



UNIREMINGTON[®]
CORPORACIÓN UNIVERSITARIA REMINGTON
RES. 2661 MEN JUNIO 21 DE 1996

DERECHO INFORMÁTICO
ESPECIALIZACIÓN EN GERENCIA INFORMÁTICA
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA

Vicerrectoría de Educación a Distancia y virtual

2016



El módulo de estudio de la asignatura Derecho Informático es propiedad de la Corporación Universitaria Remington. Las imágenes fueron tomadas de diferentes fuentes que se relacionan en los derechos de autor y las citas en la bibliografía. El contenido del módulo está protegido por las leyes de derechos de autor que rigen al país.

Este material tiene fines educativos y no puede usarse con propósitos económicos o comerciales.

AUTOR

Yolfaris Naidit Fuertes Arroyo

Ingeniera de Sistemas, Magíster en Educación

Nota: el autor certificó (de manera verbal o escrita) No haber incurrido en fraude científico, plagio o vicios de autoría; en caso contrario eximió de toda responsabilidad a la Corporación Universitaria Remington, y se declaró como el único responsable.

RESPONSABLES

Jorge Mauricio Sepúlveda Castaño

Decano de la Facultad de Ciencias Básicas e Ingeniería

jsepulveda@uniremington.edu.co

Eduardo Alfredo Castillo Builes

Vicerrector modalidad distancia y virtual

ecastillo@uniremington.edu.co

Francisco Javier Álvarez Gómez

Coordinador CUR-Virtual

falvarez@uniremington.edu.co

GRUPO DE APOYO

Personal de la Unidad CUR-Virtual

EDICIÓN Y MONTAJE

Primera versión. Febrero de 2011.

Segunda versión. Marzo de 2012

Tercera versión. diciembre de 2015

Cuarta Versión. 2016

Derechos Reservados



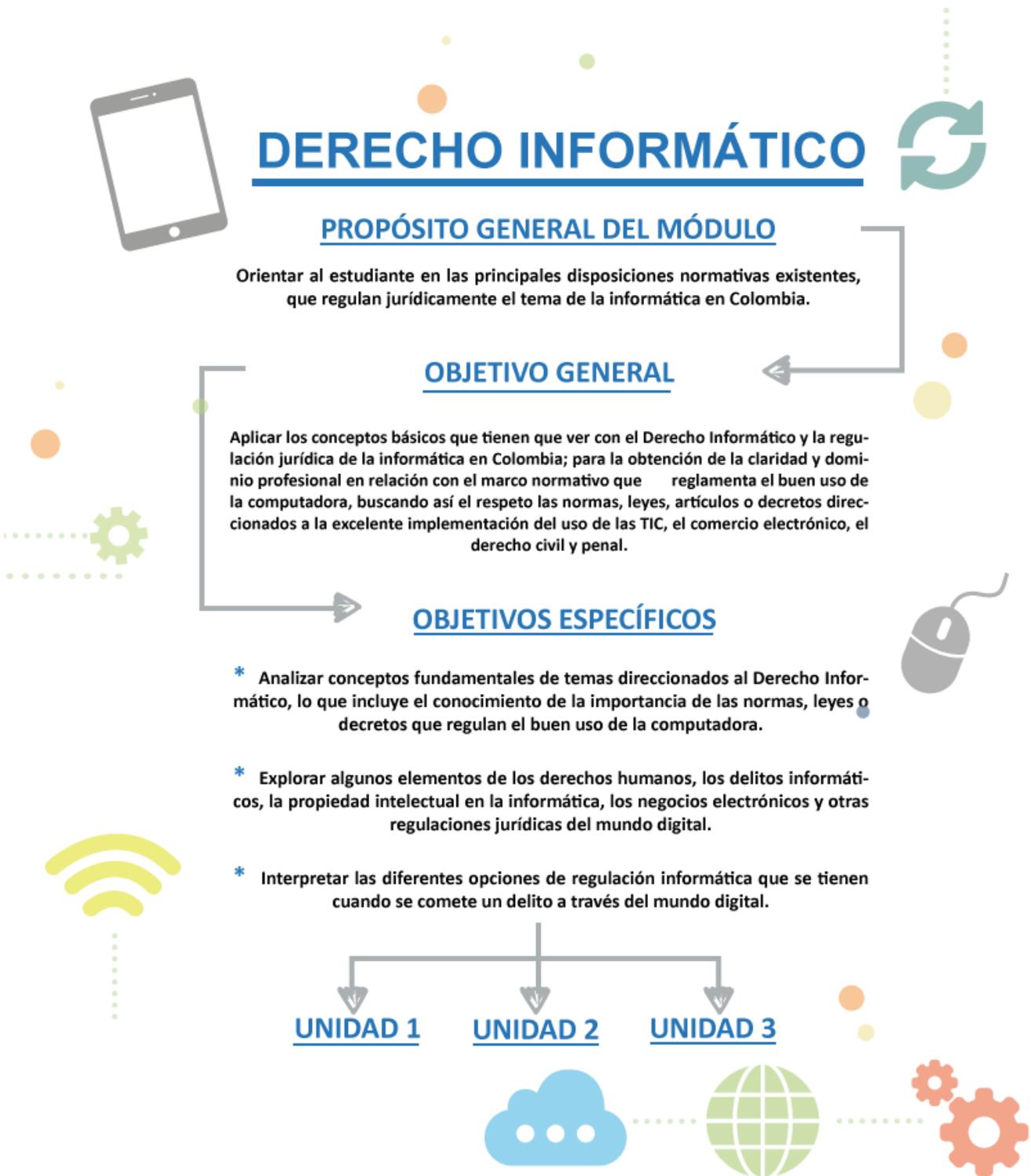
Esta obra es publicada bajo la licencia Creative Commons.
Reconocimiento-No Comercial-Compartir Igual 2.5 Colombia.

TABLA DE CONTENIDO

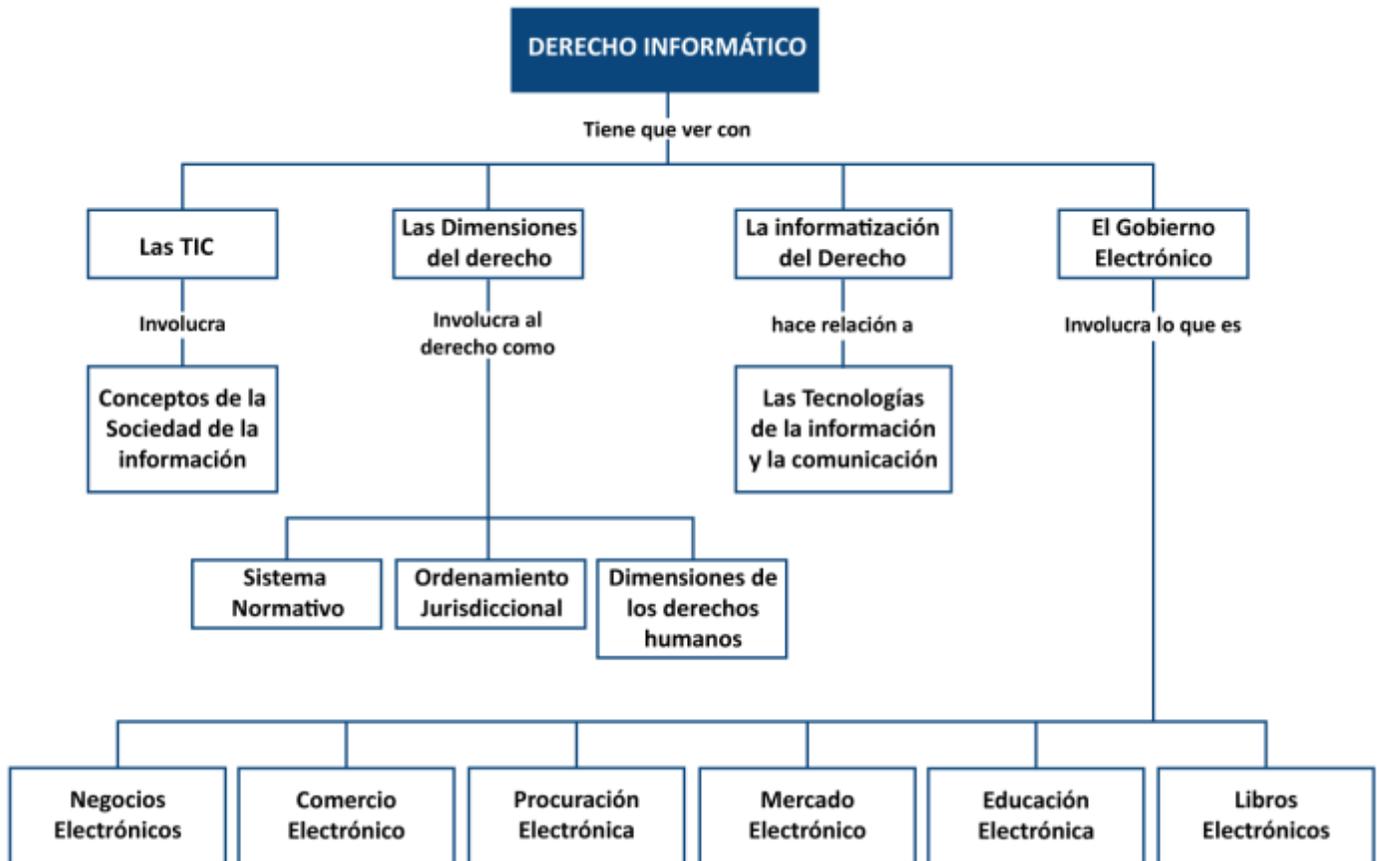
	Pág.
1 MAPA DE LA ASIGNATURA	5
2 UNIDAD 1: NOCIONES Y CONCEPTOS.....	6
2.1 TEMA 1 PERSPECTIVAS O DIMENSIONES DEL DERECHO	8
2.2 TEMA 2 INFORMATIZACIÓN DEL DERECHO.....	13
2.3 TEMA 3 GOBIERNO ELECTRÓNICO	18
2.3.1 EJERCICIO DE APRENDIZAJE UNIDAD1 TEMA 2.1	22
2.3.2 EJERCICIO DE APRENDIZAJE UNIDAD1 TEMA 2.2	24
2.3.3 EJERCICIO DE APRENDIZAJE UNIDAD1 TEMA 2.3	25
3 UNIDAD 2: INFORMÁTICA JURÍDICA – DERECHO INFORMÁTICO	27
3.1 TEMA 1 ESPECIFICACIONES	27
3.2 TEMA 2 DELITOS INFORMÁTICOS DEFINIDOS EN LA LEY PENAL COLOMBIANA	31
3.3 TEMA 3 ANÁLISIS DE PROBLEMAS.....	36
3.3.1 EJERCICIO DE APRENDIZAJE UNIDAD 2 TEMA 3.1	37
3.3.2 EJERCICIO DE APRENDIZAJE UNIDAD 2 TEMA 3.2	38
3.3.3 EJERCICIO DE APRENDIZAJE UNIDAD 2 TEMA 3.3	39
4 UNIDAD3: REGULACIONES JURÍDICAS DEL SOFTWARE Y DEL MUNDO DE LOS NEGOCIOS ELECTRÓNICOS	41
4.1 TEMA 1 NORMATIVIDAD	41
4.2 TEMA 2 INFORMÁTICA FORENSE	44
4.3 TEMA 3 PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES.....	47
4.3.1 EJERCICIO DE APRENDIZAJE UNIDAD 3 TEMA 4.1	50
4.3.2 EJERCICIO DE APRENDIZAJE UNIDAD 3 TEMA 4.2	51
4.3.3 EJERCICIO DE APRENDIZAJE UNIDAD 3 TEMA 4.3	52

