



Universidad Autónoma del Estado de México
Centro Universitario UAEM Texcoco

LICENCIATURA EN DERECHO

**UNIDAD DE APRENDIZAJE :
TECNOLOGIAS DE LA INFORMACION Y
LA COMUNICACIÓN**

**UNIDADES : I, IV y V
ELABORADO POR:
VERÓNICA TRUJILLO HURTADO**

**PERIODO:
2019 "A"**

INTRODUCCION

Como una herramienta básica en el ámbito jurídico, la tics en los últimos año han tomado gran fuerza de estudio y es que es relevante esta materia, pues como abogado debemos conocer cuales son los alcances de ciertas acciones o actividades que el área informática nos ofrece así como la seguridad para usarla,; por ello en esta presentación se abracaran los temas referentes a las unidades I, IV y V del temario de nuestra área de aprendizaje.

OBJETIVOS

- El alumno conocerá que son las tics y que es la ofimática
- El alumno conocerá como es que se clasifica la informática jurídica y en que consiste cada vertiente.
- El alumno conocerá sobre la firma electrónica y los principios que la rigen.

GUION EXPLICATIVO

La siguiente presentación muestra a través de explicación y mapas conceptuales información acerca de lo que son las tics, el derecho informática, la informática jurídica, así como todos aquellos elementos que conforman a esta área jurídica como lo son la firma electrónica, la encriptación y el gobierno electrónico.

OFIMÁTICA JURÍDICA

¿QUÉ ES?

- La ofimática jurídica es una de las disciplinas de las ciencias de la información que tiene por objetivo la aplicación de la informática en el derecho.

OBJETO

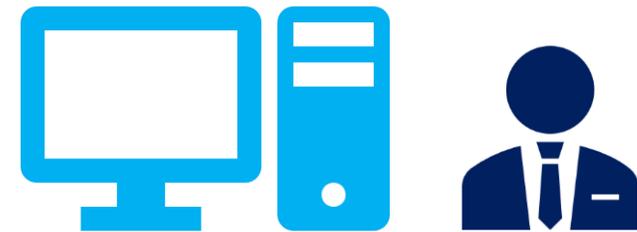
- Esta figura difiere pues en el derecho informático, que es la regulación jurídica de las nuevas tecnologías.

CONCEPTOS

Cibernética: ciencia que estudia los sistemas de comunicación y regulación automática de los seres vivos y los aplica a sistemas electrónicos y mecánicos que se parecen a ellos.

Informática: La informática es el conjunto de conocimientos técnicos que se ocupan del tratamiento automático por medio de computadoras.

Información: Conjunto de organizado de datos procesado que constituyen un mensaje de estado que cambia de estado de conocimiento del sujeto o sistema que reside dicho mensaje.



OBJETIVO DE LAS TICS

TICS

Uso razonado de las posibilidades que nuestras tecnologías ofrecen.

Conocer la relación que existe entre el derecho y la informática.

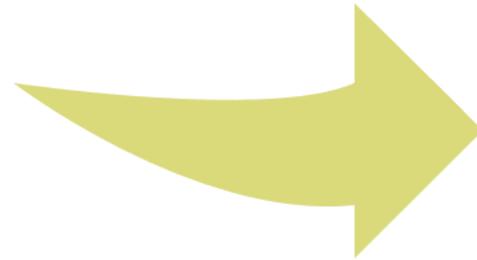
Conocer la regulación jurídica y la interrelación entre las nuevas tecnologías de la información.



DERECHO INFORMÁTICO

¿Qué es?

Es una rama de las ciencias jurídicas que estudia las consecuencias legales de uso de las tecnologías de información tanto de software como de hardware



Surge con la finalidad de regular el comportamiento en un ámbito tecnológico, en donde actualmente el derecho informático aun no es un derecho específico

INFORMÁTICA JURÍDICA

Informática jurídica documental

Es una rama
auxiliar del
derecho debido
al creciente
avance
tecnológico

Informática jurídica de control/gestión

Informática jurídica meta documental

INFORMÁTICA JURÍDICA DOCUMENTAL

¿QUÉ ES?

- Consiste en el empleo de los llamados sistemas de información y documentación jurídica estos se integran por una legislación, la doctrina y la jurisprudencia.

PRINCIPIO

- Son el fundamento principal de banco de datos jurídicos supone el tratamiento y la recuperación de información jurídica por medio de los ordenadores.

INFORMÁTICA JURISCA DE CONTROL/GESTIÓN

¿QUÉ ES?

