Deloitte.

Compliance*Trends*

by Deloitte

Edición 2

Desafíos del Compliance ante la modificación de la Ley Nº 21.459 sobre Delitos Informáticos

Por **Oscar Martínez Yvirmas** | Gerente Risk Advisory

El fenómeno de la ciberdelincuencia en las compañías se ha tornado un dolor de cabeza para las áreas de ciberseguridad, puesto que en el último período han incrementado enormemente los ataques informáticos, como, por ejemplo: ransomware (secuestro de datos) o accesos no autorizados y su filtración a terceros, por ejemplo, los sufridos en sectores regulados en nivel Latinoamérica.

Ello, no solo ha generado un impacto importante para estas áreas y han tenido que fortalecerse para dar respuesta a estos desafíos, ya que dichos ataques informáticos varias veces pueden implicar un alto riesgo de infracciones de algunas regulaciones y, por ende, la obligación de reporte a Superintendencias o autoridades judiciales, por ejemplo. En este punto, las áreas de cumplimiento se vuelven actores relevantes para afrontar correctamente estas situaciones de contingencia.

Ahora bien, si relacionamos esta situación a los requerimientos de la normativa "Ley Nº 21.459 sobre Delitos Informáticos", que incorpora de manera expresa a los ilícitos informáticos en los sistemas de cumplimiento de las compañías, el escenario se tornar un poco más complejo.

Recordemos, que la Ley Nº 20.393 sobre Responsabilidad Penal de las Personas Jurídicas atribuye la responsabilidad penal en cuanto al defecto organizacional, es decir, que debido al incumplimiento de los deberes de dirección y supervisión que tienen los sujetos señalados en el art. 3º de la citada norma, que son relacionada con Alta Dirección o Gerencia de una compañía.

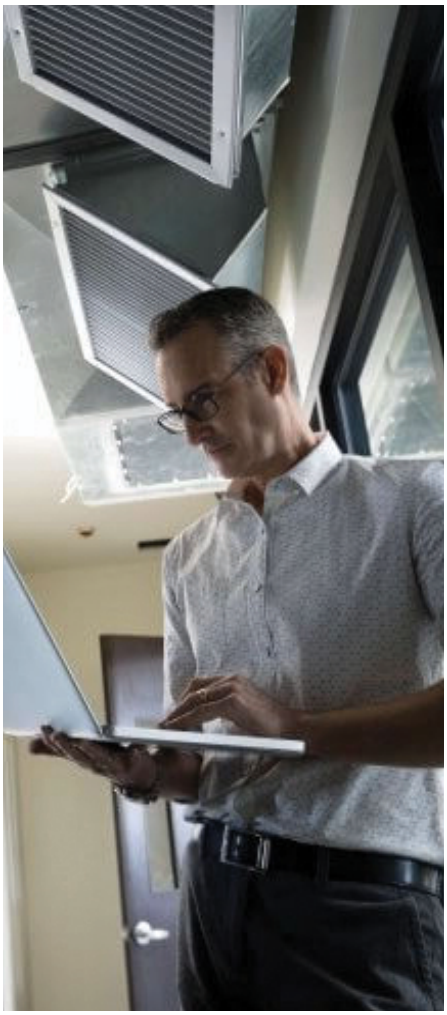
Hay que tener presente, que la eximente de responsabilidad penal (o atenuante, si procediese) se configura en cuanto exista un sistema que permite identificar las actividades, ya sea habituales o esporádicas, que permita la realización o incremento el riesgo de los delitos, entre ellos ahora los informáticos. Es importante mencionar, que la comisión del ilícito debe reportar un interés o provecho para la persona jurídica, expresiones que ha generado complejidades al momento de identificar especialmente en materia informática en cuanto a cómo se configura este "interés o provecho"; No obstante, a nivel internacional los ejemplos se presentan desde actividades en ciertos mercados competitivos hasta derechamente, ingresar a un sistema de un tercero e inutilizarlo.

Ante este desafío emergente, las organizaciones deben ser capaces de diseñar y adoptar un programa de cumplimiento enfocado a las necesidades del entorno y al perfil de riesgos organizacionales para

prevenir la ciberdelincuencia, entre los elementos claves a considerar en el programa se encuentran:

- **Identificación:** Identificar los riesgos en materia de ciberdelincuencia a los que se enfrenta la organización, teniendo en consideración el impacto y la probabilidad de que se materialicen.
- **Prevención:** Una vez identificados los riesgos, se deben diseñar, implementar y evaluar procedimientos (controles) que protejan a la organización y mitiguen los riesgos identificados.
- **Monitoreo continuo:** La eficacia de los controles implementados debe ser monitoreada de forma continua, a objeto de garantizar que los mismos se encuentren operando.
- **Generación de cultura:** Paralelamente, la Alta Administración y todos los stakeholders de la organización, deben ser capacitados, entregándoles información necesaria para llevar a cabo sus labores de acuerdo con los cambios normativos y con el objetivo de impedir debilidades internas.

Finalmente, la función de Cumplimiento debe poner un foco de atención cada vez más importante en los diversos aspectos asociados a la transformación digital en las compañías, con el objetivo de reducir las potenciales debilidades internas y potenciar las capacidades internas asociadas a la incorporación de diversas tecnologías para operar con un grado de "ciberseguridad razonable", en entornos cada día más conectados con la tecnología.



Rosario Norte 407
Las Condes, Santiago
Chile
Phone: (56) 227 297 000
Fax: (56) 223 749 177
deloittechile@deloitte.com

Av. Grecia 860
3rd floor
Antofagasta
Chile
Phone: (56) 552 449 660
Fax: (56) 552 449 662
antofagasta@deloitte.com

Alvares 646
Office 906
Viña del Mar
Chile
Phone: (56) 322 882 026
Fax: (56) 322 975 625
vregionchile@deloitte.com

Chacabuco 485
7th floor
Concepción
Chile
Phone: (56) 412 914 055
Fax: (56) 412 914 066
concepcionchile@deloitte.com

Quillota 175
Office 1107
Puerto Montt
Chile
Phone: (56) 652 268 600
Fax: (56) 652 288 600
puertomontt@deloitte.com

Deloitte.

www.deloitte.com

Las partes aceptan que COVID 19 constuye Fuerza Mayor, conforme los términos del artículo 45 del Codigo Civil. Asimismo, Las partes reconocen los riesgos que implica la propagación de la COVID-19 y las repercusiones potenciales asociadas con la prestación de los Servicios. El personal de las partes cumplirá con las restricciones o las condiciones que impongan sus res pectivas organizaciones en las prácticas laborales a medida que la amenaza de la COVID-19 continúe. Las partes intentarán seguir cumpliendo con sus obligaciones respectivas conforme a los plazos y el método establecido en la presente, pero aceptan que puede requerirse la adopción de prácticas laborales alternativas y la puesta en marcha de salvaguardas durante este periodo, tales como el trabajo a distancia, las restricciones de viaje relacionadas con destinos particulares y la cuarentena de algunas personas. Dichas prácticas y salvaguardas laborales pueden afectar o impedir la ejecución de diversas actividades, por ejemplo, talleres u otras reuniones en persona. Las partes trabajarán conjuntamente y de buena fe a fin acordar los eventuales cambios necesarios para atenuar los efectos negativos de la COVID-19 sobre los servicios, incluido el cronograma, el enfoque, los métodos y las prácticas laborales en la prestación de los mismos, y todos los costos asociados adicionales. En todo caso, Deloitte no será responsable de cualquier incumplimiento o retraso en la ejecución de sus obligaciones ocasionados o exacerbados por la propagación de la COVID-19 y sus efectos asociados.