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 amenazas y delitos Informáticos ----------

TURNO --Vespertino----------

Presidente de academia: Feder la Peña

Fecha de Elaboración: **13 de mayo 20**

Área: Ciberseguridad	Nombre de la Unidad de Aprendizaje: Análisis de amenazas y delitos Informáticos	Nivel/semestre: 4

Instrucciones generales de la guía:

Presentación: 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".

Objetivos La seguridad digital debe formar parte de la cultura de cualquier organización, ya actualmente las TI son fundamentales para todas las áreas dentro de la organización. El análisis de amenazas permite conocer todos los activos relacionados con la información dentro de la organización, identificando amenazas y vulnerabilidades que permitan definir los riesgos reales a los que se expone la información y los sistemas.

Justificación Un análisis de amenazas permite implementar las medidas necesarias que mitigan el impacto inherente a los distintos riesgos, pudiendo incluso llegar a evitar que se produzcan. En todas las organizaciones se deben realizar Análisis de amenazas y delitos Informáticos así como de seguridad, ya que actualmente dependen de la TI para realizar la mayoría de sus actividades, tanto de administración, producción y comunicación.

Estructura y contenidos Estructura y contenidos

En esta unidad de aprendizaje se abordan 3 unidades didácticas

CIBERCRIMEN Y LA APLICACIÓN DE LAS LEYES (MARCO NORMATIVO)

CIBERATAQUES Y RIESGOS.

APLICACIÓN DE PROTOCOLOS

Evaluación Esta guía de estudios bien resuelta, sin faltas de ortografía y completa equivale al 30% de la calificación final

Materiales para la elaboración de la guía Internet

Actividades de estudio

I Evaluación de conocimientos

EJERCICIO I RELACIONA LA RESPUESTA CORRECTA INDICANDO EN EL PARENTESIS LA LETRA CORRECTA

( )	Norma jurídica dictada por el legislador, es decir, un precepto establecido por la autoridad competente, en que se manda o prohíbe algo en consonancia con la justicia, cuyo incumplimiento conlleva a una sanción.	1	LEY
( )	Es la que establece principios por los que deberá regirse la legislación de un país; suele denominarse Constitución. La Constitución es la norma suprema del ordenamiento jurídico, ya que está por encima de cualquier ley..	2	LEY FUNDAMENTAL
( )	Norma de tecnologías de la Información-Técnicas de Seguridad-Código de Buenas Prácticas para el Control de la Seguridad de la información, que reproduce las disposiciones establecidas en la ISO / IEC 27002: 2013 Información Technology-Security Técnicas Código de prácticas para los controles de seguridad de la información	3	NMX-I-27002-NYCE-2015.
( )	Es un término utilizado de forma general para describir a cualquier tipo de software o aplicación maliciosa independientemente de la acción que realiza	4	MALWARE
( )	Consiste en que los ciberdelincuentes introducen malware en los anuncios publicitarios en la red, anuncios que son lo suficientemente llamativos como para que las	5	MALVERTISING

	posibles víctimas pinchen encima para conocer más información sobre el mismo..		
( )	Se define como información y datos de valor para una investigación almacenada, recibida o transmitida por un dispositivo electrónico. Esta evidencia se puede adquirir cuando se confiscan dispositivos electrónicos para su examen.	6	EVIDENCIA DIGITAL
( )	Debe haber sido obtenida y registrada en el lugar de los hechos y debe garantizarse la integridad de los archivos.	7	EVIDENCIA DIGITAL AUTENTICA
( )	Es el procedimiento que permite de manera inequívoca conocer la identidad, integridad y autenticidad de los vestigios o indicios digitales relacionados con un acto delictivo, desde que son encontrados hasta que se aportan al proceso como pruebas.	8	CADENA DE CUSTODIA DIGITAL
( )	Su trabajo es evitar el acceso no autorizado a una red privada y puede implementarse como hardware, software o una combinación de ambos.	9	CORTAFUEGOS
( )	Son una de las mejores formas de evaluar los sistemas de seguridad de la empresa y la seguridad de una infraestructura de TI, ya que intenta aprovechar las vulnerabilidades de forma segura. Estas Vulnerabilidades existen en sistemas operativos, servicios y aplicaciones, configuraciones incorrectas o comportamientos de riesgo del usuario final..	10	TEST DE PENETRACION

II Evaluación de habilidades y destrezas

Ejercicio 1. Sigue al pie de la letra las siguientes instrucciones

1.- Abre la siguiente liga https://www.iebschool.com/blog/herramientas-ciberseguridad-digital-business/

2.- Contesta las siguientes preguntas completas, tal y como están en el artículo:

- ¿Por qué es importante tener herramientas de ciberseguridad?
- ¿Qué es un Firewalls o cortafuegos?
- ¿Qué es Software antivirus?
- Infraestructura de clave pública o PKI
- Servicios MDR (Managed Detection and Response)
- Pentesting
- Formación del personal

3.- La pasas en un documento de Word con el nombre de Herramientas de Ciberseguridad.

4.-El documento a presentar es del siguiente formato:

Texto arial 12

Títulos arial 14

Justificado

Interlineado 1.5

Espaciado anterior 6 puntos, posterior 6 puntos

Márgenes estándar

6.- Revisa automáticamente la ortografía.

Ejercicio 2.- Sigue al pie de la letra las siguientes instrucciones

1.- Abre la liga https://classroom.google.com/c/NTg3MjQ0Nzk1OTA2/m/NTYyOTg2NDQ2MjUy/details

2.- Copia en un documento en Word el texto íntegro con ilustraciones "Ley de Ciberseguridad en México"

3. El formato en Word el mismo del punto anterior

III Evaluación de actitudes y valores.

Creatividad

1. Abre esta liga https://ciberseguridad.com/normativa/latinoamerica/mexico/
2. Utilizando cualquier procesador de textos, en forma creativa reproduce el texto "**MEXICO CIBERSEGURIDAD"**, añadiéndole figuras alusivas al texto

PROBLEMAS PARA AUTOEVALUACIÓN

Desarrolla un ensayo "CIBERDELINCUENCIA UN MAL QUE AFECTA A LA SOCIEDAD ACTUAL".

De la liga https://www.eumed.net/rev/cccss/29/ciberdelincuencia.html

Información adicional

Bibliografía básica Internet

Integrantes de la academia Federico Gutierrez de la Peña

Índice de contenidos

Temario

En esta unidad de aprendizaje se aborda 3 unidades didácticas

I. CIBERCRIMEN Y LA APLICACIÓN DE LAS LEYES (MARCO NORMATIVO)

II. CIBERATAQUES Y RIESGOS.

III. APLICACIÓN DE PROTOCOLOS

Contenido

CIBERCRIMEN Y LA APLICACIÓN DE LAS LEYES (MARCO NORMATIVO)

CIBERATAQUES Y RIESGOS.

APLICACIÓN DE PROTOCOLOS