5	PISTAS DE APRENDIZAJE.....	54
6	GLOSARIO.....	55
7	BIBLIOGRAFÍA.....	56

1 MAPA DE LA ASIGNATURA



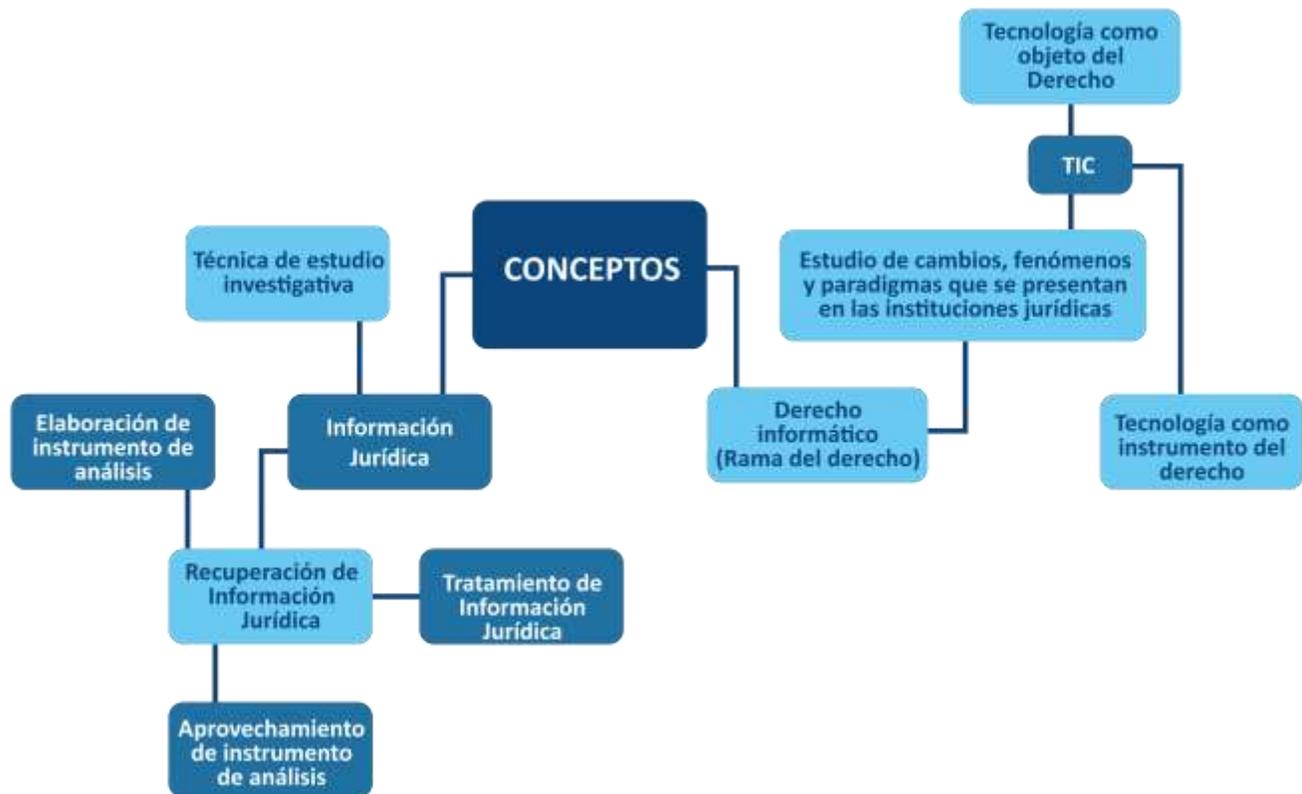
2 UNIDAD 1: NOCIONES Y CONCEPTOS



NOCIONES Y CONCEPTOS

El derecho puede ser entendido al menos en tres dimensiones o perspectivas: **como sistema normativo**, **como ordenamiento jurisdiccional**, y **desde los “derechos”**.

Figura 1. Nociones y conceptos Derecho Informático – Informática Jurídica



Fuente: Elaboración propia

Según Tato (2010), el término Derecho Informático se define como:

“el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación de sujetos en el ámbito de la informática y sus derivaciones, especialmente en el área denominada "tecnología de la información".

A partir de los conceptos de esta tecnología y de la sociedad del de la información surge la concepción del Derecho Informático.

Por su lado **EcuRed (2015)**, define el Derecho informático como “la ciencia y rama autónoma del Derecho que abarca el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en aspectos como la regulación del medio informático en su expansión y desarrollo, y la aplicación idónea de los instrumentos informáticos”.

Tecnología de la información y la comunicación

De acuerdo a Cobo (2009), la vida moderna del siglo XXI requiere del uso de una serie de dispositivos que ayudan de forma eficiente al intercambio de información y por supuesto a la comunicación entre los individuos. “Casi en todo orden de cosas el acceso a estos dispositivos parece esencial, ya no sólo para permitir la interacción a distancia entre individuos, sino que también para facilitar el comercio, la ciencia, el entretenimiento, la educación, y un sinnúmero de actividades”, las cuales están relacionadas con las exigencias del avance de esta nueva era.

“ El Derecho informático surgió como una necesidad de dar soluciones a las innumerables dificultades que día a día se presentan por la evolución de las Tecnologías de la Información y Comunicación. ”

Sociedad de la información

Según Torres (2005), “**El concepto de "sociedad de la información"**, nacido bajo los preceptos de la globalización neoliberal, sobreentiende que, en adelante, serán las “**revoluciones tecnológicas**”, las que determinen el rumbo del desarrollo; los conflictos sociales serían cosa del pasado”.

Las tecnologías de la información y la comunicación han traído una serie de cambios a la nueva era del conocimiento; es tanto el aporte que han proporcionado a la humanidad, que las personas las han convertido en una herramienta esencial al momento de realizar tareas o actividades que involucren proceso digital.

2.1 TEMA 1 PERSPECTIVAS O DIMENSIONES DEL DERECHO

Se presentan diversos conceptos de autores acerca de la sociedad tecnológica y el mundo de las TIC aplicado al Derecho Informático, lo que **incluye los derechos humanos, el sistema normativo y el ordenamiento jurisdiccional**.

El Derecho como Sistema Normativo

Hace referencia a las diferentes normas jurídicas (contratos privados o estatales; reglamentos de las entidades públicas o privadas; resoluciones de diversas instituciones; acuerdos de los concejos municipales o Distritales; ordenanzas de las Asambleas Departamentales, decretos de los alcaldes, de los gobernadores o del presidente de la república; leyes del congreso) **que, independientemente de su jerarquía, deben obedecer el contenido de la Constitución Política.**

El derecho como sistema normativo está institucionalizado. De acuerdo a Jiménez (2010) se tiene lo siguiente:

El Derecho es un sistema normativo que presenta como características el ser heterónimo, bilateral, externo y coercible.

- Heterónimo.** - Significa que las normas son creadas por **un sujeto distinto** al **destinatario** de la norma y que ésta además le **es impuesta** aún **en contra de su voluntad**. Significa la heteronomía:

“Estar sometido a la autoridad o mando de otro”.

Las normas jurídicas son creadas por los **órganos del Estado** por **la sociedad** en el Derecho consuetudinario.

- Bilateral.** - Una norma es bilateral cuando al **propio tiempo** que **impone deberes** a uno o varios sujetos, **concede facultades** otro u otros. Para señalar el mismo carácter se dice que la norma es **Imperativo-Atributiva**, es decir, se trata de reglas que además de **imponer deberes, conceden facultades**.

- Externo.** - Se determina tomando en cuenta únicamente **la adecuación externa** de **la conducta** con **el deber estatuido**, prescindiendo de **la intención** o **convicción** del obligado. **La validez** en **el cumplimiento** de los deberes jurídicos depende de **la simple observancia** de la norma, aun cuando se lleve a cabo **contra** su **propia voluntad** y **convicción**.

