



Plan Clase

31-526-PO-07-F01

Actividad 1

Unidad de Aprendizaje 1

Distinción de la normatividad del derecho informático.

Resultado de Aprendizaje 1.1

Identifica el marco jurídico del derecho informático relativo al manejo de la información y a la función del usuario, conforme a las leyes, normas y principios mexicanos.

Actividad núm. 1:

Actividad 1. Visita el siguiente link y analiza el video.

https://youtu.be/AYEQI6Z7CNc

Contesta el siguiente cuestionario basado en el video anterior

- ¿Cuál es el propósito del derecho informático?
 Es regular a través de diversas leyes y reglamentos la información y todos sus usos,
- 2. ¿Por qué piensas que el proceso de creación e inserción de leyes informáticas a la vida de una comunidad jurídica es largo y lento?

 Porque deben conocerse si su uso es aplicable, y el verificar y el que autoricen la ley.
- 3. Escribe como han revolucionado las TIC, la vida del ser humano en al menos 3 de los siguientes aspectos:

Científico: Transformando la forma en que se lleva a cabo la investigación, desde la recolección y análisis de datos hasta la comunicación de los resultados.

Comerciales: Lo evoluciono con el comercio electrónico y el surgimiento de nuevas herramientas y plataformas digitales han revolucionado la forma en que las personas compran y venden productos y servicios.

Entretenimiento: Creando diferentes formas y aplicaciones que nos proporcionan juegos, apps de streaming, redes sociales entre más cosas.





Plan Clase

31-526-PO-07-F01

- 4. Enumera los 6 tópicos más importantes que ameritan una regulación especial para ser analizado en la LEGISLACIÓN INFORMÁTICA EN MÉXICO:
 - -Protección de datos personales: La privacidad y seguridad de los datos personales son fundamentales en el mundo digital
 - Ciberseguridad: Con el aumento de amenazas cibernéticas, es importante contar con regulaciones que promuevan prácticas de seguridad robustas para proteger sistemas informáticos
 - Propiedad en línea: La regulación informática debe abordar cuestiones relacionadas con la propiedad intelectual en el ámbito digital, incluyendo la protección de derechos de autor
 - Comercio electrónico: Con el crecimiento del comercio electrónico, es necesario contar con regulaciones que establezcan estándares para las transacciones en línea, la protección del consumidor, la autenticidad de los productos entre más cosas.
 - -Neutralidad: La neutralidad en la red garantiza un acceso igualitario a internet sin discriminación por parte de los proveedores de servicios de internet. La regulación debe proteger este principio y evitar prácticas como el bloqueo.
 - Delitos informáticos y ciberdelitos: La regulación debe abordar la definición de delitos informáticos y ciberdelitos, así como establecer sanciones adecuadas para actividades como el hacking, el fraude en línea, el robo de identidad etc.

5.Define ¿Qué es la tipicidad?

Se refiere a la adecuación de la conducta de un individuo a los elementos que constituyen un delito según lo establecido en la legislación penal.





Plan Clase

31-526-PO-07-F01

6. Realiza un mapa conceptual de los 7 principales delitos informáticos que se muestran en el video.

ACCESO NO AUTORIZADO

EL ROBO DE CREDENCIALES MEDIANTE
PHISHING, KEYLOGGING O LA INTERCEPTACIÓN
DE CREDENCIALES. ADEMÁS, SE INCLUYEN LOS
ATAQUES DE FUERZA BRUTA, DONDE SE
EMPLEAN TÉCNICAS COMO BRUTE FORCE,
DICTIONARY ATTACKS O RAINBOW TABLES
PARA ADIVINAR CONTRASEÑAS.

REPRODUCCION NO AUTORIZADA DE

PROGRAMAS INFORMATICOS

LA PIRATERÍA DE SOFTWARE, QUE IMPLICA LA
DESCARGA Y DISTRIBUCIÓN ILEGAL, ASÍ COMO EL USO
DE KEYGENS, CRACKS O LA DISTRIBUCIÓN DE SERIALES
FALSOS PARA ELUDIR MEDIDAS DE SEGURIDAD.
TAMBIÉN SE MENCIONA LA DISTRIBUCIÓN DE COPIAS
ILEGALES, QUE ABARCA LA COPIA Y DISTRIBUCIÓN DE
SOFTWARE SIN LICENCIA, ASÍ COMO LA VENTA DE
SOFTWARE PIRATA.

INTERVENCION DE CORREO

ELECTRONICO

el phishing, donde se envían correos electrónicos falsificados que parecen provenir de entidades legítimas, con el objetivo de engañar a los usuarios para que revelen información confidencial o realicen acciones no deseadas. También se menciona el spoofing, que implica la falsificación de cabeceras de correo electrónico o la suplantación de direcciones de correo electrónico para engañar a los destinatarios. Estas técnicas son utilizadas para manipular a los usuarios y obtener acceso no autorizado a información sensible o realizar actividades maliciosas.

