Regulaciones impulsan adopción de seguros por riesgos cibernéticos

Boletín N°:

Ene 20, 2026 MUNDO

La conversación sobre las pólizas de seguro cibernético en México y América Latina se mueve por una fuerza concreta, la regulación. No porque las leyes obliguen a comprar una póliza, sino porque elevan el costo de un incidente al abrir la puerta a sanciones, responsabilidades frente a terceros y presiones de cumplimiento que no se resuelven solo con “mejorar la seguridad”.

En este contexto, el seguro aparece como una herramienta financiera para transferir parte del riesgo, especialmente cuando la operación digital se volvió crítica tras la aceleración tecnológica de la pandemia.

“GDPR fue el eje principal en materia normativas a nivel internacional. Brasil hizo una copia muy cercana del marco que estableció GDPR y en México en los últimos años ha habido leyes que empiezan a imponer responsabilidades, especialmente pecuniarias”, dijo Sergio Torres, Financial Lines & Cyber LATAM Leader de Aon.

De acuerdo con Torres, el marco europeo (GDPR) se convirtió en referencia para elevar estándares y responsabilidades en distintos países. A partir de ahí, la región comenzó a adoptar o adaptar normas con implicaciones económicas, es decir, multas, sanciones y exposición legal que fuerzan a las empresas a profesionalizar su gestión de riesgo.

Poca visibilidad de incidentes

Aun con ese empuje regulatorio, la región carga con un problema que frena la madurez del mercado, la poca visibilidad pública de los incidentes cibernéticos. Si no hay obligación de divulgar brechas o ataques, el termómetro estadístico se queda corto y el riesgo se subestima.

Para Torres, esto deriva en un subregistro que complica dimensionar el problema, aunque algunos países muestran una evolución más rápida por su exposición y volumen de ataques.

“En Latinoamérica, incluyendo México, como no existe la obligación de hacer divulgación de estos incidentes, hay un subregistro de incidentes a pesar de que Brasil, México y Colombia son los tres países más atacados”, dijo.

En ese marco, el seguro cibernético entra como producto con una estructura relativamente estandarizada. Torres explicó que, más allá del país, las coberturas tienden a parecerse entre sí en la región y a alinearse con lo que se negocia en

mercados más maduros, como Estados Unidos y Europa.

El diseño típico se organiza por módulos: responsabilidad civil (terceros), pérdidas propias (first party) y un componente asistencial de respuesta ante incidentes.

La lógica de los módulos ayuda a entender por qué el seguro gana tracción cuando la regulación aprieta. En responsabilidad civil, una empresa puede enfrentar reclamaciones de clientes, reguladores o competidores si un incidente compromete datos. En pérdidas propias, el golpe puede ser directo a caja: desde investigación forense y abogados hasta el costo más temido hoy, la interrupción de operación.

El tercer módulo es el que vuelve operativa a la póliza en el momento crítico: la asistencia para responder a un incidente. En la práctica, dijo Torres, funciona como una línea de ayuda que activa especialistas para contener el ataque, reducir pérdidas y apoyar decisiones inmediatas. Esta capa se vuelve relevante en ataques que exigen velocidad de respuesta, como el ransomware.

Ransomware

En ransomware, es decir, el secuestro de sistemas o información, Torres confirmó que las pólizas pueden contemplar el pago de rescates dentro del módulo de pérdidas propias, además de activar la asistencia para recuperar operatividad.

No obstante, el directivo advirtió que el uso de esa cobertura ha cambiado. Los grandes corporativos con exposición internacional tienden a ser más cautelosos porque pagar no garantiza la devolución de datos ni evita reincidencia, y además abre el dilema de incentivar el delito.

“Los ataques de ransomware en muchos casos exigen rescates estos rescates también están incluidos en las coberturas. Las pérdidas propias pueden llegar a incluir el valor de rescate pero los clientes más grandes toman posiciones más precavidas, porque pagar no equivale a la tranquilidad de que le van a devolver sus datos u operatividad y que no vuelva a suceder”, dijo Torres.

Seguro para pymes

La expansión del seguro de riesgos cibernéticos también está empujando ajustes para las pequeñas y medianas empresas (pymes), tanto en requisitos como en la forma de cuantificar el riesgo. Torres advirtió que el mercado calibra lo que exige según tamaño y facturación. Los controles y la “higiene cibernética” que son razonables para un gran conglomerado no necesariamente lo son para una empresa pequeña.

La autenticación multifactor (MFA), por ejemplo, fue “el santo grial” durante la pandemia y llegó a ser condición para obtener cobertura; hoy, ante la realidad del ecosistema pyme, las aseguradoras han ampliado su apetito.

“El nivel de madurez e higiene cibernética no se lo puedes exigir a las pequeñas y medianas empresas. Durante la pandemia, el cliente que no tuviera MFA no era objeto de cobertura. Hoy las aseguradoras han abierto su apetito, para absorber este tipo de clientes”, dijo.

Fuente

Fuente: El Economista

Enlace:
https://www.eleconomista.com.mx/amp/tecnologia/regulaciones-impulsan-adopcion-seguros-riesgos-ciberneticos-20260108-794432.html