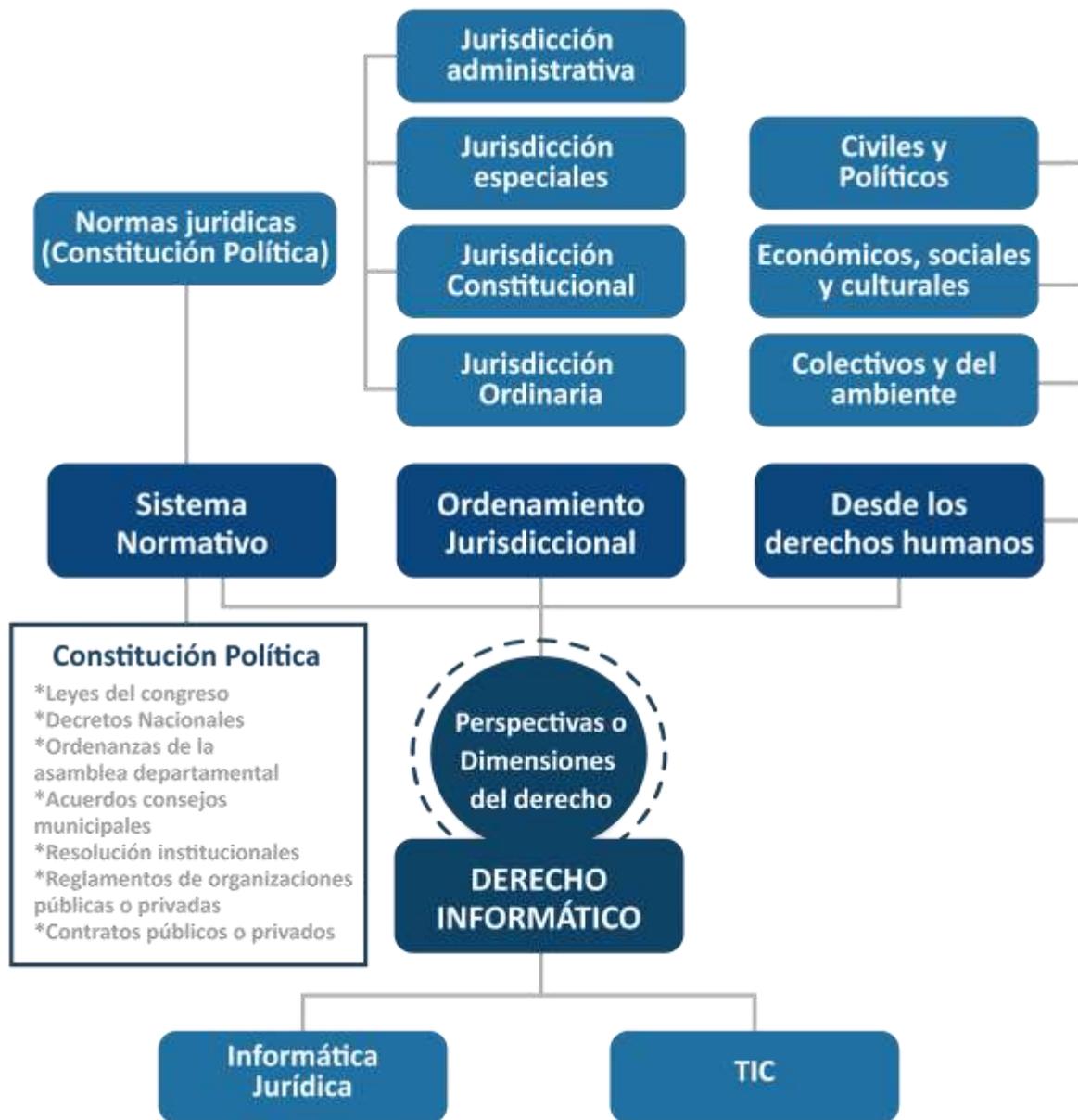
- Coercible.** - Posibilidad de que **la norma sea cumplida** en forma **no espontánea**, e incluso **en contra** de la **voluntad** del **obligado**. Ahora bien: esta posibilidad **es independiente** de **la existencia** de **una sanción**.

Figura 2 El Derecho como sistema Normativo



Fuente: segunda versión módulo de Derecho Informático, 2012.

Figura 3. Dimensiones del Derecho



Fuente: elaboración propia

El Derecho como Ordenamiento Jurisdiccional

Una jurisdicción puede ser entendida como una división del derecho por temas y por territorios. En Colombia, además de las jurisdicciones especiales se encuentra la jurisdicción Ordinaria, la jurisdicción Constitucional y la administrativa.

Figura 4. Dimensiones del derecho

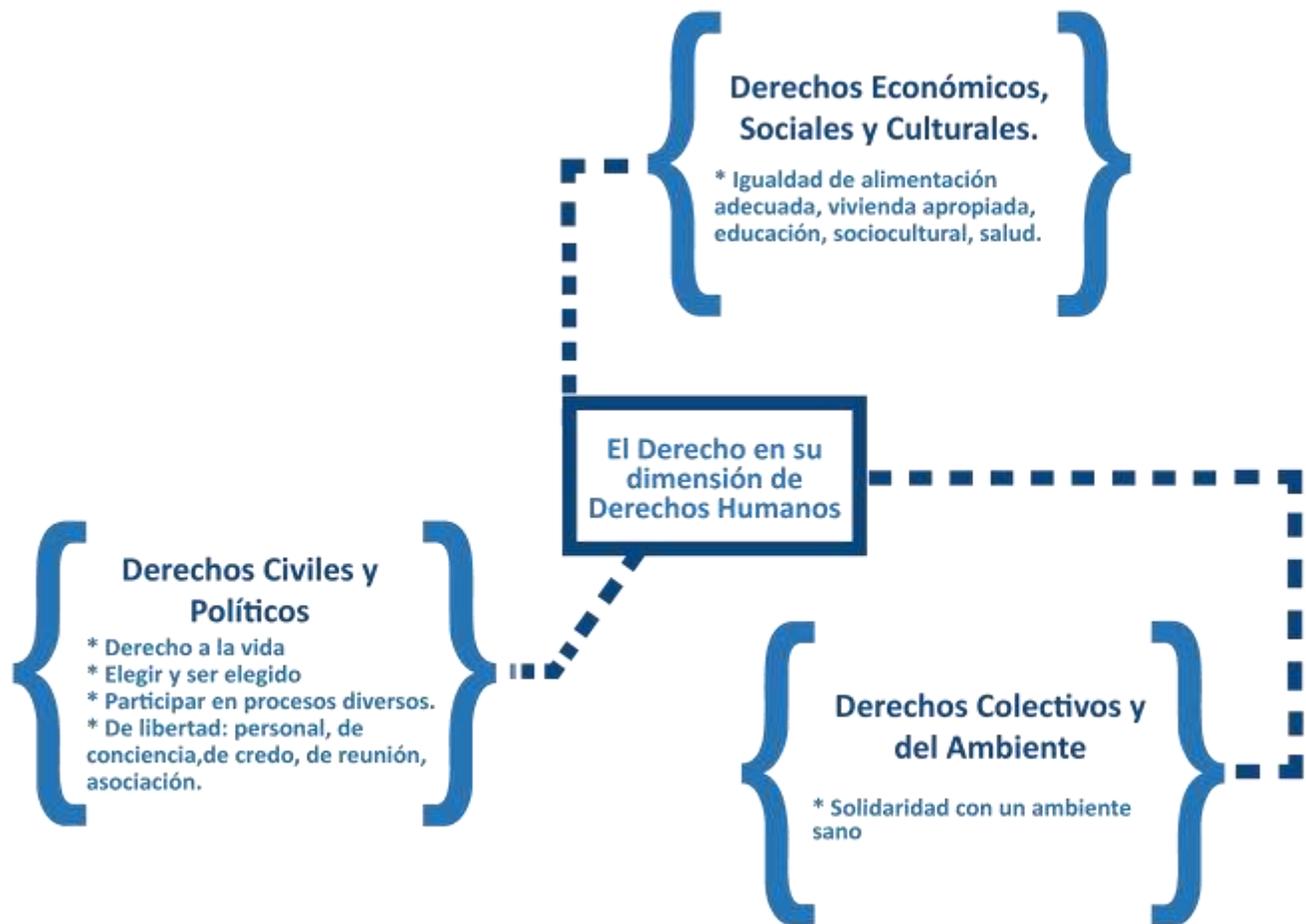


Fuente: Elaboración propia

El Derecho en su Dimensión de Derechos Humanos

Los **derechos humanos** son derechos inherentes a la persona humana, **se caracterizan por ser universales, complementarios, inalienables e imprescriptibles**. Se constituyen históricamente de la integración de los siguientes derechos:

Figura 5. El derecho en su dimensión de derechos humanos



Fuente: Elaboración propia

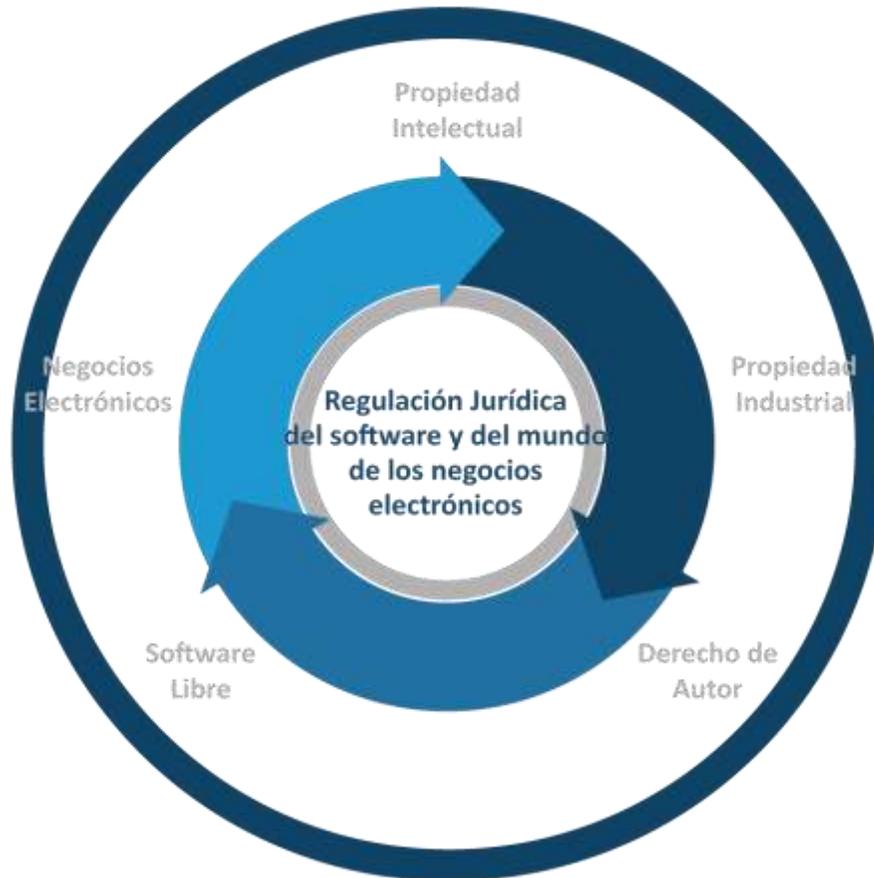
2.2 TEMA 2 INFORMATIZACIÓN DEL DERECHO

Hace referencia a **la relación** de las **TIC** con el **Derecho Informático**. Lo cual incluye:

- El mundo electrónico,
- Sociedad del conocimiento,
- Gobierno en línea,
- Negocios electrónicos,
- Comercio electrónico,
- Procuración electrónica,
- Mercadeo electrónico,
- Educación electrónica,

 Libros electrónicos.