Fraude mediante la computadora.

Acceso no autorizado.

Destrucción de programas o datos.

Reproducción no autorizada de programas informáticos

Uso no autorizado de programas y datos.

Intervención de correo electrónico.

Obtención de información que pasa por el medio Kniffer.

Conceptos que conforman Marco Jurídico del derecho informático.

FRAUDE MEDIANTE

LA COMPUTADORA

El fraude mediante la computadora involucra el uso indebido de sistemas informáticos para obtener acceso no autorizado, destruir datos, reproducir ilegalmente programas, realizar actividades no autorizadas con programas y datos, intervenir en correos electrónicos para obtener información confidencial y utilizar sniffers para interceptar datos sensibles que pasan a través de redes.

PRINCIPALES DELITOS INFORMATICOS

DESTRUCCION DE

PROGRAMAS Y DATOS

- errores numanos: Los usuarios pueden borrar accidentalmente archivos importantes o desinstalar programas necesarios.
- Fallo de hardware. Los fallos en el hardware, como discos duros defectuosos o errores en la memoria RAM. pueden resultar en la pérdida de datos.
- Ataques cibernéticos: Los virus informáticos, malware y otros tipos de ataques cibernéticos pueden causar la destrucción o corrupción de programas y datos.
- Desastres naturales: Eventos como incendios, inundaciones terremotos, etc., pueden dañar físicamente los dispositivos de almacenamiento y causar la pérdida irreversible de datos.

USO NO AUTORIZADO DE PROGRAMAS Y DATOS

cualquier acción en la que alguien accede,
manipula, o utiliza programas de software o datos
sin tener la autorización legal o permiso del
propietario o responsable de esos programas y
datos. Esto puede implicar diversas actividades,
que van desde el acceso no autorizado a archivos
hasta la copia, modificación o distribución de
software y datos sin permiso.

OBTENCION DE INFORMACION QUE PASA POR EL

MEDIO KNIFFER

El término "kniffer" probablemente es una errata o uno variante de "sniffer". Un sniffer, en el contexto de la informática y las redes, es un programa o dispositivo que se utiliza para capturar y analizar el tráfico de red que pasa a través de un punto específico de la red. Los sniffers pueden utilizarse con diversos propósitos legítimos, como el diagnóstico de problemas de red, la monitorización del tráfico o la seguridad de la red.





Plan Clase

31-526-PO-07-F01

Elabore un trabajo escrito donde interprete:

- · Que es una norma.
- · Que es una ley.
- · Que entiendes por CNDH.
- · Conceptos del derecho informático.
- · Que entiendes por Derecho informático.
- · Conceptualice el marco normativo que rige al mismo y,
- · Asocie dichos elementos al ámbito de la función informática.
- · Autenticación de usuarios.
- · Acceso de usuarios.
- Derecho Civil.
- · Derecho Penal.
- · A qué se refiere la informática jurídica
- · Enlista 6 delitos informáticos que conozcas

6	delitos informáticos que conozcas
	Conceptos que conforman Marco Jurídico del derecho
	Informatico.
0	Que es um norma: Es un principio o regla que regula el
	comportamiento de las personas en una sociedad o grupo
0	Que es una lex: Norma Unidica dictada por el legislador,
	que tiene como fin regular la conducta de los Individuos en la
	Socie dade
0	Que entiendes por CNDH, Constitución Nacional de los
	Derechos Humanos, una institución encargada de promover los
	derechos humanos en Mexico.
0	Conceptos del deresto Informatico: Condunto de normas y
	principios que regular las actividades relacionadas con la
	tecnología de la Información y la comunicación
0	El Marco normativo del desecho Homano: leves, reglamentos Y
	disposiciones que regular el uso de la tecnología y diferentes
	ambitos.
F	Psociemos estos conceptos
0	Autentinación del oscario. Proceso en el así se verifica la Identidad
-	de la passona para permittile el aceso a sistemas
0	Aceso de usuario: Permisos y reiscrepciones que se atorgan a las
H	personas para utilizar sistemas Informáticos.
0	Desecto Civilia se telaciona con contratos electronicos, responsa
H	bilided per dires Informatices
	Desecto peral: Delitos Informaticos como el aceso no autorizado o sistemas, la difunción de virus Informaticos etc.
H	A que se refiere a la Informatica Unidia. Uso de las tecnologías
1	de la información en el ambito del desecho como base de datos
H	Unidica, gestion electronica de expedientes Judiciales.
+	/ / / / / / / / / / / / / / / / / / /
1	a sistemas da a sistemas daños intermetidos, trainde
1	ciberne tia, suplantación de likertidad en linea, pomografica
+	Incaptilen Internet y Ciberacoso.
1	Internitor incure 1 decided





