OlimpIA

Razones por las que las aseguradoras deben adoptar la identidad digital e implementar estrategias de ciberseguridad

¿Sabías que en 2024 se detectaron 30.739 casos de **fraude** en seguros, con un valor superior a los **$272 mil millones?**

La identidad digital y ciberseguridad **son clave para mitigar estos riesgos y proteger a las aseguradoras.**

Si haces parte del sector de seguros, conoces que los fraudes aumentan, las exigencias regulatorias no bajan y cada vez se digitalizan más procesos. Eso implica revisar cómo operas, qué validas y con cuál tecnología estás protegiendo tus canales e información.

Tanto la identidad digital como la ciberseguridad, trabajan en conjunto para operar con precisión y evitar errores y fraudes. En este eBook encontrarás cifras actuales del sector, los puntos críticos que deberías tener en la mira y cómo desde OlimpIA podemos ayudarte a resolverlos con soluciones confiables.

Cifras clave de identidad digital

Durante el evento Next Generation ID, el primer evento de identidad digital en el país que organizamos en OlimpIA, se revelaron datos actuales del desafío que presenta el país:

Se superaron los **600 millones de validaciones de identidad digital en el último año,** demostrando la magnitud del entorno transaccional que requiere autenticación segura.

El **65% de las compañías han reportado un incremento de ataques de fraude digital,** lo cual refuerza la necesidad de implementar herramientas de verificación más precisas.

Según una encuesta realizada por Dynata para Gen (empresa matriz de Norton) en marzo de 2024, el **17% de los colombianos reportaron ser víctimas de robo de identidad digital.**

Cifras clave del asegurador en Colombia

Según Fasecolda, en 2024 el sector asegurador colombiano reporta los siguientes indicadores:

Un crecimiento real del 5,6%, superior al del PIB nacional, que se ubicó en 1,7%.

Más de 2,4 millones de riesgos asegurados, con un valor total cercano a los $2.323 billones.

Una penetración del seguro equivalente al 3,29% del PIB.

Pagos por siniestros que superan los $25,5 billones, con un incremento del 13,6% respecto a 2023.

Un consumo per cápita en seguros de $1.065.064.

Este crecimiento, no obstante, vino acompañado de un aumento considerable en los riesgos digitales y financieros, que comprometen la estabilidad operativa de las compañías.

Riesgos críticos para las aseguradoras

Las modalidades
más comunes incluyen:

Pólizas prestadas, falsas o adulteradas:

Uso indebido de pólizas originales ajenas, creación de pólizas inexistentes o alteración de datos en pólizas reales para cometer fraude.

Suplantación de identidad:

Uso de datos personales de terceros para contratar seguros, cobrar indemnizaciones o realizar trámites sin autorización.

Falsificación documental:

Presentación de documentos alterados o completamente falsos (como licencias o reclamaciones) para obtener beneficios de forma ilegítima.

Accidentes ficticios:

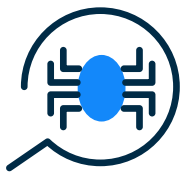
Simulación de siniestros que nunca ocurrieron, con el fin de reclamar indemnizaciones fraudulentas.

Dobles cobros:

Reclamo de una misma indemnización a través de múltiples pólizas o aseguradoras, ocultando la existencia de otros pagos.

Adicionalmente, según el Informe de amenazas cibernéticas en América Latina, realizado por Fortinet, en 2024 Colombia fue blanco de **36.000 millones de intentos de ciberataques.**

El sector asegurador, por la cantidad y sensibilidad de datos que maneja, está entre los más expuestos. Las amenazas incluyen:



Phishing dirigido a usuarios y funcionarios.

Ransomware que afecta la operación interna.

Filtraciones de datos personales de asegurados.

Suplantación de portales y robo de credenciales.

¿Sabías que...?

En 2024, el 30% de los incidentes de ciberseguridad estuvieron relacionados con el abuso de identidades válidas, consolidándose como la principal vía de acceso para los atacantes.

Fuente: IBM X-Force Threat Intelligence Index 2025.

Proyecciones del sector asegurador en Colombia para 2025

Crecimiento del mercado asegurador:

Se estima que el volumen de primas alcanzará los $27,62 billones en 2025, lo que representa un crecimiento del 7,4% respecto al año anterior.

Fuente: Valuerisk, Informe Seguros Colombia, 2024.

Primas de vida y pensiones:

Este segmento ha mostrado un crecimiento significativo, pasando de $13,7 billones en 2013 a $29,35 billones en 2023, y se espera que continúe su tendencia al alza en 2025.

Fuente: Valuerisk, Informe Seguros Colombia, 2024.

Primas de no-vida:

Este segmento muestra un crecimiento sostenido, al pasar de $11,9 billones en 2013 a una proyección de $24,8 billones en 2024, con un incremento anual del 5,2%. Las estimaciones anticipan una leve desaceleración en los próximos años, con tasas de crecimiento del 4,5% en 2025 y 3,8% en 2026, alcanzando los $27 billones.

Fuente: Valuerisk, Informe Seguros Colombia, 2024.