Figura 6. Dimensiones del derecho



Fuente: Elaboración propia

De acuerdo a **EcuRed (2015)**, el **Derecho informático** cumple un **rol prioritario** en **la prevención** de **situaciones problemáticas** que se les pueda presentar a **los usuarios** que hacen uso de **las nuevas Tecnologías** de la **Información y Comunicación**; **garantizando regulaciones** a través de **instituciones jurídicas** que se encargan de buscar **solución** a **las dificultades** que puedan generarse por **el uso** de **los medios electrónicos** en la sociedad de la información.

“El Derecho informático adquiere gran importancia y trascendencia por el desarrollo de un número cada vez mayor de elementos informáticos, electrónicos, ópticos y similares, que facilitan la vida del hombre, pero a su vez, le generan serias dificultades en su interacción con los demás seres humanos, surgiendo de esta manera una serie de circunstancias que permiten el desarrollo, fortalecimiento y perfeccionamiento del Derecho informático y sus instituciones jurídicas”.

A continuación, se define un concepto básico para cada elemento involucrado en la Informatización del Derecho, conceptos que se profundizarán cuando se describa el tema de Gobierno en Línea.

Mundo Electrónico

Los mundos virtuales son actualmente un reto para la sociedad de la información, los cuales, así como proporcionan ventajas competitivas en cuanto al manejo de la información en tiempo y espacio, también presentan desventajas si no se tiene el debido cuidado en su manipulación.

En la actual era del conocimiento se pueden observar mundos virtuales que permiten que los educandos o usuarios en línea aprovechen sus beneficios, tales como: **SecondLife, Habbo, Sanalika, Smeet, Ildom, Club penguin, entre otros, los cuales permiten la interacción cara a cara con los usuarios en línea alrededor del mundo**, además del hecho de tener disponibles recursos intelectuales que ayudan en la debida alimentación del conocimiento.

Sociedad del Conocimiento

Según el Espectador, “En el mundo globalizado actual, la llamada “sociedad del conocimiento” se entiende como el uso intensivo de los sistemas educativos y de la ciencia, la tecnología y la innovación (CT&I) para transformar realidades sociales, económicas, políticas y culturales adversas, en función del desarrollo integral, la preservación del medio ambiente, el aprovechamiento sostenible de los recursos, la generación de movilidad e inclusión social, y el logro de la estabilidad social y política de los países”

Gobierno en Línea

Se define como **el aprovechamiento de las Tecnologías de la Información y la Comunicación**, en pro a la prestación de un mejor servicio a los ciudadanos y empresas de una nación.

De acuerdo a MinTic:

“ El rol de los ciudadanos también ha venido transformándose, las formas de expresión son diversas y se basan en mecanismos más directos y más poderosos, la mayoría apoyados en el uso de las Tecnologías de la Información y las Comunicaciones-TIC. La ciudadanía tiene un conocimiento importante que puede ser aprovechado en beneficio de las sociedades y el Estado puede servir de plataforma para canalizar y potenciar dicho conocimiento. Asimismo, son los ciudadanos los beneficiarios directos de las políticas públicas y de la toma de decisiones, lo que hace cada vez más imperante involucrarlos activamente en su construcción y validación. ”

En cuanto a la industria de la tecnología, los avances también son vertiginosos, no solo en lo que respecta al desarrollo de aplicaciones o servicios, también en lo relacionado con **la gestión de la tecnología al interior de las organizaciones**, hecho que ha transformado los procesos y actividades del mismo Estado. En este contexto, la Estrategia de Gobierno en línea permite potenciar los cambios que se han presentado en la forma de operar de las naciones, aprovechando los avances de la tecnología para garantizar una mejor comunicación e interacción con la ciudadanía, que permita además la prestación de más y mejores servicios por parte del Estado.

Negocios Electrónicos

Considerablemente los negocios electrónicos son una puerta de avance al desarrollo empresarial, ya que facilita a estas la interacción con los clientes y el poder hacer negociaciones sin necesidad de desplazarse de un lugar a otro, todo por medio de las Tecnologías de la Información y la Comunicación.

Según Petrella (2007),

“

“El desarrollo explosivo de las tecnologías de la información aplicadas a los negocios tradicionales y la aparición de Internet como medio para realizar operaciones comerciales a escala mundial, ha cambiado de manera radical las formas de relacionarse entre empresas, consumidores y gobierno, generando un antes y un después. Un punto de inflexión entre los dos milenios”

”

Comercio Electrónico

Facilita la compra y venta de artículos a través del medio digital, lo que facilita la vida del ser humano, sin embargo, si se hace uso indebido del medio informático y no se tienen las precauciones necesarias al momento de hacer las transacciones comerciales, se puede tener dificultades que afecten la tranquilidad del usuario en línea. Son parte de estos procesos: los intercambios electrónicos de datos, venta de bienes y servicios, transferencia de fondos a través de la vía electrónica, transacciones en línea, entre otros...

Procuración Electrónica

Hace referencia a la compra y venta de suministros a través de internet. También involucra el intercambio electrónico de datos.

Mercadeo Electrónico

Se define como el uso de las Tecnologías de la Información y la Comunicación para realizar las actividades o tareas de comunicación o transmisión de información a través de **medios electrónicos como internet, E-mail, o web.**

El mercadeo electrónico posibilita que la información sobre el producto ofertado sea transmitida a muchas personas en muchos lugares del mundo y de forma flexible y rápida.

Educación Electrónica

Es una de los medios más utilizados hoy día por los ciudadanos para la continuidad de su formación profesional o educativa (educación a distancia). **El e-learning** permite utilizar diversas herramientas y medios como internet, intranets, CD – ROM, uso de los procesos multimedia, entre otros.

Libros Electrónicos

Se define como la edición o versión digital de un libro que tiene sus orígenes en un papel. Ósea que es **escaneado** y puesto a favor del beneficio de la comunidad como aporte a la realimentación del conocimiento.

2.3 TEMA 3 GOBIERNO ELECTRÓNICO

De acuerdo al espectador:

“ El gobierno electrónico es más que un término utilizado por expertos en la materia. Es el resultado de un crecimiento exponencial de Internet y las tecnologías de la información durante los últimos 50 años o más. Visto de esta forma, se puede considerar al gobierno electrónico como un intento por modernizar las relaciones (y servicios) entre los individuos y las autoridades, a través de nuevas reglas y herramientas de gestión modernas. ”

Hacer referencia al mundo electrónico, es hablar de cómo las TIC han incidido actualmente en muchas áreas de la vida diaria. Una de ellas es el gobierno electrónico o e – government, como la aplicación de Tecnologías de la Información y la comunicación a la administración pública con el fin de volverla más eficiente. El gobierno electrónico implica la construcción de una sociedad más abierta, dónde la información esté distribuida, de manera que se alcance una mejor calidad de vida para los ciudadanos.

El programa Gobierno en línea, por ejemplo, impulsa una visión unificada del Estado, propendiendo por la protección de la información del individuo. Este programa facilita el acceso equitativo y multi-canal: Internet, teléfono fijo, teléfono móvil, telecentros que ha venido instalando el Programa Compartel en las zonas más alejadas del país y, en un futuro cercano, la televisión digital.

Negocios Electrónicos

Otra importante área sobre la que han influido las TIC, es la de los negocios electrónicos o e – business, con la implementación de tecnología en las diferentes áreas de la administración empresarial. Se aplica en el control de inventarios, el manejo de compras, el marketing, el control e integración de las diferentes áreas internas y externas a la empresa, etc.,

Ejemplos de e – business son las aplicaciones:

Negocio -a- Negocio (business-to-business B2B).

Negocio -a-consumidor (business-to-consumer B2C).

Negocio-a-gobierno (Business-to-government B2G).

Comercio Electrónico

El comercio electrónico (e – commerce) es una forma de realizar transacciones de bienes y servicios a través del uso de medios electrónicos. La característica fundamental del comercio electrónico es que la contratación, es decir, la oferta y la aceptación de la misma, se realizan on - line, existiendo la alternativa de efectuarse el pago también on - line.

MercadoLibre.com es un ejemplo de e – commerce, Se trata de una plataforma de compras y ventas por Internet. Compradores y vendedores se encuentran para intercambiar información y realizar transacciones de comercio electrónico con una amplia gama de productos y servicios, a precio fijo o en subasta. También permite que los vendedores publiquen vehículos, inmuebles y servicios en una sección exclusiva de avisos clasificados en línea.

Procuración Electrónica

El e - procurement (procuración electrónica) es la automatización de procesos internos y externos relacionados con el requerimiento, compra, suministro, pago y control de productos utilizando el Internet como medio principal en la comunicación cliente-proveedor. Es una tecnología relacionada con la administración de la cadena de suministros (Supply Chain Management). El flujo de información se realiza en tiempo real.

Existe el **e - procurement simple** (compra de bienes y servicios que requieren un proceso sencillo de compra), el **e -procurement complejo** (los bienes y servicios de adquisición son de una relevancia que requiere selección y evaluación previa de proveedores) **y el e – procurement estratégico** (solamente se ejerce el sistema con un pequeño grupo de proveedores preseleccionados y evaluados).

Mercado Electrónico

El e-Marketing o mercadeo electrónico es la utilización de las tecnologías electrónicas para el marketing directo con el fin de lograr clientes y fidelizarlos. El e-Marketing es una opción muy utilizada por las empresas para promocionar y difundir sus productos y servicios. El motivo es el bajo costo y la obtención de las preferencias de sus clientes.

Un ejemplo de mercadeo electrónico es SAVICOM. Es un servicio de administración de listas de correo que está disponible vía internet. Administra Bases de Datos de emails y envía mensajes ya sea publicitarios o no. **Las listas de correo** se están convirtiendo en la forma más efectiva para realizar marketing directo vía email con el fin de construir y mantener relaciones comerciales permanentes con clientes, proveedores o comunidad en general.