- Tiene como objeto el tratamiento de textos jurídicos mediante el uso de procesadores de palabra y por otra parte las experiencias obtenidas en materia de optimización de registros públicos.

PRINCIPIO

- Recibe transmite comunicaciones de cualquier tipo de leer y escribir textos, de formar, organizar y actualizar archivos y registros, exigir y recibir pagos estipular condiciones y controlar su cumplimiento.

INFORMÁTICA META DOCUMENTAL

¿QUÉ ES?

- Es aquella rama que tiene mayor grado de complejidad, por cuanto no se agota en recopilación de textos documentarios en la realización de documentos jurídicos o control de asuntos.

PRINCIPIO

- Se extiende en el campo decisonal, educativo, investigativo entre otras, en ella figura la IA(Inteligencia Artificial) dando oportunidad de crear sistemas mas expertos o profesionales.

CIBERGOBIERNO Y LAS TICS

- ¿QUE ES?
- Es un método electrónico que facilita la forma de gobierno empleando las TICS en conjunto con los conocimientos de los procesos de gobierno, siendo así una forma más accesible tanto del pueblo como para los gobiernos de entablar una comunicación.
- ALGUNOS EJEMPLOS DEL GOBIERNO ELECTRÓNICO SON :
 - El uso de las TICS y particularmente el Internet.
 - El uso de las TICS en todos los ámbitos de la organización gubernamental.
 - La continua optimización de la prestación de servicios.
 - Transformación de las relaciones internas y externas a través de la tecnología y los nuevos medios de comunicación.



EL GOBIERNO DIGITAL



EL GOBIERNO HACE
USO DE
LAS TICS

PROCESAR
INFORMACION

DIGITALIZAR
DOCUMENTOS

AUTOMATIZAR
TRAMITES

La incorporación de tecnología no va a reemplazar las buenas políticas ni la correcta gestión, pero puede actuar como medio para optimizar los servicios del Estado, profundizar la participación ciudadana y transparentar la función pública.

se traduce en la implementación de portales **de información para resolver trámites**

ESTRATEGIAS DEL ESTADO EN CONJUNTO DE LAS TICS

FIRMA
ELECTRONICA

PLATAFORMAS
DEL GOBIERNO

EXPEDIENTES
ELECTRONICOS

DIGITALIZACIÓN
DE DOCUMENTOS



Instituto de Transparencia, Acceso a la Información Pública y
Protección de Datos Personales del Estado de México y Municipios



LA FIRMA ELECTRONICA

- ¿QUE ES?
 - Es el conjunto de datos que se adjuntan en un mensaje electrónico ,cuyo propósito es identificar al firmante como autor de la misma de manera única ,como si se tratara de una firma manuscrita.
 - Por su característica brinda seguridad a las transacciones electrónicas entre usuarios, ya que su uso permite identificar al firmante ,además de verificar que no se ha modificado el mensaje.
- REQUISITOS
 - Copia certificada y fotocopia del acta de nacimiento
 - Original y fotocopia de la identificación oficial
 - Original y fotocopia de un comprobante de domicilio fiscal
 - recibo de luz, agua, telefónico
 - Solicitud de certificado de Fea por duplicado y firmado
 - Disco con archivo de requerimiento

AGENTES CERTIFICADORES Y CERTIFICADO DIGITAL

- AGENTES CERTIFICADORES
- Es el encargado de emitir y revocar los certificados digitales de los firmantes y prestar los servicios relacionados con la firma electrónica
- CERTIFICADO DIGITAL
- Un certificado digital o certificado electrónico consiste en un archivo informático que ha sido generado y firmado electrónicamente a través de un prestador de servicios de certificación debidamente reconocido de tal manera que relaciona a una persona o entidad con este documento y puede ser utilizado como identificación digital y para la generación de la firma electrónica



PRINCIPIOS DE LA FIRMA ELECTRONICA AVANZADA

- **AUTENTIFICACION:** La autenticación de usuarios jurídicamente ,la identificación se sustenta en el conocimiento directo de una persona a través de sus características
- **INTEGRIDAD:** Se compone de idoneidad para garantizar que el texto recibido no haya recibido alteración alguna
- **NO REPUDIO :** Es la garantía de que no puede ser negados mensajes en comunicación telepática existen dos tipos de repudio en origen de garantizar al receptor que el mensaje ha sido enviado ,el no repudio en el destino ,que garantiza al emisor que su comunicación ha sido recibido no pudiendo negar el receptor tal comunicación
- **DE CONFIDENCIALIDAD:** Verifica que el mensaje no ha sido modificado ,aun que se pudiera de cierta forma encripta el texto dos veces en combinación con las claves públicas del receptor como emisor