Penetración del seguro:

Se proyecta que el sector asegurador colombiano mantenga una tasa de crecimiento anual compuesta (CAGR) del 6,5% hasta 2026, reflejando un crecimiento moderado pero constante en la adopción de seguros en el país.

Fuente: Fasecolda, Análisis regional del mercado asegurador, 2024.

Retos y oportunidades para las aseguradoras en 2025

Innovación tecnológica

La adopción de inteligencia artificial y tecnologías emergentes son importantes para mejorar la eficiencia operativa y personalización de productos en este sector.

Sostenibilidad y cambio demográfico

El envejecimiento de la población y disminución de las tasas de natalidad impactan la sostenibilidad de los seguros de vida, pensiones y salud, requiriendo soluciones innovadoras adaptadas a estas nuevas dinámicas.

Ciberseguridad

Ante el aumento de amenazas cibernéticas, las aseguradoras deben invertir en soluciones robustas de ciberseguridad para proteger la información sensible y mantener la confianza de sus clientes.

Te puede interesar: La identidad digital y ciberseguridad: Fortaleciendo la ConfIAnza Digital en el sector asegurador

Buenas prácticas en ciberseguridad para aseguradoras

Proteger la infraestructura con tecnologías avanzadas

Firewall de última generación y detección de intrusos (IDS/IPS) para evitar accesos no autorizados.

Análisis de vulnerabilidades y pruebas de penetración para identificar fallos de seguridad antes de que los ciberdelincuentes los aprovechen.

Cifrado de datos y almacenamiento seguro

Proteger la información de clientes, pólizas y pagos mediante cifrado avanzado, utilizando estándares como AES-256, un algoritmo ampliamente adoptado a nivel internacional por su alto nivel de seguridad.

Aplicar segmentación de red para limitar accesos internos y minimizar riesgos.

Capacitación y concienciación en ciberseguridad

El 90% de los ciberataques se originan por errores humanos, según el IBM Cyber Security Intelligence Index Report 2024. En muchos casos, se trata de clics en enlaces maliciosos, contraseñas débiles o acceso indebido a información sensible.

Formar a los equipos en temas como phishing, contraseñas seguras y control de accesos es una medida clave para reducir riesgos, especialmente en sectores como el asegurador, donde la exposición digital es alta.

Estrategia de respuesta a incidentes

Es importante actuar con rapidez y precisión frente a un ciberataque. Contar con una estructura basada en roles dentro del ecosistema de ciberseguridad es clave, aquí te contamos como funciona:

Blue Team: Encargado de la defensa activa e implementación de controles de seguridad.
Su labor incluye la detección temprana, contención de amenazas, remediación y recuperación posterior al incidente.

Red Team: Equipo ofensivo que simula ataques reales (como Ethical Hacking y Pentesting) para identificar vulnerabilidades antes de que sean explotadas por actores maliciosos.

Purple Team: Fomenta la colaboración entre el Blue y Red Team, promoviendo una defensa más sólida basada en aprendizajes compartidos y monitoreo 24/7.

Contar con una estrategia de ciberseguridad es clave para evitar pérdidas económicas, operativas, legales y reputacionales ante posibles ataques.

Adoptar soluciones de identidad digital y ciberseguridad no es solo una necesidad para prevenir fraudes, sino una **ventaja competitiva** para las aseguradoras que buscan diferenciarse en el mercado.

Soluciones de identidad digital para aseguradoras

Las aseguradoras deben involucrar dentro de sus procesos tecnología para validar la identidad de sus usuarios. Estas son las soluciones que se pueden implementar:

Biometría facial: Reconocer a las personas por sus rasgos únicos, como el contorno del rostro o la distancia entre los ojos. Ideal para validar desde cualquier canal digital.

Biometría dactilar: Verificar identidades a través de huellas digitales, una herramienta precisa y confiable para momentos clave como indemnizaciones o aperturas de pólizas.

Validación de documentos: Aplicar algoritmos y técnicas de aprendizaje automático para comparar grandes volúmenes de datos con la base del Archivo Nacional de Identificación, garantizando autenticidad y generando confianza en los resultados.

Beneficios para las aseguradoras con OlimpIA

Desafío	Con OlimpIA	Resultado
Suplantación de identidad	Biometría + IA	Reducción del fraude en onboarding y siniestros
Pérdida de datos y ciberataques	SOC monitoreo 24/7	Prevención proactiva de incidentes
Exigencia normativa	Trazabilidad + auditoría digital	Cumplimiento eficiente ante SIC y SFC
Ineficiencia operativa	Validación automatizada	Agilidad + reducción de costos en validaciones

Siguiente paso: **accionar la** transformación digital

Las aseguradoras que liderarán el futuro serán aquellas que adopten tecnología y la integren de manera estratégica en su ADN empresarial.

La verificación de identidad digital y la ciberseguridad no son solo herramientas, sino habilitadores del crecimiento y sostenibilidad del negocio.

Descubre cómo OlimpIA puede ayudarte a fortalecer tu estrategia de seguridad digital y verificación de identidad.

Hablemos