

APECOSE 2026

PROTEGIENDO NUESTRO ECOSISTEMA

Las amenazas del cliente y el rol crítico de las empresas de seguros

La Visión del Cliente

Las empresas ya no solo temen al incendio de la planta física; temen la parálisis digital operativa y la destrucción reputacional.

Como aseguradoras y corredores, gestionan su patrimonio y su confianza. Si son vulnerables, **el ecosistema entero colapsa.**

Conozcamos qué le quita el sueño a nuestros clientes asegurados.



1. IA como Herramienta de Negocio

La Adopción Acelerada

- ▶ **Fuga de datos confidenciales:** Empleados ingresando información financiera en modelos públicos.
- ▶ **Sesgos algorítmicos:** Decisiones automatizadas con fallas éticas.
- ▶ **Dependencia operativa:** Fallos en procesos críticos por "alucinaciones" de la IA.

Dato: 55% de empresas usan IA generativa sin políticas claras de seguridad corporativa.



2. IA como Amplificador de Riesgos



El Armamento Digital

- ▶ **Phishing perfecto:** Correos sin errores ortográficos en múltiples idiomas.
- ▶ **Fraude Deepfake:** Clonación de voz de CEOs para autorizar transferencias.
- ▶ **Malware mutante:** Códigos maliciosos que evaden los antivirus tradicionales.

Dato: 300% de aumento global en ataques de suplantación avanzados desde 2023.

3. Fuga de Información (Data Breach)

\$4.99M

COSTO PROMEDIO GLOBAL DE UNA BRECHA

(Reporte IBM 2026)

El impacto del dato expuesto

- ▶ **Multas Regulatorias:** Sanciones severas de la Autoridad Nacional (Ley 29733).
- ▶ **Destrucción Reputacional:** Pérdida inmediata de clientes corporativos.
- ▶ **Litigios:** Demandas de terceros por negligencia en custodia.

El sector seguros es el objetivo número 1 por el tipo de datos que maneja.

4. Malware y Ransomware

Secuestro Operativo

Las pantallas se apagan. Los servidores se cifran.
La empresa se detiene por completo.

- ▶ **Parálisis:** 21 días promedio de inactividad operativa.
- ▶ **Doble extorsión:** Robo previo de datos y amenaza de publicación.
- ▶ **Rescate financiero:** Exigencias millonarias en criptomonedas.



5. Ataques a Infraestructura

Vulnerabilidad Sistémica

El perímetro físico ya no existe. Las empresas dependen de terceros.

- ▶ **Brechas en la Nube:** Configuraciones erróneas en servidores AWS/Azure.
- ▶ **Cadena de Suministro:** Hackeo a través de proveedores menores integrados.
- ▶ **Ataques DDoS:** Sobrecarga masiva que tumba servicios críticos.



6. Amenazas Internas

Negligencia Accidental

El error humano es la principal brecha.

- ▶ Dispositivos perdidos sin cifrar.
- ▶ Uso de contraseñas débiles o repetidas.
- ▶ Envío de datos confidenciales al correo equivocado.

Dolo Malicioso

El enemigo en casa.

- ▶ Robo de cartera por empleados salientes.
- ▶ Venta de credenciales en la dark web.
- ▶ Sabotaje interno de sistemas.

Dato: El 68% de las brechas de seguridad involucran un elemento humano interno.

7. Ingeniería Social



Fraude del CEO

Interceptación de correos para desviar pagos de primas o indemnizaciones a cuentas fraudulentas.



Falsa Urgencia

Manipulación psicológica para que el empleado salte protocolos de validación financiera.



Phishing

Páginas web clonadas para robar las contraseñas de acceso a los portales de aseguradoras.

**Si estas son las amenazas que enfrentan
nuestros clientes, ¿Podemos darnos el lujo
de ser su eslabón más débil?**

LA RESPONSABILIDAD DE LA ASEGURADORA Y LOS CORREDORES

Protejamos la Casa

Gracias por su atención. Espacio abierto para preguntas.

 Eduardo José Castillo Muñoz