

TRABAJO PRÁCTICO N° 2

Materia: cibercrimen y delitos informáticos

Profesor: Roque Torres

Aula: N° 24

Apellido: Aguirre

Nombre: Ivan David

Fecha de entrega:04/08/22

cuestionario:

1. ¿Qué es un delito informático?
2. ¿Cuáles son sus características principales?
- 3.Cuál es la clasificación de los Delitos Informáticos según el Convenio sobre la Ciberdelincuencia que se firmó en Budapest? Dar un ejemplo de cada clasificación.
4. ¿Qué es el ciberdelito? Dar un ejemplo.
5. Cuáles son los tipos de ciberdelitos? Elegir uno de los tipos y explicarlo brevemente.

Ley 26.388 - Delitos Informáticos

6. Explicar con sus palabras que dice el artículo 4 de la Ley de Delitos Informáticos.
 7. Si una persona extrae dinero (de un cajero automático o a través de una página web de algún banco publicada en Internet) de la cuenta de otra persona. ¿Es un delito informático? Justificar su respuesta y en caso afirmativo detallar qué artículo de la ley 26.388 abarca.
 8. Defraudar a una persona utilizando alguna técnica informática, es un delito informático? En caso afirmativo, cuál es el artículo de la ley 26.388 que lo tipifica.
 9. Dar un ejemplo de un delito según el artículo 10 de la Ley de Delitos Informáticos.
 10. Explicar con sus palabras cómo quedó modificado el artículo 128 del Código Penal, sobre material de pornografía infantil (ver apunte de Teoría 4)
- Ley 27.411 - Aprobación Convenio sobre Ciberdelincuencia**
11. ¿Cuál es el convenio adoptó la Ley 27.411?
 12. Qué dice el artículo 8 del Convenio sobre Ciberdelincuencia, referente a Estafa Informática. Explique con sus palabras brevemente. Dar un ejemplo. Grooming
 13. ¿Qué es el grooming?
 14. Según la Ley 26.904, como se define el grooming?

RESPUESTAS:

1. Un **delito informático** es un acto dirigido contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos así como también a las acciones ilícitas llevadas a cabo a través de medios digitales (abuso de dichos sistemas, redes y datos). No se utiliza la violencia física, el que comete el delito informático no tiene la intención de hacer el mal.
2. Son delitos difíciles de demostrar ya que es complicado de demostrar las pruebas. Son actos que pueden llevarse a cabo. Se llevan a cabo de forma rápida y sencilla, en varias ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar del hecho.

Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución en sí mismo.

3. **Tipos de delitos informáticos:** “según por el convenio de ciberdelincuencia”

- **delito contra la confidencialidad, la integridad y la disponibilidad de los datos y sistema informáticos:** acceso ilícito a sistemas informáticos
interceptación de datos informáticos
interferencia en el funcionamiento de un sistema informático
abuso de dispositivos que faciliten la comisión de delitos. **Por ejemplo:** robos de identidades, conexiones de redes no autorizadas y en la utilización de spyware y de keylogger.
- **delitos informáticos:** falsificación informática mediante la introducción, borrado o supresión de datos informáticos
fraude informático mediante la introducción, alteración o borrado de datos informáticos o la interferencia en sistemas informáticos.
Por ejemplo: el borrado fraudulento de datos o la corrupción de ficheros (datos).
- **delitos relacionados con el contenido:** producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o un medio de almacenamiento de datos. **por ejemplo:** CD o DVD, pendrive, sitios web.

- **delitos relacionados con infracciones de la propiedad intelectual y derechos afines:** un ejemplo de este grupo de delito es la copia y distribución de programas informáticos o piratería informática.

4. Se consideran **ciberdelitos** los actos criminales que implican en el uso de ordenadores/ computadoras o de internet. Por ejemplo: los crímenes de odio en redes sociales, el telemarketing y el fraude de internet, el robo de identidad y de la cuenta de tarjeta de crédito son considerados como delitos cibernéticos o ciberdelitos.

5. **tipos de ciberdelitos:**

- a) phishing / spoofing
- b) extorsión
- c) hacking
- d) apuestas ilegales
- e) fraude
- f) cyberbullying
- g) pornografía infantil
- h) tráfico de drogas
- i) piratería

- **pornografía infantil:** es poseer o difundir material pornográfico que incluye a personas de menores de edad. También tienen contactos a través de perfiles falsos con fines de uso en persuadir a cualquier menor de edad para que lleve a cabo actividades sexuales.

