DF

Fecha: 24/11/2023 Audiencia: 48.450 Sección: ACTUALIDAD
Vpe: $6.023.900 Tirada: 16.150 Frecuencia: DIARIO
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 80,93%

¿Cuáles son las responsabilidades de las empresas ante un ciberataque?

JULIO CASTRO

- En Chile no existe una norma general de ciberseguridad y las obligaciones de las personas jurídicas son reguladas por normas sectoriales.
- La aprobación de los proyectos de ley marco de Ciberseguridad y el de Protección de Datos -ambos en trámite en el Congreso- podrían aumentar las obligaciones y responsabilidades.

POR M. ZECCHETTO Y R. OLMOS

La magnitud de los ataques con *ransomware* (secuestro de datos) que sufrió GTD el 23 de octubre aún mantienen a la empresa de telecomunicaciones trabajando para solucionar los daños producidos. Este evento encendió las alarmas en torno a las responsabilidades y la respuesta que deben tener las compañías ante ciberataques.

Chile hoy no cuenta con una normativa general en materia de ciberseguridad, por lo que las obligaciones, deberes y estándares aplicables de las empresas están determinados por normas sectoriales y, por ende, varían en función de cada sector regulado.

Sin embargo, y según especialistas en la materia, este escenario cambiaría una vez que se apruebe y entre en vigencia la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, que está en su segundo trámite en la Cámara de Diputados.

El proyecto crea un modelo de gobernanza que promueve la gestión de riesgos y la implementación de estándares de ciberseguridad en los sectores público y privado, a través de la definición de conceptos, principios y deberes.

Regulación sectorial

El director del grupo de Protección de Datos y Tecnología de Carey, José Ignacio Mercado, explicó que, en algunos casos, las obligaciones sectoriales pueden abarcar, por ejemplo, medidas técnicas y organizativas para gestionar los riesgos de ciberseguridad, implementar planes de continuidad operacional y la obligación de reportar incidentes.

"La normativa sectorial existente hasta el momento ha sido emitida por la Comisión para el Mercado Financiero en el sector bancario y financiero, la Subtel en el caso de operadores de telecomunicaciones, el Coordinador Eléctrico Nacional para la industria eléctrica, la Subsecretaría de Redes Asistenciales en materia de redes asistenciales, entre otros", dijo Mercado.

En tanto, el socio y experto en protección de datos de Aninat Abogados, Martín Mois, explicó que la Ley General de Telecomunicaciones establece consecuencias para la interrupción de un servicio que no esté solucionado dentro de ciertos plazos.

Según el especialista, esta ley no distingue si los usuarios son personas naturales o empresas. "Por ejemplo, si el servicio se interrumpe por más de seis horas en un día o 12 horas continuas, te hacen un descuento".

Añadió que si la interrupción sobrepasa las 48 horas y no tiene como causa un caso fortuito o de fuerza mayor, el usuario debe ser indemnizado con hasta el triple del valor de la tarifa diaria, sin considerar todos los perjuicios que se puede producir a en este caso, tanto para la empresa como para el cliente.

Además, el abogado señaló que, en estos casos, también entra en juego la Ley de Protección al Consumidor, la cual establece multas desde UTM 300 ($ 19,2 millones) hasta UTM 1.500 ($ 95,9 millones). También, la ley deja sujeto al proveedor al riesgo de enfrentar una demanda colectiva.

En tanto, Mercado, de Carey, señaló que para las empresas eléctricas, está el Estándar de Ciberseguridad para el Sector Eléctrico del Coordinador Eléctrico Nacional, el que se establece una serie de obligaciones y requisitos mínimos de resguardo de la ciberseguridad que deben aplicar las empresas. Entre otros, implementar políticas de ciberseguridad; programas de concientización y capacitación; programas de administración y revocación de accesos.

Por el lado la banca y entidades financieras, el abogado comentó que entre las normas que la CMF aplica al sector, están los lineamientos de la Recopilación Actualizada de Normas, que dicta mínimos a cumplir en ciberseguridad, como la obligación de reportar un incidente en 30 minutos y el rol del directorio.

"Se establece como obligación del directorio el asegurar que la entidad mantenga un Sistema de Gestión de la Seguridad de la Información y Ciberseguridad, que contemple la administración específica de los riesgos y que considere las mejores prácticas internacionales en la materia", dijo Mercado.

Sanciones en proyectos de ley

Según Mois, de aprobarse el proyecto de Ley de Ciberseguridad e Infraestructura Crítica en su versión actual, las multas por incumplimiento van desde las UTM 1 ($ 63.960) a UTM 1.000 en caso de infracciones leves, UTM 1.001 a 5.000 en caso de infracciones graves (pero si el operador está calificado como de importancia vital, suben a UTM 10.000), y por infracciones gravísimas de UTM 10.001 a 20.000.

Por otro lado, en el proyecto de Ley de Datos Personales -en su versión actual-, las sanciones por infracciones graves (como vulnerar o infringir las obligaciones de seguridad en el tratamiento de datos personales) pueden ascender a UTM 5.000 o, en caso de empresas, hasta el equivalente al 2% de los ingresos anuales por ventas y servicios y otras actividades del giro durante el último año calendario, con un tope de UTM 10.000.

Las multas por infracciones gravísimas (como omitir en forma deliberada la comunicación de las vulneraciones a las medidas de seguridad que puedan afectar la confidencialidad, disponibilidad o integridad de los datos personales) pueden ascender a UTM 10.000, en caso de empresas, hasta la suma equivalente al 4% de los ingresos anuales por ventas y servicios y otras actividades del giro durante el último año calendario, con un tope de UTM 20.000.

En tanto, respecto del derecho de los consumidores, Mercado señaló que, si bien las modificaciones a la normativa protectora no han contemplado el reforzamiento expreso de las normas en este contexto, el Servicio Nacional del Consumidor (Sernac) sí ha desplegado iniciativas, como promover canales de denuncia para fraudes y plagios, entre otros, "que pudieran poner en peligro los derechos de los consumidores".