Educación Electrónica

El e-Learning es el suministro de programas educacionales y sistemas de aprendizaje a través de medios electrónicos. Se basa en el uso de una computadora u otro dispositivo electrónico (por ejemplo, un teléfono móvil) para proveer a las personas de material educativo. La educación a distancia creó las bases para el desarrollo del e-Learning, que resuelve dificultades típicas de la educación tradicional.

EJEMPLOS DE E –LEARNING EN COLOMBIA SON:

SENA Virtual
Universidad Nacional Abierta y a Distancia
Universidad Autónoma de Bucaramanga,
Universidad Autónoma de Occidente, UAO
Universidad Tecnológica de Bolívar, UTB
Universidad Tecnológica de Pereira, UTP
Universidad de Los Andes
Universidad de Manizales
Universidad Manuela Beltrán
Corporación Universitaria Remington.

Libros Electrónicos

Un e-Book o libro electrónico es un archivo que algún editor ha puesto en la red, o que compramos en una librería virtual, y que descargamos a un computador. **Los e-Books tienen muchas ventajas: acceso universal, disponibilidad inmediata, precio de venta más bajo, nuevas utilidades, protección de los derechos de autor.** En algunos casos su contenido puede imprimirse y/o copiarse, si existe autorización por parte del editor.

EBOOKS de Colombia es el principal portal que da visibilidad exclusiva a los libros electrónicos producidos en el país; permitiendo que cada obra pueda ser adquirida desde cualquier parte del mundo a todo instante, con la garantía que ofrece el DRM, Digital Right Management; así como de adquirirlo físicamente con las posibilidades de Impresión a Demanda, POD, generalmente por un costo inferior al físico; gracias a las plantas de producción de Publidisa en España, México y Argentina

“ Tener en cuenta: El comercio electrónico es uno de los más grandes desarrollos de las TIC. En Colombia la Ley de Comercio Electrónico es la Ley 527 de 1999. ”

Dentro de otras regulaciones jurídicas de la informática tenemos:

La Firma Digital

“La firma electrónica es un conjunto de datos electrónicos añadidos a un mensaje que permite al receptor de los mismos comprobar su fuente e integridad y protegerse así de la suplantación o falsificación. Para su generación se suelen utilizar técnicas criptográficas”. (Kimaldi).

La firma electrónica es un concepto amplio e indefinido desde el punto de vista tecnológico. Es por tanto una expresión más genérica que la de firma digital. La firma digital es aquella **firma electrónica** que está basada en los **sistemas de criptografía** de clave pública (PKI – Public Key Infrastructure). Normalmente, la firma digital aparece en una smart card (tarjeta chip inteligente).

La firma digital es, entonces, un instrumento que garantiza tanto la autenticidad de un documento como la integridad del mismo; y tiene los mismos efectos que la firma escrita. No hay que confundir la firma digital con una firma digitalizada. Esta última es simplemente una representación gráfica de la firma manuscrita obtenida a través de un escáner.

Principios de equivalencia en la ley 527 de 1999.

- Existe equivalencia entre toda forma electrónica de escrito y su contraparte impresa.
- La función del papel como depositario de información, la cumple de manera idéntica la misma en soporte electrónico.
- Las tecnologías de la información deben imitar enteramente toda garantía que el medio o procedimiento tradicional pretenda remplazar.

El Certificado Digital

El certificado digital es un archivo emitido por la entidad de certificación, es digital, intransferible y no modificable. Este certificado lo expide la entidad de certificación. El certificado se almacena en el computador del solicitante. Este archivo es el que permite al propietario identificarse cuando realiza operaciones electrónicas. El destinatario del mensaje firmado digitalmente verifica la autenticidad de dicho mensaje y procede a descifrar su contenido mediante el uso de la llave pública, contenida en el certificado.



Entidades de Certificación

Figura 7. Ejemplo de entidades de certificación

Fuente: segunda versión módulo de Derecho Informático, 2012.

Las entidades de certificación son las personas jurídicas que poseen el software y el hardware para la generación de firmas digitales y los certificados sobre su autenticidad. **La Ley No 527 de 1999, Ley de comercio electrónico**, regula el tema de la firma digital, los certificados digitales y las entidades certificadoras.

“Tenga presente: La firma digital es un instrumento que garantiza tanto la autenticidad de un documento como la integridad del mismo; y tiene los mismos efectos que la firma escrita.”

2.3.1 EJERCICIO DE APRENDIZAJE UNIDAD 1 TEMA 2.1

1. Relacione la columna izquierda con la columna de la derecha.

a. Dimensiones del derecho

Constitucional, especial, administrativa, Ordinaria. **E**

b. Sociedad tecnológica	Técnica que tiene por objeto la investigación de los conocimientos aplicables a la recuperación informática. F
c. Derecho informático	Acción u omisión voluntaria o imprudente que se encuentra penada por la ley. D
d. Delito informático	Normatividad, Ordenamiento jurisdiccional, Derechos humanos. A
e. Tipos de jurisdicciones en Colombia	Diversidad de contextos para la garantía de los derechos humanos. B
f. Informática Jurídica	Ciencia_ cultura, alianza, beneficio, perjuicio, principios, normas. C
g. Libros Electrónicos	Se define como el aprovechamiento de las Tecnologías de la Información y la Comunicación, en pro a la prestación de un mejor servicio a los ciudadanos y empresas de una nación. H
h. Gobierno en Línea	Es una de los medios más utilizados hoy día por los ciudadanos para la continuidad de su formación profesional o educativa (educación a distancia). I
i. Educación electrónica	Se define como la edición o versión digital de un libro que tiene sus orígenes en un papel. Ósea que es escaneado y puesto a favor del beneficio de la comunidad como aporte a la realimentación del conocimiento. G

2. El derecho puede ser entendido como mínimo desde 3 perspectivas (elija la opción correcta):

- a. Sistema Normativo, Constitucional y Especial.
- b. Administrativa, Ordinario y Derechos Humanos.
- c. Sistema legal, Ordenamiento Jurídico, derechos relacionales.
- d. Como sistema normativo, ordenamiento jurisdiccional y desde los derechos.

Clave D

3. El problema de los delitos informáticos ha incrementado incalculablemente debido en gran parte al desconocimiento que tiene el hombre acerca de las normativas existentes que regulan jurídicamente el tema de la informática en Colombia. **Se propone como alternativa para resolver este problema.**

- a. Analizar la regulación jurídica de la informática en Colombia.
- b. Analizar los derechos humanos y los delitos informáticos en el contexto de la sociedad Tecnológica.
- c. Orientar al ser humano en las principales disposiciones normativas existentes, que regulan jurídicamente el tema de la informática en Colombia.
- d. Explorar los elementos básicos de aproximación a la normativa existente que regula jurídicamente el tema de la informática en Colombia.

Clave C

4. La firma digital no se puede confundir con un documento escaneado y digitalizado, porque las firmas digitales ayudan a identificar la información desde diferentes fuentes, las cuales permiten la verificación e integridad de los datos y sus fuentes. **Con base a lo anterior se puede afirmar que una firma digital.**

- a. Usa una clave para identificar fuentes de información directas.
- b. Da al destinatario seguridad en que el mensaje fue creado para el remitente y que no fue alterado durante la transmisión.
- c. Es una vigencia del certificado digital del firmante.
- d. Es una firma escaneada.

Clave B

2.3.2 EJERCICIO DE APRENDIZAJE UNIDAD1 TEMA 2.2

1. El comercio electrónico es uno de los más grandes desarrollos de las TIC. La siguiente ley regula el comercio electrónico en Colombia. **(Elija la opción correcta)**

- a. Ley 1273 de 2009
- b. Ley 527 de 1999
- c. Ley 1403 de 2010
- d. Ley 23 de 1982

Clave B

2. La siguiente es otra importante área sobre la que han influido las TIC. (Elija la opción correcta)
- a. Los negocios electrónicos
 - b. La propiedad intelectual
 - c. La propiedad patrimonial
 - d. Los derechos de autor

Clave A

3. Las entidades de certificación son las personas jurídicas que poseen el software y el hardware para la generación de firmas digitales y los certificados sobre su autenticidad. De acuerdo a lo anterior, la siguiente ley es la encargada de regular el tema de la firma digital, los certificados digitales y las entidades certificadoras.
- a. Ley 527 de 1999
 - b. Ley 1273 de 2009
 - c. Ley 428 de 1991
 - d. Ley 1703 de 2014

Clave A

4. El e – Marketing es una opción muy utilizada por las empresas para promocionar y difundir sus productos y servicios. El motivo es el bajo costo y la obtención de las preferencias de sus clientes. A este uso de las tecnologías electrónicas para el marketing directo con el fin de lograr clientes y fidelizarlos se le conoce también con el siguiente término.
- a. Educación electrónica
 - b. Libros electrónicos
 - c. Comercio electrónico
 - d. Mercado electrónico

Clave D

2.3.3 EJERCICIO DE APRENDIZAJE UNIDAD1 TEMA 2.3

Estudiantes a repasar.

¿Qué es la firma digital?

