TECNOLOGIAS DE LA INFORMACION Y CUBERSEGURIDAD

Inacap

Delitos Informáticos

Seguridad de la Información

Inacap

Definición General

Un delito es una acción u omisión que infringe la ley penal de un país y que está penada con una sanción, que puede ser una multa, una pena de prisión u otras medidas legales. En términos generales, se considera delito cualquier comportamiento que esté prohibido por la ley y que cause daño o perjuicio a la sociedad, al orden público o a la persona afectada.

Acción	Omisión
Acción se refiere al comportamiento o conducta que lleva a cabo una persona que infringe la ley. Esta acción puede ser positiva, como hacer algo ilegal (por ejemplo, robar, agredir a alguien), o negativa, como no hacer algo que la ley exige	La falta de acción o la no realización de algo que una persona tiene la obligación legal de hacer. En otras palabras, la omisión es la abstención de actuar cuando se requiere que alguien actúe, y puede ser considerada un delito si la persona tiene el deber legal de intervenir y no lo hace.

Inacap

Acción / Delito

Factor	Descripción
Tipicidad	La acción debe estar claramente definida y prohibida por la ley. En otras palabras, debe ser un comportamiento que esté expresamente descrito como delito en el Código Penal o en leyes relacionadas.
Antijuricidad	La acción debe ser contraria al derecho, es decir, no puede estar justificada por una causa legal, como la legítima defensa o el estado de necesidad.
Culpabilidad	La persona que realiza la acción debe ser responsable de su comportamiento, es decir, debe tener la capacidad de entender que su acción es ilegal y tener la intención o la negligencia de realizarla.
Resultado	En algunos delitos, la acción debe causar un resultado concreto, como en el caso del homicidio, donde la acción de matar debe llevar a la muerte de la víctima. No todos los delitos requieren un resultado, ya que algunos son delitos de mera conducta, como el robo, que solo requiere la acción de sustraer un bien, independientemente de si se causa un daño adicional.

Omisión /Delito

Tipología	Ejemplo
Omisión Propia : La persona tiene el deber de realizar una acción específica y no lo hace. Este tipo de omisión por sí sola puede constituir un delito	- No socorrer a una persona en peligro cuando se tiene la capacidad de hacerlo y se está obligado por la ley a prestar asistencia (como en algunos países, la obligación de ayudar a alguien en un accidente de tráfico). - No cumplir con el deber de alimentar o cuidar a un menor de edad cuando se tiene la responsabilidad legal de hacerlo.
Omisión Impropia: Obligación legal de actuar en virtud de una posición de garante (es decir, alguien que tiene una responsabilidad específica sobre el bienestar de otra persona) y, al no actuar, causa un resultado delictivo. La persona no comete el delito directamente por omitir una acción, pero su omisión da lugar a un daño.	- Un padre que no protege a su hijo de un daño, o un profesor que no impide una agresión en su aula. - El gerente de una empresa que no toma medidas para evitar un accidente de trabajo en un ambiente peligroso.

Delitos Informáticos

Los delitos informáticos son aquellos que se cometen utilizando tecnología informática, como computadoras, internet o dispositivos electrónicos, con el fin de obtener un beneficio ilícito, causar daño o violar los derechos de otras personas. Estos delitos pueden implicar una amplia variedad de actividades ilegales que involucran sistemas informáticos, datos o redes.

Ejemplos delitos informáticos

Hacking:	Acceder ilegalmente a sistemas o redes informáticas para robar información, alterar datos o causar daños.
Phishing	Engañar a las personas para que revelen información confidencial, como contraseñas o datos bancarios, a través de correos electrónicos o sitios web fraudulentos.
Robo de Identidad	Obtener y usar la información personal de otra persona sin su consentimiento para cometer fraudes o delitos.
Virus /malware	Crear y distribuir software malicioso (como virus, troyanos o ransomware) para dañar equipos, robar información o bloquear sistemas.
Fraude cibernético	ealizar actividades fraudulentas en línea, como el uso de tarjetas de crédito robadas o engañar a personas para obtener dinero o bienes de manera ilícita.
Ciberacoso	Utilizar las tecnologías de la información para acosar, intimidar o amenazar a otra persona a través de redes sociales, correos electrónicos u otros medios digitales.
Pirateria de SW	Distribuir o utilizar software de manera ilegal sin licencia, lo que infringe los derechos de autor.
Interceptacion ilegal	Escuchar, ver o copiar comunicaciones privadas sin autorización, como correos electrónicos, mensajes instantáneos o llamadas telefónicas.

Ley 21.459

En Chile, los delitos informáticos son acciones que se cometen contra sistemas informáticos o datos informáticos. La Ley 21459/2022 establece las normas sobre estos delitos.

