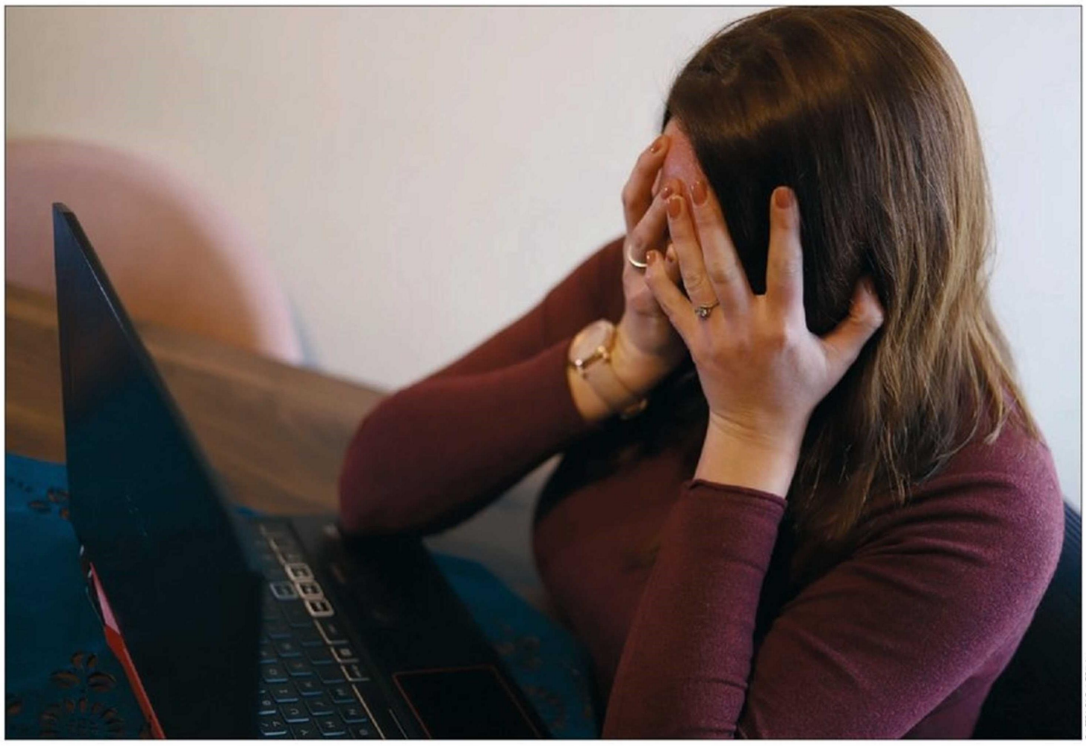
LITORALPRESS

Fecha: 22-06-2022
Medio: Las Últimas Noticias
Supl. : Las Últimas Noticias
Tipo: Actualidad
Título: **Expertos aclaran con ejemplos la nueva ley de delitos informáticos**

Pág. : 12
Cm2: 778,9
VPE: $ 4.283.166

Tiraje: 91.144
Lectoría: 224.906
Favorabilidad: No Definida

La norma anterior sobre delitos informáticos data de 1980.



PATRICIO LEPIN

Robo de contraseñas o información confidencial puede ser castigado incluso con prisión

Expertos aclaran con ejemplos la nueva ley de delitos informáticos

ARIEL LARA

Con su publicación en el Diario Oficial acaba de entrar en vigencia la ley que moderniza la normativa sobre delitos informáticos, definiendo ocho tipos de ilícitos y sus respectivas penas asociadas. A continuación, el detalle y algunos ejemplos de conductas que serán sancionadas.

Pedro Huichalaf, investigador del Centro de Ciberseguridad de la Universidad Mayor, participó de la discusión en el Parlamento como experto invitado. "Esta ley deroga la actual normativa vigente desde 1980, que más que nada sancionaba delitos asociados a equipos (físicos), más que afectación a la información. No estaban consideradas las nuevas formas que tenemos de relacionarnos con la tecnología".

▶Artículo 1°. Ataque a la integridad de un sistema informático. Conducta definida como "obstaculizar o impedir el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos". La pena asociada es presidio menor en sus grados medio a máximo. Hans Poo, consultor informático experto en ciberseguridad, ejemplifica: "Puede ser botarle intencionalmente la conexión de internet a una empresa; o si me meto a su disco duro y borro datos, cambio claves y luego no pueden usarlo; o, peor, un incendio en un data center".

▶Artículo 2. Acceso ilícito. Se dice del que "sin autorización o excediendo (...) medidas tecnológicas de seguridad acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de 11 a 20 unidades tributarias mensuales. Si el acceso fuere realizado con el ánimo de apoderarse de información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimo a medio". Huichalaf comenta que es un "acceso no autorizado a un sistema vulnerando las contraseñas, usando keyloggers (software malicioso que registra las pulsaciones en un teclado), por ejemplo".

Ataque a la integridad de los datos informáticos y receptación de datos figuran entre las figuras punibles.

▶Artículo 3°. Interceptación ilícita. Sanciona al que "capte por medios técnicos datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en sus grados medio a máximo". Huichalaf dice que, por ejemplo, "utilizar un escáner para interceptar el wifi del vecino y descifrar contraseñas podría ser considerado delito".

▶Artículo 4°. Ataque a la integridad de los datos informáticos. Se definió así el "alterar indebidamente, dañar o suprimir datos informáticos". La pena es "presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de los datos". Poo ejemplifica: "Supongamos que me meto a los sistemas de un banco y me hago una transacción de $100 millones, o borro la base de datos de deudas de contribuyentes a Impuestos Internos. La vulneración a la integridad es corromper los datos, alterarlos".

▶Artículo 5°. Falsificación informática. Penaliza a quien "indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo". Si el autor del delito es empleado público, las penas aumentan. "Este es un nuevo delito, que se asocia a los funcionarios públicos, por ejemplo, mediante la modificación maliciosa de documentos oficiales", detalla Huichalaf.

▶Artículo 6°. Receptación de datos informáticos. Castiga a quien, "conociendo el origen de los datos, su origen o no pudiendo menos que conocerlo, comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos". La pena varía, ya que esta conducta se asocia a delitos anteriores. "Una persona, por ejemplo, que descargue la base de datos del Registro Civil (previamente robada) y la utilice con fines lucrativos cometería este ilícito", define Huichalaf.

▶Artículo 7°. Fraude informático. "El que, causando perjuicio a otro, 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". Las penas son proporcionales al perjuicio causado (desde multas a cárcel efectiva). "Acá entra el phishing: cuando alguien intenta engañarte para robar tu información mediante un sitio web o correo electrónico malicioso", explica Huichalaf.

▶Artículo 8°. Abuso de los dispositivos. Esta conducta quedó establecida como quien desarrolle o diseñe dispositivos, programas computacionales, contraseñas, códigos de seguridad "principalmente para la perpetración de delitos". La sanción va desde presidio menor en su grado mínimo y una multa. Lo aclara Poo: "Esto antiguamente era pinchar un cable en la red interna de una empresa o un banco para que me transmitiera los datos hacia donde quiera. Es mal usar dispositivos para capturar tráfico de datos". Complementa Huichalaf: "Acá también entran los ataques de denegación de servicio, que son muchos computadores que se conectan para atacar a un servidor para que caiga".