año. Por un lado, permitirá crear sistemas defensivos automatizados, detección de anomalías y respuesta más rápida ante incidentes. También se está convirtiendo en una herramienta de ataque: los ciberdelincuentes están usándola para generar phishing hiperrealista, deepfakes creíbles y malware autorreprogramable.
En 2026, las organizaciones deberán adoptar una IA responsable, basada en datos seguros, auditorías constantes y supervisión humana. El objetivo debe ser utilizar la inteligencia artificial como escudo en las organizaciones.

Zero Trust: el modelo que se consolidará como estándar

El enfoque de “nunca confíes, siempre verifica” dominará la estrategia de seguridad en 2026.
El modelo Zero Trust parte del principio de que ninguna conexión, usuario o dispositivo es confiable por defecto.
Su aplicación implica autenticación multifactor adaptativa (MFA), microsegmentación de red, gestión de identidades privilegiadas y monitoreo continuo. Gracias a esto, las organizaciones logran controlar cada acceso y reducir el riesgo de movimientos laterales dentro de su infraestructura.
Este modelo convertirá la identidad digital y la ciberseguridad en el nuevo perímetro de defensa.

Ransomware industrializado: ataques más dirigidos y costosos

Los virus evolucionarán hacia un modelo de negocio cada vez más estructurado. Los grupos criminales buscarán operar como verdaderas empresas que desarrollan, venden y alquilan herramientas de ataque cibernético, incluso con asistencia técnica incluida.

Los ataques serán más selectivos y personalizados, con foco en infraestructuras críticas, banca, salud y servicios públicos. El rescate promedio podría superar los USD $2 millones por incidente.

Para enfrentarlo, las organizaciones deberán invertir en ciberresiliencia: copias inmutables, planes de recuperación, pruebas de contingencia y análisis continuo de vulnerabilidades. La diferencia entre una empresa resiliente y una reactiva será su capacidad de recuperación.

Protección de infraestructuras críticas: foco en energía y transporte

La digitalización de los sistemas industriales y su conexión con redes de TI ha creado nuevos puntos de entrada para los atacantes. Los sectores energético, transporte, agua y telecomunicaciones serán prioritarios para la ciberprotección en 2026.

Los ataques en estos entornos pueden generar interrupciones de servicio, afectaciones económicas y riesgos físicos. Por ello, veremos un impulso en soluciones de monitoreo inteligente con IA, segmentación de redes, autenticación biométrica para accesos técnicos y protocolos de emergencia digital.

Automatización inteligente: respuesta más rápida ante incidentes

La escasez de talento especializado ha impulsado el desarrollo de automatización inteligente en ciberseguridad. Las herramientas de SOAR (Security Orchestration, Automation and Response) permitirán priorizar alertas, ejecutar acciones automáticas y reducir los tiempos de respuesta de horas a segundos.
En 2026, los centros de operaciones (SOC) adoptarán modelos híbridos: IA + automatización + supervisión humana, logrando una defensa continua y más eficiente.

Retos que enfrentan las organizaciones

La digitalización masiva ha elevado la complejidad de la gestión de riesgos. Entre los principales desafíos destacan:

- Brechas por falta de talento especializado.
- Dependencia de procesos manuales para la detección de amenazas.
- Dificultades para proteger entornos híbridos y múltiples nubes.

Mayor exposición a ataques dirigidos a APIs y dispositivos IoT.

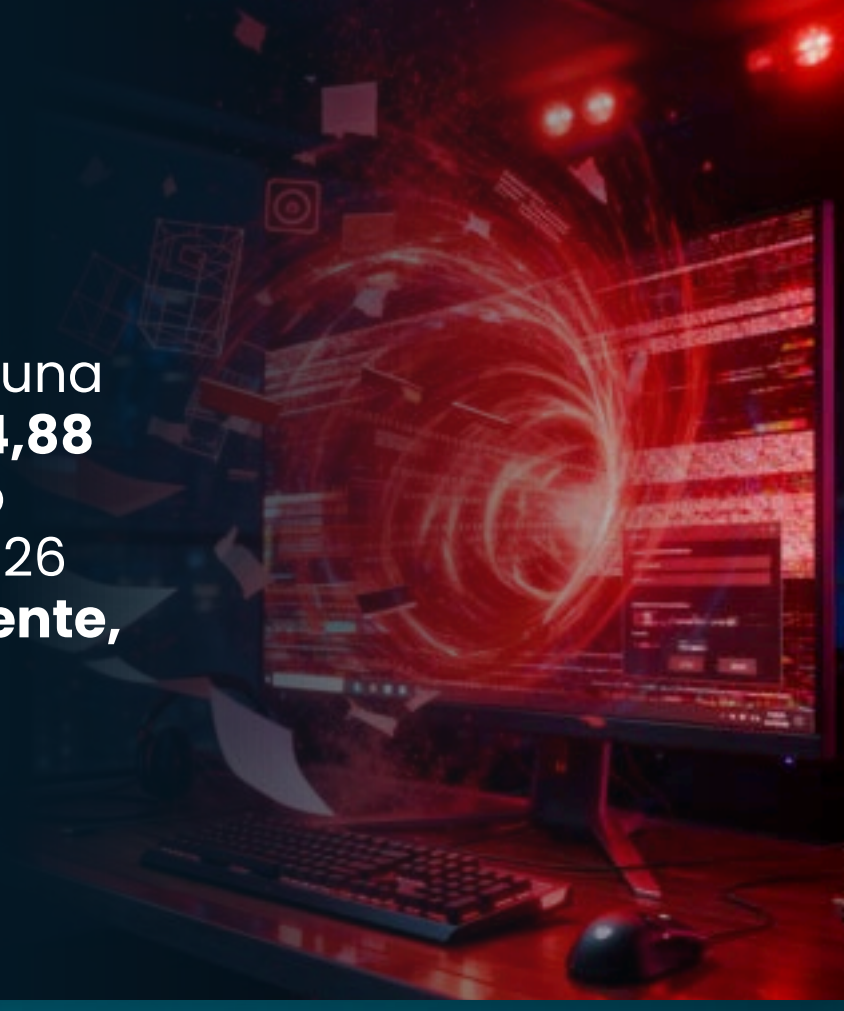
Incremento en los costos de cumplimiento y respuesta ante incidentes.