EL ACCESO A LA INFORMACION PUBLICA

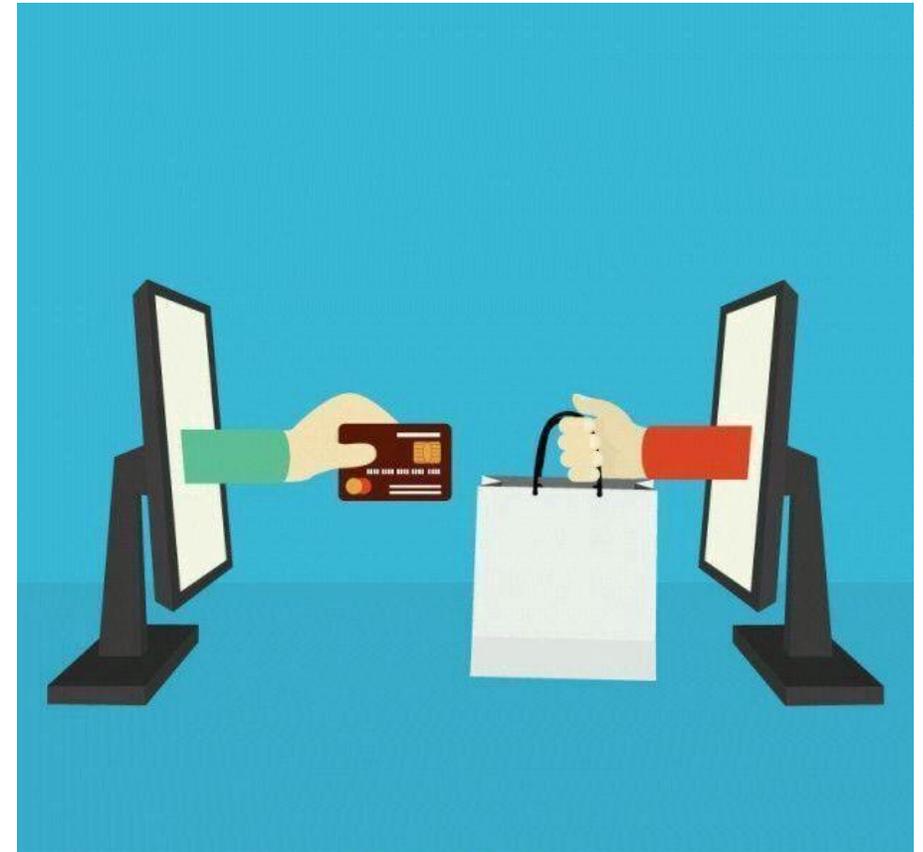
- Artículo 6.
- La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.
- Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión. Para áreas adicionado DOF I I-a6-2013 El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet.
- Para tales efectos. el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.



EL COMERCIO ELECTRÓNICO

El comercio electrónico, también conocido como e-commerce (electronic commerce en inglés) o bien comercio por Internet o comercio en línea, consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como redes sociales y otras páginas web.

Originalmente, el término se aplicaba a la realización de transacciones mediante medios electrónicos tales como el Intercambio electrónico de datos; sin embargo con el advenimiento de la Internet y de la World Wide Web, a mediados de la década de 1990 comenzó a referirse principalmente a la venta de bienes y servicios a través de Internet, usando como forma de pago medios electrónicos tales como las tarjetas de crédito.



COMERCIO ELECTRÓNICO VENTAJAS

Mejoras en la distribución: Ofrece a los proveedores acercarse mas a la industria de lo digital como ejemplo podemos observar la venta de libros digitales, servicio de información o productos digitales.

Beneficios operacionales: El uso en la web reduce errores, tiempo y sobre costos al acceder de manera interactiva a las bases de datos de operaciones de oportunidades de ofertas.

Comunicación comercial vía electrónica: La mayoría de empresas usa la web para informar a los clientes sobre la compañía aparte de productos o servicios tanto como de comunicaciones con otras empresas como de clientes.

Facilidad de fidelizar clientes: Mediante la aplicación de protocolos y estrategias de comunicación efectivas que le permitan al usuario final del portal web plantear inquietudes, levantar requerimientos o simplemente hacer comentarios.

CARACTERÍSTICAS

Ubicuidad: la tecnología de internet o web está disponible en todos lados, en el trabajo, en el hogar y en cualquier otro lado a través de los dispositivos móviles, en cualquier momento, el mercado se extiende más allá de los límites tradicionales y se elimina de una ubicación temporal y geográfica.