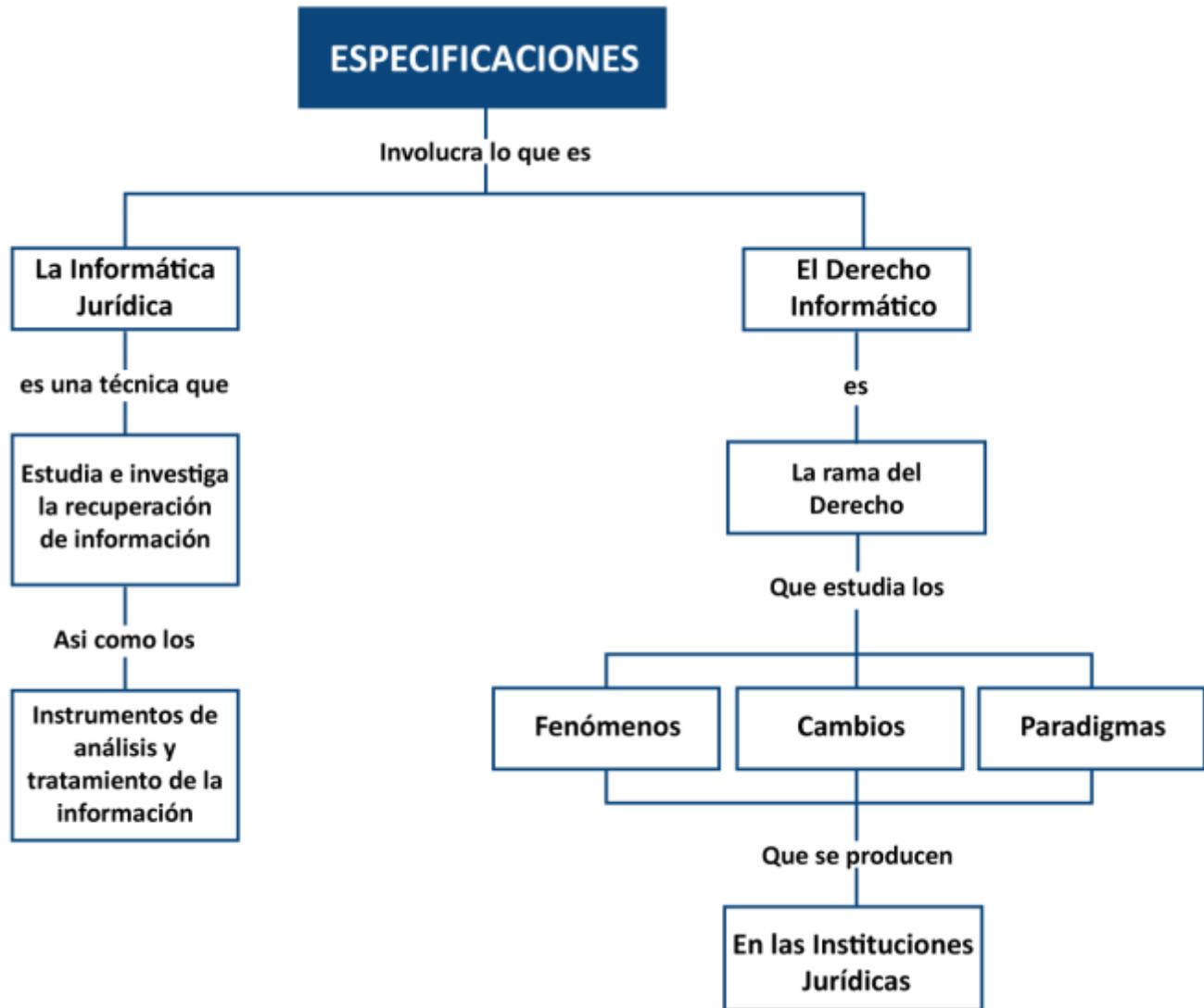
“La firma electrónica es un conjunto de datos electrónicos añadidos a un mensaje que permite al receptor de los mismos comprobar su fuente e integridad y protegerse así de la suplantación o falsificación. Para su generación se suelen utilizar técnicas criptográficas”. (Kimaldi).

¿Qué es informática jurídica?

Es una técnica que tiene por objeto el estudio e investigación de los conocimientos aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamientos de los instrumentos de

	análisis y tratamiento de información jurídica, necesaria para lograr dicha recuperación.
¿Con que no se debe confundir una firma digital, y porque?	No se debe confundir con una firma digitalizada, porque esta es simplemente una representación gráfica de la firma manuscrita obtenida a través de un escáner.
Defina que es la propiedad intelectual	Es el conjunto de derechos que corresponden a los autores y a otros titulares (artistas, productores, organismos de radiodifusión...) respecto de las obras y prestaciones fruto de su creación.
Menciona 4 tipos de licenciamiento de software	Freeware, Shareware, Adware y Software Libre.
¿Cuál es la principal característica de la firma digital?	Garantizar tanto la autenticidad de un documento como la integridad del mismo.
¿Cuántas y cuáles son las dimensiones que abarca la propiedad industrial?	Abarca dos dimensiones: <ul style="list-style-type: none"> a. La propiedad industrial (que se patenta) b. Los derechos de autor (que se registran)
¿Ante quién se patenta la propiedad intelectual?	Se patenta ante la Superintendencia de Industria y Comercio, los derechos de autor se registran ante la Dirección Nacional de Autor.

3 UNIDAD 2: INFORMÁTICA JURÍDICA – DERECHO INFORMÁTICO



3.1 TEMA 1 ESPECIFICACIONES

Informática jurídica y derecho informático.

La informática jurídica es una técnica que tiene por objeto el estudio e investigación de los conocimientos aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica, necesaria para lograr dicha recuperación.

Un ejemplo importante de informática jurídica en Colombia es JURISCOL. Cuenta con una base de datos con las leyes expedidas hasta la fecha desde 1964 y decretos expedidos hasta la fecha desde 1982, Las normas se presentan

en su texto original, es decir, tal cual fueron publicadas. En relación con la jurisprudencia el objetivo es presentar la jurisprudencia de la Corte Constitucional desde 1992, año de su creación hasta la fecha.

Otros ejemplos de proyectos de informática jurídica, son los emprendidos por Legis, la Universidad Externado de Colombia, la Biblioteca Jurídica Digital y Avance Jurídico.

El derecho informático, por su parte:

“

Es “la rama del Derecho encargada de estudiar los cambios, fenómenos y paradigmas que se producen actualmente en las instituciones jurídicas debido a la intromisión de las tecnologías de la información y comunicación en la sociedad, afectando las estructuras jurídico políticas, económicas inclusive interpersonales. El Derecho Informático aborda el estudio de las tecnologías de la información y comunicación desde dos ejes, el primero de ellos estudia la tecnología como objeto del Derecho, y estudia la tecnología como instrumento del Derecho”. (ACODITIC, 2010).

”

Ejemplos de regulaciones jurídicas de la informática o de su uso son: los derechos humanos en el ciberespacio, los delitos informáticos, la propiedad intelectual sobre el hardware y el software, el gobierno electrónico, los negocios electrónicos, la firma electrónica, los contratos informáticos, las direcciones IP y los nombres de dominio.

“

Tener en cuenta: La informática jurídica es la informática aplicada al derecho; el derecho informático es el derecho aplicado a la informática.

”

Diversos conceptos sobre el Derecho Informático.

El derecho y la Informática se relacionan de dos maneras. Una es como herramienta o instrumento, esto es: la informática jurídica. Otra manera es cuando se considera la informática como objeto del Derecho, esto es: el Derecho Informático. A continuación, se exponen algunas definiciones sobre el derecho informático.

“

“El término “Derecho Informático” fue acuñado por el Prof. Dr. Wilhelm Steinmüller, académico de la Universidad de Regensburg de Alemania en los años 70. Sin embargo, no es un término unívoco, pues también se han buscado una serie de términos para el Derecho Informático como

Derecho Telemático, Derecho de las Nuevas Tecnologías, Derecho de la Sociedad de la Información, Iuscibernética, Derecho Tecnológico, Derecho del Ciberespacio, Derecho de Internet, etc.”

”

(<http://www.informaticalegal.com.ar/derecho-informatico/>)

“Constituye una ciencia y rama autónoma del derecho que abarca el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en dos aspectos: a) Regulación del medio informático en su expansión y desarrollo y b) Aplicación idónea de los instrumentos informáticos”.

<http://internet-proceso.blogcindario.com/2008/10/00005-definiciones-de-derecho-informatico.html>

“Conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación de sujetos en el ámbito de la informática y sus derivaciones, especialmente en el área denominada "tecnología de la información".

http://www.nicolastato.com.ar/esp/index.php?option=com_content&view=article&id=6:artderechoinformaticonuevarama&catid=10:catgderechoinf&Itemid=7

“Se define como un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la informática. Por otro lado, hay definiciones que establecen que es una rama del derecho especializado en el tema de la informática, sus usos, sus aplicaciones y sus implicaciones legales”.

“Se considera que el Derecho Informático es un punto de inflexión del Derecho, puesto que todas las áreas del derecho se han visto afectadas por la aparición de la denominada Sociedad de la Información, cambiando de este modo los procesos sociales y, por tanto, los procesos políticos y jurídicos. Es aquí donde hace su aparición el Derecho Informático, no tanto como una rama sino como un cambio”.

<http://www.slideshare.net/josephito9/derecho-informatico-4829061>

“Constituye una ciencia y rama autónoma del derecho que abarca el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en dos aspectos: a) Regulación del medio informático en su expansión y desarrollo y b) Aplicación idónea de los instrumentos informáticos”.

<http://hechoencu.wordpress.com/2008/05/27/el-concepto-de-derecho-informatico-como-rama-autonoma/>

“Universalidad de problemas que surgen de las transformaciones que el derecho ha ido realizando como imposición de ciertas actividades novedosas que se desarrollan en el ámbito social y que requieren nuevas regulaciones o una reinterpretación de las regulaciones ya existentes a fin de dar respuestas en el sentido de la justicia”.

<http://www.palermo.edu/ingenieria/downloads/pdfwebc&T8/8CyT05.pdf>

“**Tenga presente: Al considerarse la informática como objeto del derecho, estamos en el terreno del derecho informático.**”

Delito informático

Acerca de los delitos.

Un delito es una acción u omisión voluntaria o imprudente que se encuentra penada por la ley. Para que la conducta sea punible se requiere que sea típica, antijurídica y culpable. El Código Penal colombiano define cada una de estas dimensiones esenciales:

La tipicidad hace referencia a que la ley penal debe definir de manera inequívoca, expresay clara las características básicas estructurales del tipo penal.

La antijuridicidad hace referencia a que una conducta típica, para que sea punible, requiere que lesione o ponga efectivamente en peligro, sin justa causa, un bien jurídicamente tutelado por la ley penal.

La **culpabilidad** se refiere a que no se contempla la responsabilidad objetiva, por tanto, aquí sólo se pueden imponer penas por conductas realizadas con culpabilidad.

El delito informático puede definirse como “Conducta ilícita que utiliza la informática como medio como fin”.

Como medio, ejemplo: fraude electrónico.

Como fin, ejemplo: los delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.

3.2 TEMA 2 DELITOS INFORMÁTICOS DEFINIDOS EN LA LEY PENAL COLOMBIANA

La **Ley 1273 de 2009** creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes. El nuevo bien jurídico tutelado se denomina: “De la Protección de la información y de los datos”.

El Título VII bis del Código Penal contiene los siguientes delitos:

“Capítulo I: de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. <Artículo adicionado por el artículo 1 de la Ley 1273 de 2009. El nuevo texto es el siguiente:>

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,

incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000

salarios mínimos legales mensuales

vigentes.

ARTÍCULO 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DETELECOMUNICACIÓN.