Superar estos retos implica **construir una estrategia integral** en la que identidad, inteligencia artificial, automatización y cumplimiento normativo se integren bajo un mismo propósito, que es **proteger con anticipación.**

TE PUEDE INTERESAR:

Conoce las principales modalidades de ciberataques en Colombia

DATO RELEVANTE



En 2025, el costo promedio global de una filtración de datos alcanzó los **USD $4,88 millones,** el valor más alto registrado hasta ahora, y se espera que para 2026 supere los **USD $5 millones por incidente,** impulsado por el uso de inteligencia artificial en ciberataques.

Fuente: IBM Cost of a Data Breach Report 2025.

Así construimos confIAnza digital desde OlimpIA

Acompañamos a las organizaciones en su transformación segura, **ayudándolas a anticipar los riesgos,** cumplir con las normativas y proteger lo más valioso la continuidad de su operación, seguridad de sus datos y confianza de sus clientes.

Sabemos que la ciberseguridad no se trata solo de tecnología, sino de personas, procesos y cultura digital. Por eso, nuestras soluciones combinan inteligencia artificial, automatización y experiencia humana para fortalecer cada capa de defensa.
A continuación, te compartimos paso a paso cómo lo hacemos en OlimpIA:

Verificación de identidad real

Combinamos biometría facial, detección de vida o liveness facial (acreditado por iBeta 1 e iBeta 2), OCR inteligente y visión por computador para garantizar que detrás de cada acceso o transacción haya una persona real.
Validamos documentos con fuentes oficiales y analizamos la consistencia de la información en tiempo real, detectando fraudes sofisticados como tampering, deepfakes o screen fraud.
De esta forma, las organizaciones pueden evitar suplantaciones, falsificaciones y pérdidas por fraude, mientras agilizan sus procesos de afiliación o vinculación.

Detección proactiva de riesgo

Nuestros algoritmos de inteligencia artificial analizan en segundos el comportamiento, ubicación y dispositivo de cada usuario, evaluando el riesgo antes del clic final. Esto permite identificar patrones sospechosos y emitir alertas inteligentes sin afectar la experiencia del usuario.
Así, las empresas pueden anticiparse a ataques de ingeniería social, accesos no autorizados o transacciones anómalas, reduciendo al mínimo los incidentes.

Autenticación adaptativa y continua

Implementamos autenticación multifactor (MFA), que se ajusta al canal, tipo de operación y nivel de riesgo detectado.
Protegemos accesos, pagos y gestiones sensibles en todos los canales digitales mediante autenticación continua. De este modo, las organizaciones pueden mantener el equilibrio perfecto entre seguridad y usabilidad, fortaleciendo la relación con clientes y colaboradores.
Así mismo, capacitamos a los equipos para que comprendan la importancia de la autenticación segura, como primera línea de defensa.

Cumplimiento automatizado

Nuestras soluciones generan evidencia verificable de cada validación, registro y autenticación, simplificando auditorías y reduciendo costos administrativos. Cumplimos con los estándares de la Superintendencia Financiera de Colombia (SFC), la Superintendencia de Industria y Comercio (SIC) y la norma ISO 27001, asegurando un marco sólido de gobernanza digital.
El resultado que tenemos se basa en procesos trazables, auditables y conformes con la regulación, lo que refuerza la reputación y confianza de cada organización.

Cultura y resiliencia digital

Ayudamos a las empresas a crear conciencia y cultura cibernética, porque un equipo informado puede detener un ataque antes de que comience.
Impulsamos programas de formación y simulacros de phishing, promovemos el uso de contraseñas seguras, fomentamos la práctica de respaldo y monitoreo constante como hábitos fundamentales.

El futuro de la ciberseguridad empieza ahora

Las organizaciones que se adelanten a los riesgos, inviertan en **IA confiable y fortalezcan su identidad digital** serán las que lideren la transformación segura.

En OlimpIA, ayudamos a las empresas a construir confIAnza digital para **proteger lo que más importa:** las personas, los datos y la reputación.

Agenda una reunión con nuestros expertos y **descubre cómo preparar tu empresa** para los nuevos riesgos digitales.

Haz clic aquí para contactarnos

OlimpIA | Sentry