Alcance global: la tecnología se extiende más allá de los límites nacionales, alrededor de la tierra. Se habilita el comercio a través de los límites culturales y nacionales sin problemas ni modificaciones. El Marketspace incluye potencialmente miles de millones de clientes y millones de negocios en todo el mundo.

Estándares universales: hay un conjunto de estándares de tecnología, a saber, estándares de internet. Hay un conjunto de estándares de medios técnicos en todo el mundo.

Interactividad: la tecnología funciona a través de la interacción con el usuario, los consumidores entablan un diálogo que ajusta en forma dinámica la experiencia para el individuo, y hace del consumidor un copartícipe en el proceso de entrega de bienes en el mercado.

LA WEB

Actualmente podemos dividir la Web por niveles. A continuación se explica de manera breve lo que podrás encontrar en cada uno de ellos.

Nivel 0:

Web común El más superficial de todos, dominando por un pequeño número de páginas que todos conocemos y que actualmente dominan el mundo internauta, tales son Google, Youtube, el mundo Yahoo!, Wikipedia, Redes sociales y similares.

Nivel 1:

Web Superficial: Aquí se encuentran web un poco menos conocidas pero de fácil acceso. Son en su mayoría foros, páginas pornográficas y pequeñas páginas independientes de interés no tan común como en el nivel anterior.(4chan, Reedit y parecidos)

Nivel 2:

Bergie Web:Está compuesto por dominios web aún menos conocidas y por los buscadores independientes tales como lo son Ares y Emule. El material que se puede obtener en este nivel es de moralidad dudosa y no apto para estómagos débiles. El morbo suele ser un tema recurrente.

LA WEB

- Hasta aquí hemos tocado solo la parte superficial del ciber-mundo. es a partir de aquí donde está el verdadero peligro Es ahora cuando se da el primer paso dentro de Deep Web.
- **Nivel 3:**
- Deep Web d'abord : A partir de aquí las cosas cambian radicalmente las páginas que se rigen en este oscuro mundo suelen tener dominios compuestos por caracteres dejados caer de manera totalmente aleatoria. En ellas no hay publicidad, ni color y lo mas significativo es que no se relacionan entre ellas como las paginas superficiales, de hecho, ni siquiera aparecen en buscadores como Google, ni aunque copies el link de la página completa e intentes buscarlo. Los URL no terminan con .com o .org, sino con la terminación .onion
- **Nivel 4:**
- Charter Web: Los niveles anteriores eran peligrosos, pero con un proxy(aclaración mas adelante) y un buen antivirus era suficiente, pero aquí no. El cuarto nivel y lo que está por delante están plagados de hackers. Y por hackers no me refiero a chiquillos tontos cuyo único pasatiempo es infectar computadoras, me refiero a verdaderos piratas informáticos, lo mejor de entre lo mejor cuando a robo y malversación de datos se refiere.

LA WEB

- **Nivel 5:**

- Marianas Web: Su nombre se debe a la Fosa de las Marianas en el océano Pacífico, el lugar más profundo del mar en sí. Hay muy poca información sobre este nivel. Se dice que aquí se exponen los secretos militares y de estado más impactantes e importantes de todos y donde se aprueban estos mismos y donde se controla su progreso. También se cree que la entidad que realmente domina el mundo intercambia información entre sus contra partes por aquí. En este nivel se necesitan algoritmos que no se sabe con certeza si existen, además de computadoras que solo posee el gobierno.

- **Nivel 6:**

- The Fog: Aquí los hackers que logran entrar utilizan la computación cuántica para poder superar la encriptación. Es muy confuso en cuanto a lo que realmente está contenida en este nivel porque no hay pruebas concretas que alguien haya encontrado, pero creo que la computación cuántica se requiere para navegar por las cantidades masivas de datos en este nivel y por el grado y complejo nivel de seguridad de los datos transmitidos allí.

LA WEB

- **Nivel 7:**

Virus Soup: Este nivel es al parecer el de los "jugadores grandes" . Está lleno de un montón de códigos, para tratar de evitar que la gente 'avanzada' acceda a capas cada vez más profundas. En este nivel, todo el mundo está luchando para mantener a otros por fuera de él, gracias a el valor de los sistemas manejados y la lucha por el poder que este ofrece. La mejor manera de describir el nivel 7, sería una zona de guerra. Donde cada hombre trabaja para sí mismo explotando además las bondades que brinda este nivel(mayor ilegalidad, casi indetectables para muchos gobiernos) e intentando llegar al nivel 8 y evitando que otras personas para llegar allí.

