INSTITUTO POLITÉCNICO NACIONAL
SECRETARIA ACADÉMICA
DIRECCIÓN DE EDUCACION MEDIA SUPERIOR
CENTRO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS No. 13
"RICARDO FLORES MAGÓN"

G U Í A

d e e s t u d i o p a r a
presentar ETS de la
UNIDAD DE APRENDIZAJE
ANÁLISIS DE AMENZAS Y DELITOS INFORMÁTICOS
Semestre 2026-2
TURNO MATUTINO

Integrantes de la academia: GODELINDA MELGOZA PONCE

Fecha de Elaboración: __MAYO/26

FORMATO DE LA GUÍA DE ESTUDIO

Área:	Nombre de la Unidad de Aprendizaje:	Nivel/semestre:
Tecnológica	**Análisis de Amenazas y Delitos Informáticos**	**Medio/Cuarto**

Instrucciones generales de la guía:

1. **Para poder presentar el examen el alumno debe conocer:**
   - Identificar los conceptos clave del cibercrimen así como el marco normativo vigente que lo regula
   - Reconocer los ciberataques más comunes y la relación con la legislación vigente
   - Adaptar protocolos para las organizaciones a fin de prevenir y combatir el cibercrimen

La guía no tiene valor.

Presentación:

La Unidad de Aprendizaje de Análisis de Amenazas y Delitos Informáticos pertenece al área de formación profesional del Área Ciencias Sociales y Administrativas del Bachillerato Tecnológico Bivalente del Nivel Medio Superior del Instituto Politécnico Nacional. Se ubica en el cuarto nivel del plan de estudios en la modalidad escolarizada.

Objetivos

Esta Unidad de Aprendizaje contribuye a entender los estándares y normas de la Seguridad de Informática, así como las principales leyes que existen en México para tipificar delitos informáticos y los acuerdos internacionales que los países han firmado y desarrollado con el fin de combatir este problema. Introduce al campo conceptual y procedimental que posibilite al estudiante contar con una visión crítica del marco regulatorio permitiendo frenar el crecimiento exponencial de los delitos informáticos en los últimos años, relacionándola con la "Gestión de la Ciberseguridad".

Justificación

La Unidad de Aprendizaje de "Análisis de Amenazas y Delitos Informáticos" propone fortalecer en el estudiante la construcción de un ser analítico y responsable a fin de que colabore en su entorno, diseñando e innovando técnicas aplicadas a las Tecnologías de Información y Comunicación (TIC) a partir del conocimiento de la normativa ya existente, y así difundirlas y aplicarlas en las organizaciones.

Estructura y contenidos

- **Identifica conceptos clave referentes al cibercrimen**
- **Identifica leyes federales, locales y particulares que sancionan al cibercrimen**
- **Identifica los ciberataques más cometidos en las organizaciones**
- **Relaciona los ciberataques con el tipo de delito cometido de acuerdo con las leyes civiles y penales y la normatividad vigente**
- **Conoce diferentes metodologías para salvaguardar información cibernética**
- **Adecua y propone protocolos y reglamentos internos a favor de evitar el cibercrimen dentro de la organización**

Evaluación

Sin valor.

Materiales para la elaboración de la guía

- Computadora personal, de preferencia Sistema Operativo Windows 8.1 o superior.
- Internet
- Documentación sobre delitos cibernéticos
- (HERNANDEZ, 2014)
- (LLINARES, 2012)
- (CARLOS, 1996)
- (MARCOS, 2017)
  -

Actividades de estudio

1. ¿Cuál de estos no es un cibercrimen?
a. Fraude por correo electrónico e Internet.
b. Robo y venta de datos corporativos.
c. Robo de datos financieros o de la tarjeta de pago.
d. Minar criptomonedas

2. ¿Qué es el Adware?

Este software, se inicia con nuestro equipo y recopila toda la información posible en nuestro ordenador para transmitirla a otro equipo anónimo, afectando a nuestra privacidad, rendimiento de nuestro dispositivo y recursos de red.
a. Malware que secuestra archivos cifrándolos y pide un rescate monetario al usuario para volver a utilizarlos.
b. Estos programas son básicamente publicidad que a menudo se nos instala en nuestros navegadores o incluso como ventanas emergentes, usualmente se instalan junto con la instalación de programas gratuitos. Este tipo de software es menos nocivo para nuestro ordenador, pero si no tenemos cuidado, puede afectar en gran medida a nuestra comodidad y rendimiento de nuestro equipo.
c. Este software, se inicia con nuestro equipo y recopila toda la información posible en nuestro ordenador para transmitirla a otro equipo anónimo, afectando a nuestra privacidad, rendimiento de nuestro dispositivo y recursos de red.