… Es el delito que comete quien conociendo su origen o no pudiendo menos que conocerlo, comercialice, transfiera o almacene datos informáticos, obtenidos mediante delitos de acceso ilícito, interceptación ilícita y falsificación informática


Ley 21459

ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS, DEROGA LA LEY Nº 19.223 Y MODIFICA OTROS CUERPOS LEGALES CON EL OBJETO DE ADECUARLOS AL CONVENIO DE BUDAPEST

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

Publicación: 20-JUN-2022 | Promulgación: 09-JUN-2022

Fecha Versión: 20-JUN-2022

Inicio Vigencia: 01-DIC-2021

Fin Vigencia: 31-MAR-2020

Url Corta: https://bcn.cl/2r2ng

LEY NÚM. 21.459

ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS, DEROGA LA LEY Nº 19.223 Y MODIFICA OTROS CUERPOS LEGALES CON EL OBJETO DE ADECUARLOS AL CONVENIO DE BUDAPEST

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente

Proyecto de ley:

TÍTULO I
DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES

Artículo 1º.- Ataque a la integridad de un sistema informático. El que obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informatizados, será castigado con la pena de presidio menor en su grado medio a máximo.

Artículo 2º.- Acceso ilícito. El que, sin autorización o superando la autorización que posea y vulnerando las medidas de seguridad establecidas para impedirlo, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

El acceso ilícito cometido con el ánimo de

nacap

Algo sobre lo que significa «Presidio»

La pena de presidio menor, según el sistema penal de Chile, es una pena privativa de libertad que se impone a una persona condenada por un delito. Es una de las penas previstas en el Código Penal chileno y se considera menos grave que el presidio mayor, que es una pena más severa.

El presidio menor se divide en tres grados: grado mínimo, grado medio y grado máximo. Cada grado corresponde a una duración diferente de la pena, y la ley establece los períodos de tiempo que se deben cumplir en prisión, dependiendo de la gravedad del delito cometido

nacap

Algo sobre lo que significa «Presidio menor»

Tipo presidio	Detañe
Presidio menor en su grado mínimo:	Se impone por delitos de menor gravedad. La pena de prisión es de 61 a 540 días (entre 2 meses y 18 meses).
Presidio menor en su grado medio	Se aplica a delitos de mayor gravedad que los del grado mínimo, pero no tan graves como los del grado máximo.La pena de prisión es de 541 días a 3 años.
Presidio menor en su grado máximo:	Es la pena más alta dentro del presidio menor. La pena de prisión es de 3 a 5 años.

El juez determina el grado de la pena dependiendo de las circunstancias del delito, como la intención del delincuente, la gravedad del hecho, los antecedentes penales, y si hay atenuantes o agravantes que puedan modificar la pena.

Algo sobre lo que significa «Presidio Mayor»

Es una pena privativa de libertad más grave que el presidio menor y se aplica a delitos que son considerados más serios o de mayor impacto. Es una pena que se impone a quienes cometen delitos graves, y está definida en el Código Penal chileno.

Presidio mayor → Grado mínimo
Presidio mayor → Grado Medio
Presidio mayor → Grado Máximo

Algo sobre lo que significa «Presidio»

Tipo de presidio mayor	Penas aflictivas
Presidio mayor en su grado mínimo	La pena es de 5 a 10 años de prisión
Presidio mayor en su grado medio	La pena es de **10 a 15 años** de prisión.
Presidio mayor en su grado máximo	La pena es de 15 a 20 años de prisión.

Se aplica principalmente a los delitos más graves, tales como:
Homicidio simple.
Violación (en ciertos casos).
Robos con violencia.Secuestro.
Delitos de gran daño o peligro para la sociedad.

Principales aspectos Ley 21.459

Aspecto	Descripción
Delitos informáticos	La ley incorpora nuevos tipos de delitos informáticos, como la creación, distribución y posesión de software malicioso (virus, malware, etc.), el acceso no autorizado a sistemas informáticos, y la interceptación ilegal de comunicaciones electrónicas.
Sanciones mas severas	Aumenta las penas y sanciones para aquellos que infringen la privacidad de datos personales, incluyendo el uso de información sensible sin consentimiento.
Reformas Código penal	Introduce modificaciones al Código Penal chileno para tipificar más delitos vinculados con la informática, incluyendo la alteración de datos, la falsificación electrónica, y el acceso ilícito a información confidencial.
Enfoque preventivo	La ley también contempla medidas de prevención y protección para evitar el uso indebido de las tecnologías, así como estrategias para fomentar la seguridad digital tanto a nivel individual como organizacional.

Delitos Informáticos/ Integridad de un sistema

Delito	Sanción
Artículo 1°.- Ataque a la integridad de un sistema informático. El que obstaculice o impida 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,	será castigado con la pena de presidio menor en sus grados medio a máximo.

pena privativa de libertad que se impone a una persona condenada por un delito. Es una de las penas previstas en el Código Penal chileno y se considera menos grave que el presidio mayor, que es una pena más severa.

Delitos Informáticos /Acceso ilicito/ejemplo Ley 21459

Artículo 2°.- Acceso ilícito. El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático	será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

Delitos Informáticos/Interceptación ilícita/ ejemplo Ley 21459

Artículo 3°.- 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.
El que, sin contar con la debida autorización, 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.