- **Nivel 8:**

The Primarch System o Sistema Primario: En alusión a este nivel se especula que es el control primario del mismo Internet. Se dice que accediendo a este nivel se maneja a su antojo la web. Aunque es imposible para nuestras computadoras de romper estos códigos y encriptaciones.

LOS DELITOS INFORMATICOS Y EL CODIGO PENAL

- Delito informático, delito cibernético o ciberdelito es toda aquella acción antijurídica que se realiza en el espacio digital o de internet. Ante el extendido uso y utilización de internet en todas las esferas de la vida (economía, cultura, industria, ciencia, educación, información, comunicación etc) y el creciente número de usuarios, la delincuencia también se ha expandido a esta dimensión. Gracias al anonimato y a la información personal que se guarda en internet, los delincuentes han ampliado espectacularmente su campo de acción y los delitos y amenazas a la seguridad se han incrementado exponencialmente.
- Además de los ataques que tienen como objetivo destruir y dañar activos, sistemas de información u otros sistemas de computadoras, utilizando medios electrónicos y/o redes de Internet, se producen nuevos delitos contra la identidad, la propiedad y la seguridad de las personas, empresas e instituciones. Existen también otras conductas criminales que aunque no pueden considerarse como delito, se definen como ciberataques o abusos informáticos y forman parte de la criminalidad informática. La criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, son llevados a cabo utilizando un elemento informático

LOS DELITOS INFORMATICOS Y EL CODIGO PENAL

CODIGO PENAL FEDERAL

- El artículo 336 del Nuevo Código Penal del Distrito Federal, 23 relativo a la Producción, Impresión, Enajenación, Distribución, Alteración o Falsificación de Títulos al Portador, Documentos de Crédito Públicos o Vales de Canje, dispone que se impondrán de tres a nueve años de prisión y de cien a cinco mil días multa al que, sin consentimiento de quien esté facultado para ello, altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios (fracción IV); acceda a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo (fracción V); adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída, de esta forma (fracción VI); y a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios, o de los titulares de dichos instrumentos o documentos. (fracción VII).

LOS DELITOS INFORMATICOS Y EL CODIGO PENAL

CODIGO PENAL ESTATAL

- El artículo 174 del Código Penal del Estado de México,²⁴ relativo a la Falsificación y Utilización Indebida de Títulos al Portador, Documentos de Crédito Público y Documentos Relativos al Crédito, prevé que se impondrán de cuatro a diez años de prisión y de ciento cincuenta a quinientos días de salario mínimo de multa al que altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios (fracción IV); y a quien acceda indebidamente a los equipos de electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo (fracción V). No obstante lo anterior, se tiene prevista la imposición de las mismas penas, a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios.

DELITOS INFORMATICOS Y SANCIONES A ESTOS

- Artículo 217. Comete delito informatico, la persona que dolosamente y sin derecho:
- I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el proposito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o informacion; o
- li. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte logico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.
- Al responsable de delito informatico se le impondra una pena de seis meses a dos años de prision y de noventa a trescientos dias multa.



¿CUÁL ES LA DIFERENCIA ENTRE UN HACKER Y UN CRACKER?

Hacker

El término hacker se asocia comúnmente con ciberdelincuentes, pero ¿realmente todos los hackers realizan actividades ilícitas? Si consultamos su significado en la Real Academia Española (RAE) aún es definido como un pirata informático.

No obstante, autoridades en materia de ciberseguridad afirman que su segunda definición: persona experta en el manejo de computadores, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora, es la más acertada de todas.

Cracker

- Por lo que la palabra correcta para definir a la persona que viola un sistema informático es cracker, quien es el encargado de usar sus conocimientos informáticos produciendo un daño a la red que ha ingresado.

Aunque tanto un cracker como un hacker pueden tener los mismos conocimientos, la diferencia primordial entre ambos - como lo afirma David Pereira, CEO de Secpro-, “es que un hacker normalmente ataca una estructura con autorización del dueño de la infraestructura, mientras que un cracker no, no tiene autorización en absoluto de nadie para hacer lo que hace y normalmente tiene motivos maliciosos, es decir, robarte información, secuestrarla para luego pedir rescate”.

BIBLIOGRAFIA



BIBLIOGRAFIA

- Pozo, L, (1992) Informática en Derecho. México. Trillas.
- Rojas, A, (2000). El uso de Internet en el Derecho. México. Oxford.
- Tellez, V. (1996) Derecho Informático. México. Mc Graw Hill
- <https://www.edomex.gob.mx>
- <https://www.scjn.gob.mx/>
- <https://consultas.curp.gob.mx/>