Plan Clase

31-526-PO-07-F01

Actividad 2. Menciona al menos 15 tecnologías de información y comunicación, así como sus cambios más relevantes (características, conductas y fenómenos sociales) de hoy (año 2022) y de hace 10 años (año 2007) que perjudiquen, dañen o pongan en riesgo la integridad de un usuario informático o bien informático. Desarróllalo en una tabla comparativa,

TABLA COMPARATIVA DE TECNOLOGIAS

Tecnología	Cambios Relevantes (2022)	Cambios Relevantes (201
Redes Sociales	Mayor interconexión global, aumento de desinformación y polarización, privacidad comprometida, regulación de contenido.	Explosión de popularidad menos regulación, prime casos de ciberacoso y bullying en línea.
Internet de las Cosas	Mayor conectividad de dispositivos, aumento de riesgos de seguridad y privacidad, preocupaciones sobre el control remoto de dispositivos.	Desarrollo incipiente, me dispositivos conectados, preocupaciones iniciales sobre privacidad y seguridad.
Ciberseguridad	Aumento de ciberataques sofisticados y frecuentes, mayor inversión en protección de datos, tendencias de hacking ético.	Menos concientización, ciberataques menos frecuentes pero significativos, enfoque reactivo en lugar de preventivo.
Inteligencia Artificial	Avances en aprendizaje automático y procesamiento de lenguaje natural, preocupaciones éticas sobre la IA, aplicaciones más integradas en la vida cotidiana.	Desarrollo incipiente, aplicaciones limitadas, menos preocupaciones éticas y regulatorias.
Blockchain	Mayor adopción en finanzas y más allá, seguridad y transparencia mejoradas, preocupaciones sobre el consumo de energía.	Desarrollo inicial, principalmente asociado con criptomonedas, men atención y comprensión pública, menos preocupaciones ambientales.
Big Data	Mayor recopilación y análisis de datos, preocupaciones sobre privacidad y ética, avances en análisis predictivo.	Desarrollo incipiente, me datos disponibles, meno preocupaciones sobre privacidad y ética, enfoqu más descriptivo que predictivo
Realidad Virtual/Aumentad	Mayor adopción en entretenimiento, educación y empresas, preocupaciones sobre adicción y aislamiento.	Tecnología emergente, aplicaciones principalme en juegos, menos atenció preocupaciones sobre impacto social y psicológico.





Plan Clase

31-526-PO-07-F01

TABLA COMPARATIVA DE TECNOLOGIAS

5G	Mayor velocidad y capacidad de datos, habilita Internet de las Cosas a gran escala, preocupaciones sobre la privacidad y la seguridad.	Desarrollo incipiente, menos capacidad de datos y velocidad, menos preocupaciones sobre la privacidad y la seguridad.
Computación en la nube	Mayor adopción en empresas y usuarios, preocupaciones sobre seguridad y privacidad de datos, tendencias de trabajo remoto.	Desarrollo incipiente, menos confianza en la seguridad de la nube, menos aplicaciones y servicios disponibles.
Biometría	Mayor uso en seguridad y autenticación, preocupaciones sobre privacidad y uso indebido de datos biométricos.	Desarrollo incipiente, menos aplicaciones y adopción, menos preocupaciones sobre privacidad y uso indebido de datos biométricos.
Sistemas de reconocimiento facial	Mayor uso en seguridad y vigilancia, preocupaciones sobre privacidad y discriminación.	Tecnología emergente, menos aplicaciones y adopción, menos preocupaciones sobre privacidad y discriminación.
Dispositivos móviles	Mayor poder de procesamiento, más aplicaciones y funciones, preocupaciones sobre adicción digital y seguridad de datos.	Desarrollo de smartphones, menos poder de procesamiento y funcionalidades, menos aplicaciones, menos preocupaciones sobre adicción y seguridad.
Impresión 3D	Mayor uso en la fabricación y la medicina, preocupaciones sobre propiedad intelectual y seguridad.	Desarrollo incipiente, menos aplicaciones y adopción, menos preocupaciones sobre propiedad intelectual y seguridad.
Cryptomonedas	Mayor adopción y legitimación, preocupaciones sobre volatilidad, fraude y lavado de dinero.	Desarrollo inicial, menos adopción y legitimación, menos preocupaciones sobre volatilidad, fraude y lavado de dinero.
Vehículos Autónomos	Avances en tecnología de conducción autónoma, preocupaciones sobre seguridad, privacidad y desplazamiento laboral.	Desarrollo incipiente, menos avances en tecnología, menos preocupaciones sobre seguridad, privacidad y desplazamiento laboral.