



Ley N°21.459 Delitos Informáticos.

Value Consultores

El pasado 20 de junio de 2022, se publicó en el Diario Oficial una nueva ley sobre delitos informáticos que deroga Ley N° 19.223, esto en conjunto con la tramitación del proyecto de ley de protección y tratamiento de datos personales, buscan regular las interacciones digitales y actualizar la legislación de acuerdo con los avances tecnológicos de los últimos años y adaptarlos a los convenios internacionales.

La nueva ley de delitos informáticos establece nuevos delitos y agravantes especiales.

I. Nuevos delitos

La ley introduce 8 nuevas figuras penales, además de establecer definiciones de una serie de conceptos que las componen:

- Responsabilidad penal de la empresa.
- Presidio menor en su grado mínimo a presidio mayor en grado mínimo.
- Multas de hasta 30 UTM.

a) Ataque a la integridad de un sistema informático

Toda persona que obstaculice o impide el normal funcionamiento, aunque sea de forma parcial de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos.

b) Acceso ilícito

Toda persona que sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático.

c) Interceptación ilícita

El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio.

d) Ataque a la integridad de los datos informáticos

El que indebidamente altere, dañe o suprima datos informáticos causando un daño grave al titular de estos mismos, será castigado con presidio menor en su grado medio.

e) Falsificación informática

El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos.

f) Receptación de datos informáticos

El que comercialice, transfiera o almacene datos informáticos provenientes de la ejecución de las figuras de las letras b, c y e anteriores

g) Fraude Informático

El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos.

h) Abuso de los dispositivos

El que entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares para la ejecución de los delitos señalados en las letras a, b, c y d.

II. Atenuantes

Se considerará como atenuante la cooperación eficaz que conduzca al esclarecimiento de hechos investigados que sean constitutivos de alguno de los delitos o permita la identificación de sus responsables.

Se entiende por cooperación eficaz el suministro de datos o informaciones precisas, verídicas y comprobables.

III. Agravantes

Se considerará agravante el que cometa delitos abusando de una posición de confianza en la administración de sistema y/o custodio de los datos, como así mismo abusando de la confianza o desconocimiento de niñas, niños o adultos mayores

- **Atenuante:** Cooperación eficaz.
- **Agravante:** abuso de posición de confianza.
- **Hacking ético**



IV. Responsabilidad Penal de la persona jurídica

La ley establece que en el plazo de 6 meses se incorporan estos delitos a la ley de responsabilidad penal de la persona jurídica, por lo que a contar de 20 de diciembre del presente año las personas jurídicas podrán ser condenadas por ellos.

V. Hacking Ético

Una de las grandes novedades de la ley es la introducción del concepto de “hacking ético” que dice relación con personas que son contratadas para hackear un sistema e identificar y reparar posibles vulnerabilidades, con el objeto de prevenir eficazmente la explotación por hackers maliciosos.

En efecto el artículo 16 de la ley, permite expresamente esta actividad siempre y cuando exista autorización expresa del dueño del sistema informático.

Conclusión.

La nueva ley de delitos informáticos implica un cambio significativo en la ciberseguridad, sumado al tratamiento de datos por parte de las empresas que tengan bases de datos o actividad digitales. Recomendamos capacitar a los miembros de su empresa e implementar un sistema de control y protección de datos, con el objeto de prevenir este tipo de delitos e implementar un sistema de cumplimiento que permita eximir a la empresa de responsabilidad penal.

María-Ignacia Barría
Diego Pinto Bravo
Günther Goecke

mbarria@valueconsultores.cl
dpinto@valueconsultores.cl
ggoecke@valueconsultores.cl

