EL MERCURIO

ECONOMÍA Y NEGOCIOS | B

www.economiaynegocios.cl | @eyn_elmercurio | SANTIAGO DE CHILE, JUEVES 11 DE ABRIL DE 2024 | economiaynegocios@mercurio.cl

BOLSAS DE VALORES

Índice	Valor	Var. (%)
SP IPSA	6.688,03	0,29
SPCLXIGPA	33.868,27	0,32
Dow Jones	38.461,51	-1,09
Nasdaq	16.170,36	-0,84
Bovespa	128.053,74	-1,41

UF

Día	Valor ($)
Miércoles 10	37.162,94
Jueves 11	**37.167,89**
Viernes 12	37.172,84
Sábado 13	37.177,78
Domingo 14	37.182,73

MONEDAS

	Valor	Var. (%)
Dólar observado	953,51	1,37
Dólar interbancario	953,30	1,22
Euro	1.024,40	0,36
Peso argentino (US$)	865,29	-0,07
Bitcoin (US$)	70.739,85	1,34

MATERIAS PRIMAS

	Valor	Var. (%)
Cobre (US$/Libra)	4,25	0,75
Petróleo Brent (US$/Barril)	90,48	1,19
Oro (US$/Onza)	2.334,04	-0,80
Celulosa NBSK (US$/Ton.)	1.399,12	0,36
Hierro 62% (US$/Ton.)	109,00	0,46

Despachan a ley proyecto de **estabilización de las tarifas eléctricas**

MODERARÁ ALZAS PREVISTAS | B 8

Directores podrían ser responsables de ilícitos informáticos que ocurriesen en la compañía:

El efecto amplificador de la nueva norma de ciberseguridad en la Ley de Delitos Económicos

CATALINA MUÑOZ-KAPPES

La nueva legislación, junto con la ley ya vigente, aumenta la necesidad de las empresas de incluir aspectos de ciberseguridad en sus modelos de prevención.

El lunes se publicó la Ley Marco de Ciberseguridad, legislación que busca dictar protocolos para prevenir, reportar y resolver incidentes de ciberseguridad, y que establece la creación de la Agencia Nacional de Ciberseguridad (Anci).

Un aspecto más desconocido es la vinculación de esta regulación con la Ley de Delitos Económicos, normativa que se publicó el año pasado y que ya está vigente para ejecutivos de las empresas.

Delitos informáticos

Rodrigo Reyes, director jurídico de Prelafit Compliance, explica que "los delitos informáticos son considerados económicos y la empresa podría responder criminalmente cuando el delito es cometido desde una posición en una empresa o en provecho económico de esta", de acuerdo con la Ley de Delitos Económicos.

Carlos Vernaza, abogado penalista y socio de Estudio Navarro, detalla que los delitos informáticos incluyen una gama amplia de acciones, tales como ataques a la integridad de un sistema informático, acceso ilícito, interceptación ilícita, ataque a la integridad de los datos informáticos, falsificación informática, receptación de datos informáticos, fraude informático y abuso de los dispositivos.

Pese a que la Ley de Ciberseguridad no tiene incidencia penal directa, afirma José Ignacio Mercado, director de Carey, con esta legislación se pueden derivar consecuencias para las empresas. Por ejemplo, multas por no haber cumplido los estándares de diligencia exigibles o no haber dado cumplimiento a las obligaciones de notificación.

Modelos de prevención

Ambas normativas en su conjunto hacen necesario que las compañías incluyan en sus modelos de prevención los riesgos asociados a la ciberseguridad.

AFP

La Ley Marco sobre Ciberseguridad fue promulgada este lunes.

"De cara a los directorios, los deberes fiduciarios, más las consecuencias que para una empresa sujeta a la Ley de Ciberseguridad pueden derivar de eventos de ciberseguridad, generan la necesidad de adoptar las acciones necesarias para mitigar estos riesgos, más que para 'prevenir' la ocurrencia de un ilícito", afirma Mercado. Añade que por las consecuencias extremadamente gravosas para una empresa, "es evidente que una compañía debe identificar sus riesgos tecnológicos y adoptar las medidas para atenuarlos".

Vernaza asevera que un modelo de prevención, para ser considerado eficaz, debe "necesariamente incluir aspectos relacionados a la ciberseguridad". Esto incluye los delitos informáticos que puedan ser cometidos por miembros de las firmas, pero también por terceros que les presenten servicios, acota.

En ese sentido, los directores pueden tener responsabilidad por los delitos informáticos cometidos dentro de la empresa. "Los directores serán responsables de la ciberseguridad en tanto no contribuyan a la implementación de un ambiente de control de ciberseguridad en la empresa", dice Ramón Montero, director de operaciones de BH Compliance. Agrega que "en caso de que no exista un Modelo de Prevención de Delitos debidamente implementado y se cometiera algún delito informático, la consecuencia es que podría generar una responsabilidad penal de la empresa".

Hacking ético

Un aspecto del Código Penal que sí modifica la Ley de Ciberseguridad es respecto al delito de acceso ilícito. Mercado detalla que la nueva legislación establece una exención de responsabilidad penal bajo ciertas condiciones.

"La lógica detrás de esto es permitir las actividades de *ethical hacking*, sin necesidad de requerir el consentimiento de la entidad respectiva, pero asegurándose de que quien lleva a cabo estas actividades no se aproveche de esta circunstancia especial", señala.

Sin embargo, esto aplica solo para los órganos de la administración del Estado, ya que respecto de instituciones privadas, es necesario el consentimiento de la empresa.