FASE 3 CONSTRUCCION - SEGURIDAD INFORMATICA

HERNAN DE JESUS QUINTANA

JUAN IGNACIO BOLIVAR

OMAR YOVANY FORERO DIAZ

CARLOS ALBERTO SOSA

TUTOR

GRUPO: 301122_29

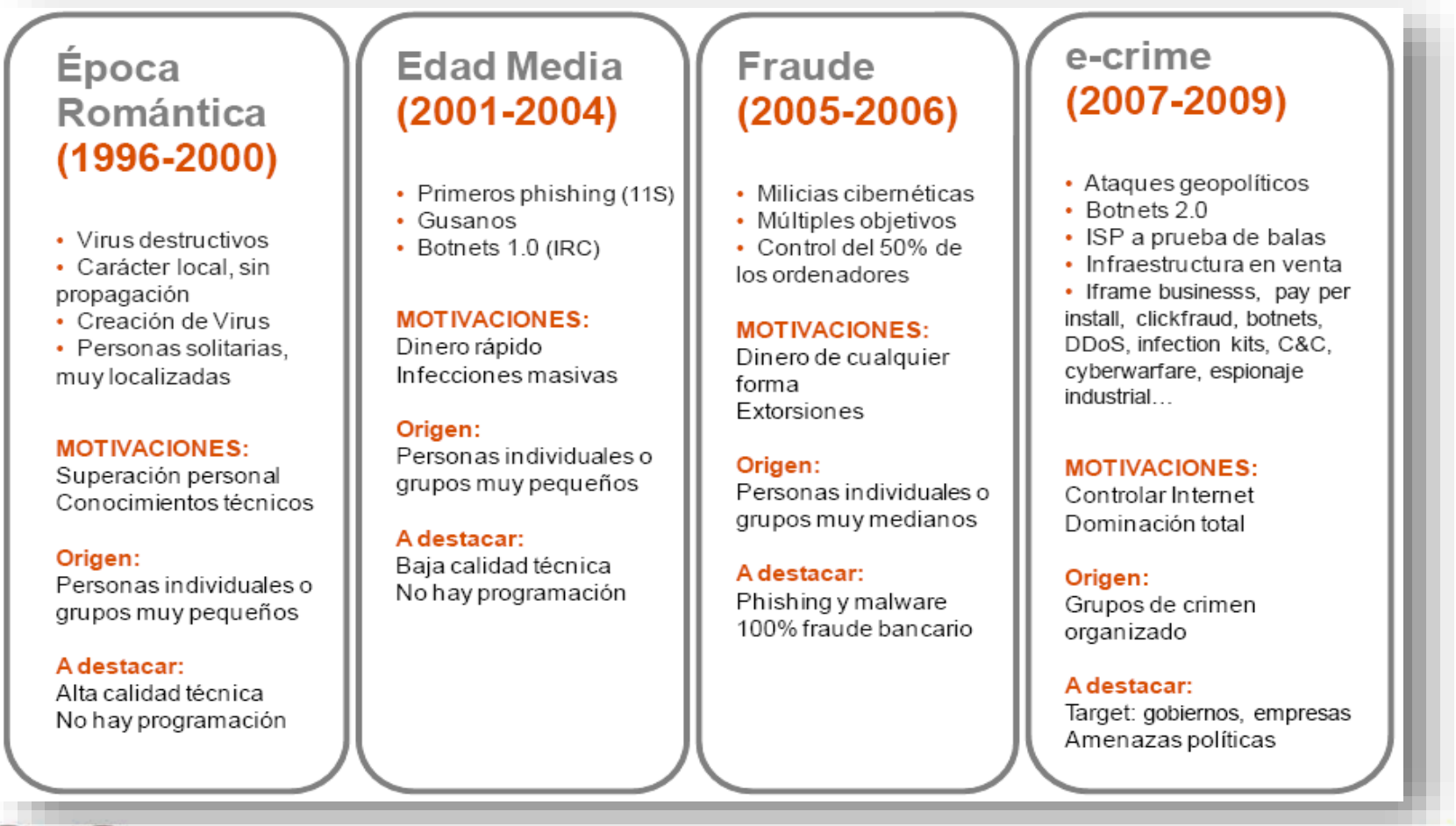
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

DISEÑO DE SITIOS WEB

JUNIO 2019

DELITOS INFORMATICOS Y LEGISLACION

La implantación y desarrollo de las TIC ha creado nuevas posibilidades de delincuencia antes impensables. El delito informático es aquel que se refiere a actividades ilícitas realizadas por medio de ordenadores o de internet.



También incluye delitos tradicionales como fraude, robo, estafa, chantaje, falsificación y malversación de caudales públicos. Los perjuicios ocasionados por este tipo de delitos son superiores a la delincuencia tradicional y también es mucho más difícil descubrir a los culpables.

La Organización de Naciones Unidas (ONU) reconocen los siguientes tipos de delitos informáticos:

- Fraudes cometidos mediante manipulación de ordenadores.
- Manipulación de los datos de entrada.
- Daños o modificaciones de programas o datos computarizados.

Cuando se comete un delito informático, siempre hay dos tipos personas involucradas:

- **Sujeto activo**: aquella persona que comete el delito informático.
- **Sujeto pasivo**: aquella persona que es víctima del delito informático.

CÓDIGO PENAL COLOMBIANO LEY 599 DE 2000

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave.

BIBLIOGRAFÍA

- Junio de 2019 Policía Nacional de Colombia, Normatividad sobre delitos informáticos. Recuperado de: http://e-ducativa.catedu.es/44700165/aula/archivos/repositorio/1000/1063/html/12_delitos_informticos_y_legislacin.html

- Febrero de 2017 Revista Dinero, Imagen Ciber crimen A.P / 123RF. Recuperado de: https://www.dinero.com/edicion-impresa/tecnologia/articulo/las-cifras-que-mueven-el-cibercrimen-a-nivel-global/241593

- Imagen policía cibernética, Recuperado de: https://micarrerauniversitaria.com/c-policia/policia-cibernetica/

GRACIAS