3. Son daños o modificaciones de programas o datos computarizados, excepto:
a. Sabotaje informático
b. Gusanos
c. Piratas Informáticos
d. Bomba lógica o cronológica

4. ¿Que son los Professional criminals?

a. que escriben códigos destinados exclusivamente a dañar otros sistemas.
b. piratas informáticos que siguen los preceptos de la primera generación de hacker
c. crackers con elevados conocimientos y especializados en espionaje industrial y operaciones de inteligencia contra gobiernos, agencias de seguridad nacional, etc
d. capaces de escribir programas pequeños, que utilizan principalmente para alterar páginas web, enviar correos spam, realizar actos vandálicos en el ciberespacio, etc.

5. ¿Que son los White Hat Hackers?

a. se dedican a traspasar los niveles de seguridad de los sistemas informáticos y ofrecer sus servicios como administradores de seguridad. Su finalidad no es delictiva, aunque tampoco es altruista

b. son los encargados de la seguridad de los sistemas informáticos, dedicados a estudiar y fortalecer las brechas de seguridad o errores (bugs) en los mismos. Su actividad es inocua desde una perspectiva criminológica (lo que no necesariamente significa que no sea delictiva formalmente para algunos sistemas de control social formal) y busca básicamente la mejora del sistema.

c. encajan materialmente con el concepto de cibercriminal, puesto que se dedican a vulnerar la seguridad de sistemas, realizar intrusiones no autorizadas e ilegales a sistemas privados con intenciones delictivas: descubrir, revelar, apoderarse o dañar datos. Para ellos, violar un sistema de información y extraer sus secretos, robar la información y venderla fuera es un comportamiento normalizado.

6. ¿Qué es un spammer?

a. puede definirse como la creación y difusión de mensajes no deseados, en su mayoría publicitarios

b. se trata de hackers especializados en la guerra virtual, con el objetivo final de inutilizar la capacidad militar de un oponente. Su cometido es principalmente militar, siendo su tarea principal la de penetrar en los sistemas o redes de otro Estado con la intención de provocar daños, interrupciones o explotaciones de datos.

c. sujeto que compra y registra dominios con el fin de explotarlos económicamente: inversores en nombres de dominio. En muchas ocasiones, estos dominios son adquiridos por el domainer ante determinados sucesos de especial repercusión mediática, utilizando nombres no registrados

d. hackers sigilosos que se infiltran en los sistemas de datos de las grandes empresas para obtener información e intercambiarla por dinero

7. ¿Qué articulo menciona lo siguiente?
Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a

trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Articulo 1610

A. ARTICULO 211 bis 1.-
B. ARTICULO 211 bis 3.
C. Artículo 231. XIV.

8. Los ataques de suplantación de la identidad presentan varias posibilidades, siendo una de las más conocidas la denominada IP Spoofing,

a. Espionaje informatico
b. La técnica del salami
c. Ciberterrorismo
d. Phishing

9. ¿Qué son los viruckers?

a. los creadores de virus informáticos, su especialidad es, por tanto, la fabricación de programas (malware) que permiten la intrusión en otros sistemas informáticos o la destrucción y alteración de datos (daños informáticos).
b. se trata de una especialización en el desarrollo y venta de programas malware,
c. se trata de piratas informáticos especializados en el robo de información dentro del ámbito financiero.
d. se trata de hackers especializados en la guerra virtual, con el objetivo final de inutilizar la capacidad militar de un oponente. Su cometido es principalmente militar, siendo su tarea principal la de penetrar en los sistemas o redes de otro Estado con la intención de provocar daños, interrupciones o explotaciones de datos.

10. ¿De que habla el artículo 211 bis 4?

a. Al que estando autorizado para acceder a sistemas y equipos de informática del estado,
b. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

c. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del estado

Información Adicional

•

Bibliografía Básica

CIBERATAQUES Y RIESGOS

• BECCARIA Alessandro.1997. De los Delitos y las Penas. Santa Fe de Bogotá, Colombia. Temis S.A

• DALLAGLIO Edgardo Jorge.1990. La Responsabilidad Derivada de la Introducción y Propagación del Virus de las Computadoras. en El Derecho.

• FERNÁNDEZ CALVO.1996.El Tratamiento del llamado "Delito Informático" Centro Regional de Extremadura, Mérida.

• FROSINI Vitorio.1988. Informática y Derecho. Bogotá, Colombia. Temis.

•