12

Ciberseguridad en México: un reto crítico en la gestión de siniestros tecnológicos

En un contexto global donde el ámbito digital ha ganado protagonismo, México enfrenta un escenario complejo en términos de ciberseguridad. La rápida digitalización tanto en el sector público como privado, acompañada de una inversión insuficiente en protección digital, ha propiciado un entorno favorable para el incremento de ciberataques. En este artículo, analizamos las características del problema, su impacto económico y empresarial, así como las acciones clave en el sector seguros para mitigar estos siniestros tecnológicos.

1. CRECIMIENTO EXPONENCIAL DE CIBERDELINCUENTES

Un estudio del Banco Mundial revela que durante la última década el número de ciberdelincuentes en México y América Latina ha crecido un 25 % anual, muy por encima del promedio global del 21 % entre 2014 y 2024. Esta tendencia se asocia directamente a la falla en inversión y regulación en ciberseguridad, donde México destina hasta un 30 % menos que los países desarrollados.

Como consecuencia, el país vive una aceleración de los ciberincidentes: un aumento del 145 % en dispositivos IoT (son objetos físicos con sensores, software y conectividad que les permiten recopilar y compartir datos a través de internet.) y 280 % en plataformas de ecommerce ha ampliado el vector de ataque, provocando mayores brechas de seguridad.

2. SECTORES VULNERABLES ANTE LOS ATAQUES

Según el mismo informe, los sectores más afectados en economías emergentes como México son el gobierno (35 % de los incidentes) y la salud, objetivo frecuente de ataques de ransomware.

Igualmente, otros estudios señalan que México concentra más de la mitad de los ataques cibernéticos de América Latina, con hasta 31 000 millones de intentos en la primera mitad de 2024. Esto se debe tanto a su tamaño económico como a su posición relevante en cadenas globales y el nearshoring.

3. IMPACTO ECONÓMICO DE LOS CIBERATAQUES

No solamente se trata de escalada en eventos delictivos: los efectos en la economía son sustanciales. Un ataque que paralice sistemas clave del gobierno puede llegar a representar hasta 2,4 % del PIB del país. En cambio, una reducción del 75 % en incidentes cibernéticos podría traducirse en un aumento del PIB de hasta 1,5 %.

El volumen de ataques confirma esta tendencia: en 2024 se registraron entre 28 y 31 millones de incidentes contra empresas y ciudadanos mexicanos, con un incremento del 25 % anual.

Jorge Salas Benito
Director Ejecutivo Ancora Seguros y Garantías

4. FRAUDES Y SINIESTROS EN EL SECTOR EMPRESARIAL

Paralelamente, el entorno corporativo mexicano se enfrenta a un panorama preocupante: según El Ceo, el 45 % de las empresas en México reportaron haber sido víctimas de algún tipo de fraude en 2024.

De acuerdo con un estudio de KPMG en 15 estados, los fraudes más frecuentes son:

- Conflicto de interés: 55 % de los casos.
- Robo de identidad: 44 %.
- Malversación de efectivo: 35 %.
- Robo de activos: 32 %.

Además, un 16 % de las compañías enfrentó corrupción que en algunos casos superó los 5 millones de pesos, y un 22 % no pudo calcular con exactitud las pérdidas.

Esta grave situación se ve amplificada por el fragilidad de las empresas en materia de prevención: solamente el 24 % reporta recibir capacitación para la detección de fraudes financieros, y un alarmante 60 % carece de formación adecuada en este ámbito.

5. EL PAPEL DE LAS ASEGURADORAS ANTE LA CRECIENTE OLA DE SINIESTROS

Los datos anteriores plantean una propuesta clara: las compañías de seguros deben ampliar y profundizar sus estrategias en torno a la ciberseguridad:

1. Diseño de pólizas especializadas: incluir coberturas frente a ransomware, robo de identidad, interrupción de negocio digital y filtración de datos.
2. Prevención activa: ofrecer servicios de monitoring de intrusiones (IDS/IPS), análisis de vulnerabilidades y soporte en redacción de protocolos de respuesta a incidentes.
3. Formación y concienciación: implementar programas de capacitación regular en ciberseguridad y detección de fraudes para clientes corporativos.
4. Inspección y auditoría: verificar la implementación de normas como ISO 27001 o NIST dentro de sus clientes, como condición de asegurabilidad.
5. Resiliencia y respuesta rápida: colaboración con empresas de forense digital y crisis managers para actuar inmediatamente tras un incidente.
6. Asesoría regulatoria: orientar a los clientes sobre leyes nacionales —la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)— y normas internacionales.

6. CONCLUSIÓN

México está en un punto crítico en materia de ciberseguridad: un incremento del 25 % anual en ciberdelincuentes, millones de ciberataques registrados, y casi la mitad de las empresas sufriendo fraudes reflejan una realidad vulnerable. La inversión deficiente en protección digital y la falta de conciencia frente a estos riesgos no solo generan siniestros recurrentes, sino también un impacto negativo significativo en la economía y en la reputación institucional.

En este contexto, el sector asegurador está en una posición privilegiada para liderar la transición hacia un entorno más seguro. Las pólizas deben replicar la complejidad del cibercrimen, no solo indemnizando las pérdidas, sino acompañando activamente a los clientes con prevención, resiliencia y respuesta efectiva. Es el momento de elevar la ciberpreparación de México, con colaboraciones público-privadas, inversiones estratégicas en seguridad y un seguro cibernético robusto como herramienta esencial en la gestión moderna de siniestros.