COMPLIANCE

ALERTA LEGAL

NUEVA LEY SOBRE DELITOS INFORMÁTICOS

Con fecha **20 de junio de 2022** se publicó en el Diario Oficial la nueva ley sobre delitos informáticos, cuyo objetivo es actualizar nuestra normativa en materia de delitos informáticos y ciberseguridad, reemplazando a la actual Ley 19.223 y modificando otros cuerpos normativos, de manera de adecuar nuestra legislación al Convenio de Budapest sobre Ciberdelincuencia.

Es importante destacar que esta Ley **modifica a la Ley 20.393,** sobre Responsabilidad Penal de las Personas Jurídicas, en términos que ahora las personas jurídicas podrán ser responsables por los delitos señalados en la normativa.

Dentro de las disposiciones incorporadas por la ley destacamos las siguientes:

I. Se contemplan los siguientes **delitos**:

1. De **ataque a la integridad de un sistema informático**, en aquellos casos en que se obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático por la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos y, en caso de que el ataque sea **solo a la integridad de datos informáticos**, ya sea alterándolos, dañándolos o suprimiéndolos, la normativa establece una pena disminuida en un grado.

2. De **acceso ilícito**, en el que se sanciona a quien, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático. Ahora, si tal acceso fuese con el ánimo de apoderarse o usar la información contenida en el sistema informático o se divulgase la información a la que se accedió de manera ilícita, se aplicará una pena en un grado mayor.

3. De **interceptación ilícita** para quienes indebidamente intercepten, interrumpan o interfieran, por medios técnicos, la transmisión no pública de información en un sistema informático. Si a través de tal interceptación se capten datos contenidos en un sistema informático será castigado con una pena aumentada en un grado.

4. La **falsificación de datos informáticos** para que sean tomados como auténticos o utilizados para generar documentos auténticos. Luego, en caso

Nota: El presente documento fue preparado sólo para fines informativos y no debe ser considerado como asesoría legal.

de que quien realice esta conducta sea un funcionario público, abusando de su oficio, se aumenta el rango de penas que se podrán imponer.

5. **Receptación de datos informáticos** para quien comercialice, transfiera o almacene datos informáticos provenientes de los delitos descritos anteriormente, sea que conozca el origen ilícito de tales datos, o no pueda menos que conocerlo.

6. De **fraude informático** para quien, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos. En este caso la ley establece una escala de penas de acuerdo con el nivel de perjuicio ocasionado.

7. **Abuso de los dispositivos** para quien obtuviere, importare, difundiera o realizare otra forma de puesta de disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados para la perpetración de los delitos expuestos anteriormente.

II. Luego, la Ley introduce una serie de circunstancias **atenuantes y agravantes**:

1. **Atenuante especial de cooperación eficaz** en el esclarecimiento de los hechos investigados que sean constitutivos de algunos de los delitos de la Ley o que sirva para prevenir o impedir la perpetración de otros delitos de igual o mayor gravedad de los contemplados en la Ley.

2. **Agravantes:**
   a. En caso de que el ilícito se cometa **abusando de la posición de confianza en la administración** del sistema o custodia de datos.

   b. O, si se cometiera el delito **abusando de la vulnerabilidad** confianza o desconocimiento de NNA o adultos mayores.

   c. Y, en caso de que la comisión del delito **hubiese interferido con la provisión o prestación de servicios de utilidad pública** o **procesos electorales**.

      Además, en estos casos la investigación podrá ser iniciada por querella del Ministerio del Interior y Seguridad Pública, de los Delegados Presidenciales Regionales y de los Delegados Presidenciales Provinciales.

Nota: El presente documento fue preparado sólo para fines informativos y no debe ser considerado como asesoría legal.

III. En **materias procedimentales**, se permite en la investigación de estos delitos la solicitud de medidas intrusivas de investigación contempladas en los artículos 222 a 226 del Código Procesal Penal y, además, con el fin de esclarecer los hechos tipificados en la Ley, impedirlos, comprobarlos o establecer la identidad y participación de personas determinadas en la comisión de estos el Juez de Garantía, a solicitud del Ministerio Público, podrá ordenar a las policías **actuar bajo identidad supuesta** ("agente encubierto") en comunicaciones mantenidas en canales cerrados de comunicación.

Señalándose, además, que el agente encubierto estará **exento de responsabilidad criminal** por aquellos delitos en los que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden debida proporcionalidad con su finalidad.

Asimismo, se permite al Ministerio Público, previa autorización judicial, requerir a proveedores de servicios la información relativa al tráfico y el contenido de comunicaciones de sus abonados, correspondiente a un periodo determinado. A su vez, los proveedores de servicios deberán **mantener dicho requerimiento en secreto** hasta por un plazo de dos años renovables mediante resolución fundada.

IV. Finalmente, en el artículo 19 de esta Ley se **modifica también la Ley 19.913** que crea la Unidad de Análisis Financiero ("UAF") agregando como ilícito en el artículo 27 de tal normativa, quien disimule u oculte el origen ilícito de determinados bienes a sabiendas de que provienen de delitos informáticos, convirtiéndose, por tanto, en un tipo base de la normativa y, por tanto, un ilícito fiscalizable por la UAF y que debe prevenirse por parte de las personas jurídicas obligadas.

Esta ley contempla una vigencia inmediata, desde su publicación en el Diario Oficial, excepto en lo que respecta a las modificaciones introducidas a la Ley 20.393 sobre Responsabilidad Penal de las Personas Jurídicas y a la Ley 19.913 que crea la Unidad de Análisis Financiera y sanciona el lavado de activos y financiamiento del terrorismo, las que comenzarán a regir el 20 de Diciembre de 2022.

En este contexto, de parte de HD Compliance recomendamos, **para prevenir estos delitos**:

i. Mantener los Sistemas que se utilizan en la Empresa actualizados,
ii. Contar con el certificado sitio seguro (https) para páginas web,
iii. Supervisar el correcto uso de los correos electrónicos por todo quien tenga acceso a ellos,
iv. Monitorear y alertar el tráfico anormal en las redes de la Empresa,

Nota: El presente documento fue preparado sólo para fines informativos y no debe ser considerado como asesoría legal.

v. Utilizar firewall o cualquier otro mecanismo que garanticen una conexión segura a internet,
vi. Contar con identificadores de códigos maliciosos, por ejemplo, antivirus,
vii. Monitorear constantemente las bases de datos,
viii. Supervisar las transferencias de datos, por ejemplo, estableciendo protocolos para no uso de pendrives o dispositivos periféricos,
ix. Contar con políticas de cambio de contraseñas en que, por ejemplo, se exija un cambio periódico de contraseñas o se utilicen contraseñas complejas,
x. Dependiendo del tamaño de la Empresa, se recomienda contar con equipo especializado para la protección de los sistemas informáticos o contar con un servicio externo que supla este tipo de necesidades.

Para más información, por favor contactar a: Rebeca Zamora y Carlos Frías, socios de HD Compliance, en sus correos rzamora@hdycia.cl y cfrias@hdycia.cl, respectivamente.

Nota: El presente documento fue preparado sólo para fines informativos y no debe ser considerado como asesoría legal.