LITORALPRESS

Fecha: 13-01-2026
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Columnas de Opinión
Título: **Columnas de Opinión: El seguro que no cubrirá el próximo ciberataque**

Pág. : 16
Cm2: 253,5

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

TRIBUNA LIBRE

El seguro que no cubrirá el próximo ciberataque

SEBASTIÁN DUEÑAS
PROGRAMA DE DERECHO, CIENCIA Y TECNOLOGÍA UC

MATÍAS ARÁNGUIZ
PROGRAMA DE DERECHO, CIENCIA Y TECNOLOGÍA UC

En junio de 2017, el malware NotPetya se propagó desde Ucrania al mundo en horas, causando un daño total estimado en US$ 10 mil millones. Maersk perdió cerca de US$ 300 millones, Merck más de US$ 800 millones y FedEx aproximadamente US$ 400 millones.

Cuando Merck reclamó a sus aseguradoras, estas rechazaron el pago argumentando que NotPetya fue obra del GRU (la inteligencia militar de Rusia) y, por tanto, constituía un "acto de guerra" excluido de cobertura. Siguieron siete años de litigio por US$ 1.400 millones.

Merck ganó en tribunales, pero la victoria fue pírrica. Lloyd's de Londres reaccionó exigiendo que, desde 2023, toda póliza de ciberseguridad excluya explícitamente los ciberataques respaldados por Estados. De esta forma, el mercado asegurador global cambió las reglas.

¿Qué significa esto para Chile? Que las pólizas de ciberseguridad emitidas o renovadas en los últimos años probablemente contienen exclusiones que podrían dejar desprotegidas a sus titulares. Si mañana un malware atribuido a Rusia, China o Corea del Norte afecta una empresa chilena como "daño colateral" de un conflicto lejano, la aseguradora podría rechazar el reclamo.

> "Si mañana un malware atribuido a Rusia, China o Corea del Norte afecta a una empresa chilena como 'daño colateral' de un conflicto lejano, la aseguradora podría rechazar el reclamo".

El problema es la atribución. Una porción significativa de los ciberataques contemporáneos responde a lo que se denomina "guerra híbrida": operaciones en el ciberespacio ejecutadas por agentes estatales o proxies de otras naciones, diseñadas precisamente para dificultar la identificación del responsable. ¿Quién determina si un ataque es "estatal"? ¿Qué pasa si la atribución cambia con el tiempo, o si responde a motivaciones políticas más que a evidencia técnica? Las cláusulas modelo de Lloyd's dejan estas preguntas abiertas, creando significativa incertidumbre contractual.

Para Chile, esto no es abstracto. Por ejemplo, nuestros sectores minero y de energía (infraestructura crítica por excelencia) están expuestos a espionaje estatal por cobre, litio, estimaciones de consumo energético, entre otros. Asimismo, existe riesgo de contagio desde ciberoperaciones contra Argentina o Brasil en contextos de tensión geopolítica regional. La pregunta es si las pólizas actuales cubrirían estos escenarios.

La Ley 21.663 obliga a entidades críticas a implementar medidas de seguridad y mitigación en ciberseguridad. Pero, ¿incluye esto la exigencia de cobertura aseguradora adecuada? Si las pólizas excluyen precisamente los ataques más probables y devastadores, como aquellos respaldados por Estados, ¿están las empresas cumpliendo realmente con estándares efectivos de gestión de riesgo?

En Chile, la paradoja es evidente. Mientras se construye un marco regulatorio para prevenir y responder a ciberataques, el mercado asegurador global se retira silenciosamente de los riesgos más catastróficos. De esta manera, la brecha entre exposición real y cobertura contratada puede ser enorme.

NotPetya demostró que US$ 1.400 millones pueden quedar en disputa por seguros diseñados para décadas pasadas. Hoy, la pregunta no es si habrá otro ataque de esa magnitud, sino quién asumirá el costo cuando los seguros no lo hagan.