6. En el **art 4 de la ley 26.388** explica la sanciones penales por el **código penal en el articulado 153** que manifiesta, por abrir o acceder indebidamente a una comunicación electrónicamente o cualquier tipo de medio de comunicación informático (en un despacho telegráfico, telefónico o de cualquier tipo de naturaleza), al apoderarse una carta o otro papel privado aunque no esté cerrado, que se desvíe de su destino en correspondencia o una comunicación electrónica que no le esté dirigida; **Serán reprimidos con prisión de 15 (días) a 6 (meses)**. También habla de una **pena de prisión de 1 (mes) a un 1 (año)**, si los autores además de que comunique a otros y/o publiquen el contenido de la carta (en forma de escrito o de un despacho en comunicación electrónica) y si el hecho lo haga un funcionario público de que abuse de sus funciones además de cumplir con esa pena, se le agrega la inhabilitación especial por el doble del tiempo en condena.

7. Es un **delito informático** ya por el fraude informático mediante la alteración o borrado de datos informáticos y/o la interferencia en sistemas informáticos; Además considero un **ciberdelito** por la utilización del modus operandi (**phishing/ spoofing**) enviar múltiples correos electrónicos o varios mensajes electrónicos comercial con la intención de engañar a los destinatarios, y/o falsificar información del encabezado en varios mensajes de correo electrónico.

Para la **ley 26.388 de Delitos informáticos** embarca en el art 5: donde incorpora el **art 153 bis y art 157 bis del código penal: “protección a la privacidad”** que habla, de una pena de 1(mes) a un 1(año) de prisión cuando el acceso fuere en perjuicio de un sistema o datos informativos de un organismo público estatal o un proveedor de servicios públicos o de servicios financieros.

- Sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, acceder, de cualquier forma, a un banco de datos personales.

8. Si es un **delito informático**, ya que en la misma definición de “**fraude**” (en delitos informáticos) dice: elaboración de cualquier tipo de plan para defraudar, o para la obtención de dinero o bienes mediante pretextos físicos o fraudulentos **usando internet con el fin de ejecutar el plan.**

Para la **ley 26.388 de delitos informáticos** embarcaron en los **artículos 153, 153 bis, 155, 157 y 157 bis**, que hablan de la “**protección a la privacidad**”.

9. El ejemplo más concreto y conciso que puedo distribuir del art 10 de la ley 26.388 delitos informáticos, es en **el sabotaje y/o la piratería informática (donde se divide la acción como hurto de tiempo de máquina, y/o la apropiación o hurto software y datos)** donde el modus operandis de estos dos hechos delictuosos son el fraude cometidos a través mediante la manipulación de una computadora, desde el inicio está la manipulación de datos de entrada, como acto final podemos concluir el daño o modificaciones de programas y/o datos computarizados donde entraría el sabotaje informativo en eliminar, modificar funciones y el acceso no autorizado a servicios y sistemas informáticos.

10. La **modificación del artículo 128** del código penal sobre el material de pornografía infantil es reprimir a los agresores tanto sean por medios que produzcan, financie, ofrezca o comercialice a través de publicaciones o divulgaciones por distintos medios, son penados en condición de encarcelar en una cantidad de años como sentencia por el hecho de estar con materiales de

pornografía infantil de menores de 18 y también se le puede sentenciar con otro tipo de penas y sentenciar por ser menores de 13.

11. En la **ley 27.411** adoptó el convenio sobre el cibercrimen de consejo de Europa, adoptada en la ciudad de Budapest, Hungría que consta de 48 artículos.

12. Quiere decir que las partes se van a adoptar a las medidas que se estiman necesarias para prever como **infracción penal en las estafas informáticas** van a ser tomadas como dolosas (intención) o sin autorización de esos hechos, a través de la introducción, alteraciones o borrados de los datos informáticos y/o atentados al funcionamiento de un sistema informática que provee la intención fraudulenta o delictiva con el sin autorización con objetivo de una remuneración económica para el fraudulento en sí o un tercero.

13. El grooming es la práctica llevada adelante por un adulto, de forma deliberada, que consiste en el acoso sexual hacia un niño o niña donde el modus operandis es el engaño de hacerse pasar por menores o adolescentes a través de internet. La misma puede darse tanto por medio del establecimiento previo de una relación de confianza o no.

14. La ley 26.904 define al **grooming**, uso de comunicaciones electrónicas, telecomunicaciones u otros tipos de tecnologías de transmisión de datos, que contactare a una persona menor edad, con el propósito de cometer cualquier **delito contra la integridad sexual de la misma**.