aseguradores
Nº 516 AÑO 2025

ENTREVISTAS

Carmen González
Allianz
Pedro Agudo Novo
Policía Nacional

ESPECIAL

El tamaño importa: las micropymes lo pasarán peor

Hogar: Los nuevos servicios que se incorporan a las pólizas

pelayo

DAVID FIÑANA
CIO - Director de Tecnología
y Contact Center de Pelayo

Desafíos de ciberseguridad ante la era de la IA

La industria aseguradora atraviesa un momento decisivo marcado por una profunda digitalización. La contratación, la gestión de siniestros y la relación con el cliente se desarrollan en plataformas online, automatización, entornos multicloud y una red cada vez más amplia de proveedores. Esta transformación incrementa de forma significativa la exposición al riesgo cibernético.

Las cifras lo confirman: en 2024 se gestionaron más de 97.000 incidentes de ciberseguridad, un 16% más que el año anterior, según INCIBE. Además del crecimiento cuantitativo, los ataques son cada vez más sofisticados. El ransomware se consolida como la amenaza más relevante, evolucionando desde el simple cifrado de datos hacia el robo de información y la extorsión mediante su publicación. El sector asegurador, por la criticidad de sus procesos y el volumen de datos sensibles que maneja, se ha convertido en un objetivo prioritario para los ciberdelincuentes.

En este contexto, la inteligencia artificial representa un arma de doble filo. Bien utilizada, permite anticipar amenazas, automatizar respuestas y mejorar la eficiencia; mal gestionada, facilita ataques más complejos, como phishing altamente personalizado o fraudes en siniestros mediante imágenes falsas. El desafío va más allá de la tecnología e implica integrar la IA de forma segura, garantizar la continuidad del negocio y responder a un entorno regulatorio cada vez más exigente. Marcos como DORA, NIS2, el AI Act y el RGPD refuerzan las obligaciones en resiliencia, gobernanza y protección de datos, con sanciones económicas y daños reputacionales relevantes en caso de incumplimiento.

La Mediación de seguros ocupa un papel especialmente crítico. Como primer punto de contacto con el cliente, suponen un vector de riesgo clave. Aunque muchos no estén obligados formalmente por DORA, un incidente en un mediador puede tener impacto sistémico. Por ello, es esencial adoptar buenas prácticas de ciberseguridad en todo el ecosistema. El reto es compartido: si uno falla, el riesgo se propaga.

Cumplimiento Integral DORA

La entrada en vigor de la Digital Operational Resilience Act en enero de 2025 marca un punto de inflexión en la gestión del riesgo tecnológico. Esta normativa busca garantizar que las entidades financieras y aseguradoras puedan resistir, responder y recuperarse ante incidentes TIC, imponiendo obligaciones claras en gobernanza, reporting y pruebas de resiliencia.

Para las aseguradoras, esto implica mantener un inventario dinámico de activos críticos, desde aplicaciones y sistemas hasta proveedores estratégicos, vinculado a evaluaciones de impacto. También exige planes de continuidad robustos que contemplen escenarios de ciberataque, interrupciones en servicios cloud y fallos en la cadena de suministro, con pruebas periódicas obligatorias. La gestión contractual cobra protagonismo: los acuerdos con terceros deben incluir cláusulas específicas sobre seguridad, derechos de auditoría y mecanismos de rescisión en caso de incumplimiento.

Otro aspecto clave son las pruebas TLPT, pruebas de penetración basada en amenazas (Threat-Led Penetration Testing), que permite evaluar si son capaces de resistir ante amenazas que simulan ataques reales y requieren una madurez operativa notable en detección y respuesta. Cumplir con DORA no es solo una obligación legal, sino una oportunidad para reforzar la resiliencia y la confianza del mercado. Integrar IA en este proceso —por ejemplo, para automatizar la clasificación de activos o mejorar la detección en pruebas— puede marcar la diferencia entre una postura reactiva y una estrategia proactiva.

Evolución de las amenazas

El ransomware ha dejado de ser un ataque simple para convertirse en una amenaza compleja y altamente rentable. Hoy hablamos de doble y triple extorsión, donde los delincuentes no solo cifran datos, sino que también exfiltran información sensible y presionan a clientes y socios para maximizar el impacto.

Este fenómeno se traduce en interrupciones críticas en procesos de siniestros, riesgos regulatorios por exposición de datos personales y costes directos e indirectos que afectan a la reputación. Para garantizar la seguridad, se aconseja realizar la regla de la triple copia de respaldo, segmentar las redes y emplear sistemas avanzados de monitorización con inteligencia artificial que permitan detectar patrones inusuales. La realización de simulaciones y ejercicios de respuesta es esencial para reducir tiempos de contención.

La IA es clave para anticipar movimientos laterales y automatizar respuestas, pero es igualmente utilizada por los atacantes para perfeccionar sus campañas. De ahí la necesidad de un enfoque integral que combine tecnología, procesos y cultura organizativa.

La dependencia de proveedores tecnológicos y servicios cloud convierte la cadena de suministro en un punto crítico de vulnerabilidad. Las aseguradoras deben evaluar de forma continua la postura de seguridad de sus proveedores, reforzar los contratos con cláusulas específicas sobre cifrado y notificación de incidentes, y desplegar plataformas de monitorización en tiempo real. Las pruebas de resiliencia compartidas y las simulaciones conjuntas son prácticas recomendadas para validar la respuesta ante incidentes.

Identidad y Zero Trust

Las fronteras físicas, traducidas al mundo digital, corresponden al perímetro de la identidad. Y eso es lo que debemos proteger con el modelo Zero Trust. Su premisa es sencilla: ningún usuario o dispositivo debe ser automáticamente confiable, independientemente de su ubicación dentro o fuera de la red de la empresa. Esto implica aplicar autenticación multifactor (código a través del móvil o del mail habitualmente) y verificar de forma continua cada acceso.

En esta línea, la modernización del SOC (Centro de Operaciones de Seguridad) con inteligencia artificial (sea interno o externo) permite correlacionar eventos en tiempo real, reducir falsos positivos y acelerar la respuesta. En un contexto donde las credenciales son la puerta de entrada más habitual, reforzar este pilar es prioritario.

Conclusión

La ciberseguridad en el sector no es solo un reto tecnológico, sino una cuestión estratégica que impacta en la continuidad del negocio, la confianza del cliente y la reputación corporativa.

Normativas como DORA y NIS2 establecen un marco exigente que obliga a las aseguradoras a evolucionar hacia modelos de resiliencia integral. Pero no se trata solo de evitar sanciones, sino de garantizar la continuidad del servicio, proteger la confianza del cliente y, en última instancia, preservar el margen. Un ataque de ransomware que paraliza el sistema de siniestros durante 48 horas no es solo un problema técnico: es un golpe directo a la experiencia del asegurado y a la reputación de la compañía. Del mismo modo, un fallo en la gestión de terceros puede derivar en costes millonarios si no se han previsto cláusulas de salida o pruebas de resiliencia en los contratos.

La IA será un aliado imprescindible para enfrentar amenazas cada vez más sofisticadas, siempre que su adopción vaya acompañada de gobernanza sólida y controles efectivos. Las compañías que entiendan esta lógica y actúen con visión —invirtiendo en tecnología, procesos y personas— estarán mejor preparadas para un entorno donde la pregunta no es si habrá un incidente, sino cuándo y con qué impacto. Y en ese momento, la diferencia entre perder millones o salir reforzado dependerá de las decisiones que se tomen hoy.