<Artículo adicionado por el artículo 1 de la Ley 1273 de 2009. El nuevo texto es el siguiente:> 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, incurrirá en pena de prisión de cuarenta

y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

ARTÍCULO 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. <Artículo adicionado por el artículo 1 de la Ley 1273 de 2009. El nuevo texto es el siguiente:> 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 incurrirá en pena de

prisión de treinta y seis (36) a setenta y dos (72) meses.

ARTÍCULO 269D. DAÑO INFORMÁTICO. <Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.

El nuevo texto es el siguiente:> 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, incurrirá

en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios

mínimos legales mensuales vigentes.

ARTÍCULO 269E. USO DE SOFTWARE MALICIOSO. <Artículo adicionado por el artículo 1 de la Ley 1273 de 2009. El nuevo texto es el siguiente:> 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, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96)

meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES. <Artículo adicionado por el artículo 1 de la Ley 1273 de

2009. El nuevo texto es el siguiente:> 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, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en

multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. <Artículo adicionado por el artículo 1 de la Ley 1273 de 2009. El nuevo texto es el siguiente:> El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe envíe página electrónica, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a

noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre

que la conducta no constituya delito sancionado con pena más grave.

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. <Artículo adicionado por el artículo 1 de la Ley 1273 de 2009. El nuevo texto es el siguiente:> 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.**

”

Capítulo II: de los atentados informáticos y otras infracciones.

ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. <Artículo adicionado por el artículo 1 de la Ley 1273 de 2009. El nuevo texto es el siguiente:> 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 aun usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

ARTÍCULO 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. <Artículo adicionado por el artículo 1 de la Ley 1273 de 2009. El nuevo texto es el siguiente:> 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, incurrirá en pena de prisión de cuarenta y ocho (48) asientos veinte (20) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

“Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad”.

Ingeniería social.

La “Ingeniería Social” puede definirse como el conjunto de habilidades, técnicas, artilugios, tretas y engaños usados por ciberdelicuentes para engañar a sus víctimas, de tal manera que revelen contraseñas u otra información que sirva para defraudarlas económicamente. La ingeniería social enfoca en que, en un sistema de seguridad total siempre habrá una brecha o una debilidad, el factor humano.

Se utilizan diversas formas para engañar a las personas:

Suplantación de identidad (phishing): Se combina con el spam. Emails acerca de famosos: Supuestamente se difunden fotos XXX, supuestas muertes, etc. Sorteos y concursos: Correos que anuncian que puede participar o que incluso ha ganadoun sorteo o concurso.

Cartas nigerianas: e-mails en las que el remitente promete negocios muy rentables.

“ Tener en cuenta: El delito informático se puede presentar por el uso de la informática comomedio o como fin. Ejemplo del primer caso es la suplantación de sitios web para obtener datos personales; del segundo, el daño informático. ”

3.3 TEMA 3 ANÁLISIS DE PROBLEMAS

El aprendizaje basado en problemas y el estudio de casos, ayudan al estudiante a pensar y proponer soluciones viables a situaciones problemáticas que tienen que ver con su área del saber.

El Servicio de Innovación Educativa de la Universidad Politécnica de Madrid, **citando a Prieto (2006)** señala que “el aprendizaje basado en problemas representa una estrategia eficaz y flexible que, a partir de lo que hacen los estudiantes, puede mejorar la calidad de su aprendizaje universitario en aspectos muy diversos”, entre esos aspectos tenemos: la comunicación, toma de decisiones, trabajo en equipo, entre otros...

El estudio de casos se ha convertido en un método de investigación importante, ya que ofrece resultados e información viables para la toma de decisiones. Este estudio es totalmente cualitativo.

Según castro (2010), citando a Yim (1994), un estudio de casos puede ser simple o múltiple, lo cual dependerá de la cantidad de casos a estudiar y de sus diversas unidades de análisis.

De acuerdo a Chopan (2010), para simplificar la diferenciación entre un **ABP** y **el estudio de casos**, se propone el siguiente cuadro comparativo.

Tabla 1. Cuadro comparativo ABP – Estudio de casos

ABP	Estudio de Casos
-----	------------------

Tiene etapas o pasos definidos en forma correctiva.	Los procesos no necesariamente pueden estar estructurados secuenciada.
El problema es presentado por escrito.	El proceso de elaboración plantea interrogantes.
Requiere la búsqueda de información técnica.	Análisis de casos en forma conjunta.
Se tiene que definir el problema.	Está enfocado a reforzar los conocimientos ya adquiridos.
No existe necesariamente una solución que sea la verdadera.	Solución razonada, se cuenta con los datos del caso en búsqueda de una solución.

En el ABP, el estudiante adquiere o realimenta el aprendizaje a través de una situación problemática propuesta para este fin, la cual lleva a los educandos a evaluar sus propias necesidades de aprendizaje, ya que estos investigan, proponen hipótesis y entregan diversos resultados de resolución del problema propuesto. Este instrumento de aprendizaje se puede trabajar de forma individual o colaborativa.

En el estudio de casos se hace la propuesta del caso a estudiar, lo cual debe estar basado en información real previamente analizada. De acuerdo a Chopan, el profesor debe motivar y facilitar el estudio del caso a los estudiantes, brindando diversas posibilidades para su posible solución. Los estudiantes por su parte, se comprometen a investigar respecto al caso, discutir sus hallazgos, proponer y comprobar hipótesis. Un estudio de caso permite al estudiante verificar los aprendizajes adquiridos acerca de temas tratados.

3.3.1 EJERCICIO DE APRENDIZAJE UNIDAD 2 TEMA 3.1

1. El delito informático puede definirse como “conducta ilícita que utiliza la informática como medio o como fin”.

Con base a lo anterior, un ejemplo de una conducta ilícita como medio es la siguiente.

- Violación a la Integridad
- Copiar una obra literaria
- Fraude electrónico
- Violación a los derechos humanos

Clave C

2. Es una modalidad de distribución de software, en la que el usuario puede hacer uso de forma gratuita del producto, pero con limitaciones o restricciones definidas. Con base a lo anterior, a este tipo de software se le da el siguiente nombre.

- a. shareware
- b. freeware
- c. adware
- d. copyleft

Clave A

3. Es un derecho exclusivo de un autor para explotar una obra literaria, científica o artística durante un tiempo definido, proviene del derecho anglosajón y se relaciona con el área patrimonial de los derechos de autor. **Con base a lo anterior, esta afirmación hace referencia al siguiente término.**

- a. copyleft
- b. copyright
- c. freeware
- d. adware

Clave B

4. Es el estudio de las tecnologías de la información y comunicación desde los ejes, el primero de ellos estudia la tecnología como objeto del Derecho, y estudia la tecnología como instrumento del Derecho (ACODITIC, 2010). **Con base a lo anterior, esta afirmación hace referencia al siguiente término.**

- a. informática jurídica
- b. derecho informático
- c. informática forense
- d. delito informático

Clave B

3.3.2 EJERCICIO DE APRENDIZAJE UNIDAD 2 TEMA 3.2

1. De acuerdo a la ley 1273 de 2009, 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, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

La anterior afirmación está contenida en el siguiente artículo.

- a. 269C
- b. 269A
- c. 269G
- d. 269H

Clave B

2. De acuerdo a la ley 1273 de 2009: 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, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

La anterior afirmación está contenida en el siguiente artículo.

- a. 269G
- b. 269B
- c. 269E
- d. 269F

Clave C

3. De acuerdo a la ley 1273 de 2009,
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, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

La anterior afirmación está contenida en el siguiente artículo.

- a. 269B
- b. 269D
- c. 269H
- d. 269A

Clave A

4. De acuerdo a la ley 1273 de 2009, 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 aun usuario ante los sistema de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este código.

La anterior afirmación está contenida en el siguiente artículo.

- a. 269J
- b. 269B
- c. 269I
- d. 269H

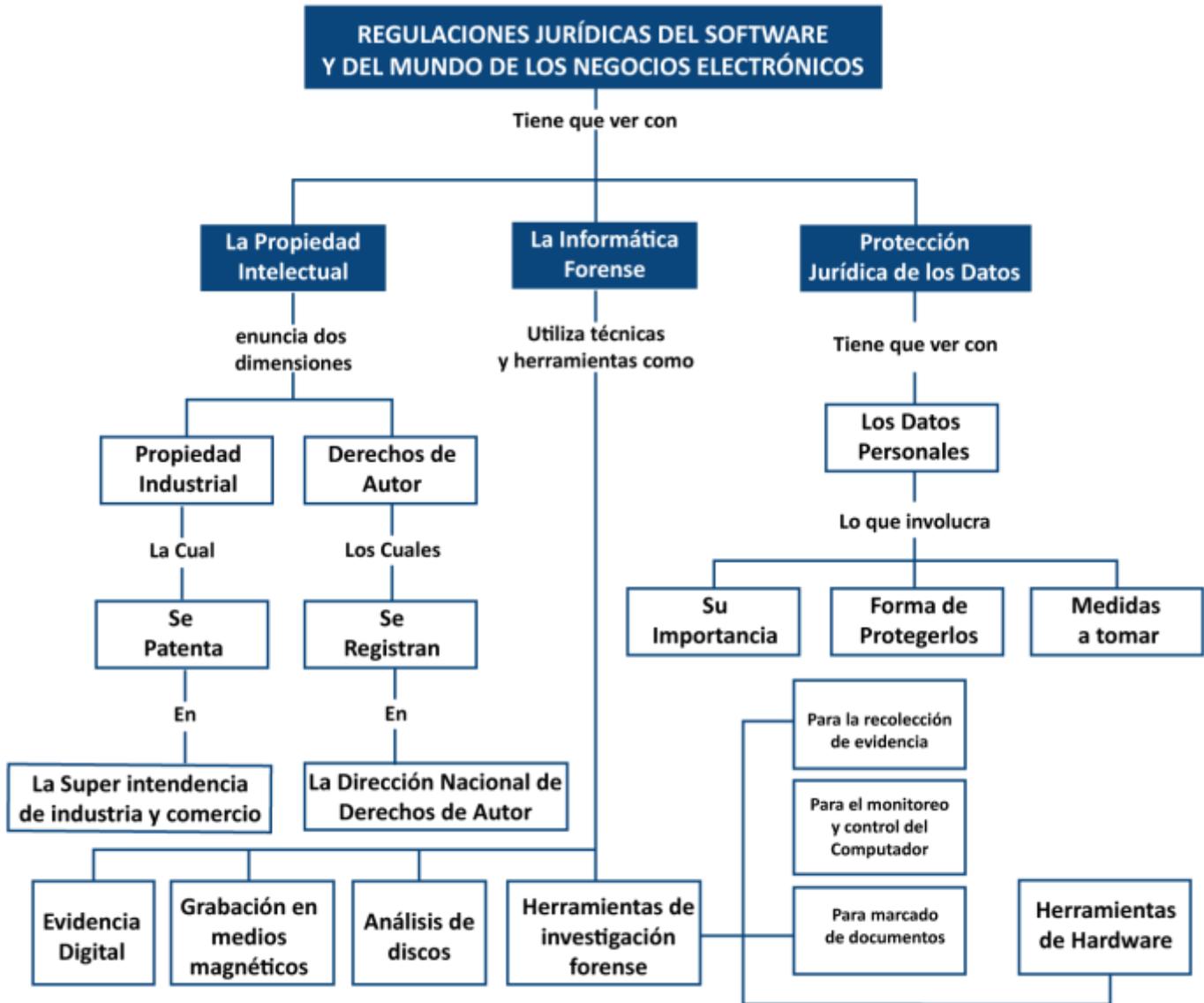
Clave C

3.3.3 EJERCICIO DE APRENDIZAJE UNIDAD 2 TEMA 3.3

Estudiantes a repasar.

¿Es necesario las firmas digitales para poder aplicar el derecho informático?	No es necesario porque la firma digital es para garantizar la autenticidad de un documento y la integridad del mismo.
¿Qué es ingeniería social	Es un conjunto de habilidades, técnicas, artilugios, tretas y engaños usados por ciberdelincuentes para engañar a sus víctimas, de tal manera que revelen contraseñas y otra información que sirva para defraudarlas económicamente.
¿Qué es Copyleft?	Es un concepto establecido por el movimiento GNU (acrónimo de GNU no es Unix), líder del Linux, que se refiere a un método para hacer software libre o de código abierto, que exige que todas las versiones del mismo sean también libres.
¿Qué es Copyright?	Proviene del derecho anglosajón, y se relaciona con el área patrimonial de los derechos de autor.
¿Qué es shareware?	Es un software que se distribuye con limitaciones, como versión de demostración o evaluación.
¿Qué es Adware?	Es software gratuito al que se le incorpora normalmente publicidad.
¿En dónde se realiza el proceso para obtener la firma digital?	Se realiza en la entidad de certificación son las personas jurídicas que poseen el software y el hardware para la generación de firmas digitales y los certificados sobre su autenticidad.
¿Cuál es la entidad encargada de la firma digital?	(CERTICAMARA) entidad de certificación autorizada por la Superintendencia de Industria y Comercio.

4 UNIDAD3: REGULACIONES JURÍDICAS DEL SOFTWARE Y DEL MUNDO DE LOS NEGOCIOS ELECTRÓNICOS



4.1 TEMA 1 NORMATIVIDAD

Propiedad intelectual, industrial y derechos de autor.

La propiedad intelectual abarca dos dimensiones: a) La propiedad industrial (que se patenta) y b) Los derechos de autor (que se registran). La primera se adquiere sobre invenciones, marcas, slogans, circuitos integrados, diseños, etc. Los segundos se adquieren sobre obras literarias, artísticas, científicas, incluyendo en esta

categoría al software. La propiedad industrial se patenta (ante la Superintendencia de Industria y Comercio), los derechos de autor se registran ante la Dirección Nacional de Derechos de Autor.

“ Los derechos sobre la propiedad industrial se protegen por un tiempo de diez a veinte años, sobre los derechos de autor mientras dure la vida del mismo, más ochenta años más. La Ley 23 de 1982, sobre derechos de autor, consagra los derechos morales y los derechos patrimoniales. ”

En relación con los derechos patrimoniales, se consagra que:

“Artículo 12º.- El autor de una obra protegida tendrá el derecho exclusivo de realizar o de autorizar uno cualquier de los actos siguientes:

- a. Reproducir la obra.
- b. Efectuar una traducción, una adaptación, un arreglo o cualquier otra transformación de la obra.
- c. Comunicar la obra al público mediante “representación, ejecución, radiodifusión o por cualquier otro medio”.

Sobre los derechos morales se señala:

“Artículo 30º.- El autor tendrá sobre su obra un derecho perpetuo, inalienable, e irrenunciable

para:

- a. Reivindicar en todo tiempo la paternidad de su obra y, en especial, para que se indique su nombre o seudónimo cuando se realice cualquiera de los actos mencionados en el artículo 12 de esta Ley.
- b. A oponerse a toda deformación, mutilación u otra modificación de la obra, cuando tales actos puedan causar o acusen perjuicio a su honor o a su reputación, o la obra sede merite, y a pedir reparación por esto;
- c. A Conservar su obra inédita o anónima hasta su fallecimiento, o después de él cuando asilo ordenase por disposición testamentaria;

d. A modificarla, antes o después de su publicación;

e. A retirarla de la circulación o suspender cualquier forma de utilización, aunque ella hubiere sido previamente autorizada”.

Los derechos patrimoniales se pueden negociar, pero a los derechos morales no se puede renunciar, ni pueden ser cedidos.

Figura 8. Copy Right



Fuente: segunda versión módulo de Derecho Informático, 2012.

El término Copyright proviene del derecho anglosajón, y se relaciona con el área patrimonial de los derechos de autor. El Copyright se circunscribe concretamente a la obra y no considera la relación de esta con su autor excepto por la paternidad de la misma.

Figura 8. Copy Left.



Fuente: segunda versión módulo de Derecho Informático, 2012.

El Copyleft es un concepto establecido por el movimiento GNU (acrónimo de GNU No es Unix), líder del Linux, que **se refiere a un método para hacer software libre o de código abierto**, que exige que todas las versiones del mismo sean también libres. La forma de lograrlo es ponerlo bajo dominio público, sin derechos de autor, o como se ha etiquetado “izquierdos de autor”.

Freeware, Shareware, Adware y Software Libre.

Las licencias convencionales corresponden al software privativo. El freeware es todo software que se distribuye gratuitamente bajo licencia GPL (General Public License), ejemplo Mozilla. El Freeware no tiene por qué ser libre, igual que el software libre no tiene por qué ser gratuito. El software libre se denomina así porque es de código abierto (open source), ejemplo Linux.

El shareware y **el adware** son variantes **del freeware**. El shareware se distribuye con limitaciones, como versión de demostración o evaluación. El adware es software gratuito al que se le incorpora normalmente publicidad, ejemplo el Messenger. (Aulaclac, 2005).

De clic sobre este enlace ara ampliar el tema del software libre.

“Tenga Presente: Los derechos de autor tienen dos contenidos; los derechos patrimoniales, que se pueden negociar, y los derechos morales, que son irrenunciables.”

4.2 TEMA 2 INFORMÁTICA FORENSE

De acuerdo a Canedo (2010), con el avance de la tecnología informática y su influencia en casi todas las áreas de la vida social y empresarial, el mundo ha ido evolucionando dándole innegables ventajas y comodidades, pero a su vez ha traído simultáneamente amenazas, riesgos e incertidumbre para las personas y organizaciones que las utilizan.

A medida que el uso del internet se ha extendido, ha aumentado el riesgo de su uso inadecuado. Los delincuentes cibernéticos viajan por el mundo virtual y realizan incursiones fraudulentas cada vez más frecuentes y variadas, como el acceso sin autorización a sistemas de información, piratería informática, fraude financiero, sabotaje informático y pornografía infantil, entre otros.

Pero además de los delincuentes informáticos, otros tipos de delincuentes han encontrado espacios propicios en los distintos medios de comunicación electrónica para desarrollar sus crímenes. Pedófilos, estafadores, falsificadores, defraudadores, secuestradores, proxenetas, traficantes de armas, de drogas, de personas, de pornografía, de información, sicarios y terroristas son algunos de los delincuentes que utilizan el ciberespacio y la red para multiplicar sus negocios, sus ilícitas ganancias y sus manifestaciones criminales.

Para enfrentar y descubrir delitos informáticos varios países han dispuesto un sistema judicial especializado (informática forense), que permite procesar y castigar dichos delincuentes. No obstante la informática forense es una herramienta judicial que debe ser manejada en base a rígidos principios científicos, normas legales y procedimientos con el fin de garantizar el debido proceso otorgando información veraz y confiable. En Colombia se estableció la ley

1273 de 2009, mediante la cual la legislación colombiana se equipara con la de otros países en cuanto a la normatividad sobre el delito informático.

La informática forense consiste en la investigación de los sistemas de información con el fin de detectar evidencias de la vulneración de los sistemas, por tanto, sirve para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información. La informática forense tiene una función preventiva y una probatoria, cuando la seguridad de la empresa ya ha sido vulnerada. Para realizar un adecuado análisis de Informática forense se requiere un equipo multidisciplinario que incluya profesionales expertos en derecho de las TIC y expertos técnicos en metodología forense. (Pérez, 2011).

Entre las múltiples técnicas y herramientas utilizadas por la informática forense podemos mencionar las siguientes. (López et al.)

- Evidencia Digital.
- Grabación en Medios Magnéticos.
- Análisis de Discos.
- Herramientas de Investigación Forense:
 - Herramientas para la Recolección de Evidencia. Herramientas para el Monitoreo y/o Control de computadores.
 - Herramientas de marcado de documentos.
 - Herramientas de hardware.

¿Cuál es la legislación sobre ataques informáticos en Colombia?

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

En una auditoría se puede incluir la informática forense como una herramienta importante a tener en cuenta dentro de una compañía, es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la

organización y utiliza eficientemente los recursos. La auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría.

El objetivo de un análisis forense es realizar un proceso de búsqueda detallada y minuciosa para reconstruir a través de todos los medios acontecimientos que tuvieron lugar desde el mismo instante cuando el sistema estuvo en su estado íntegro hasta el momento de detección de un estado comprometedor.

Según Guerrero (2009), Los objetivos fundamentales de la informática forense son bastante sencillas: la conservación, la identificación, la extracción, la documentación, y la interpretación de los datos informáticos. La informática forense está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y/o al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada y al extenso uso de computadores por parte de las compañías de negocios tradicionales. Es por esto que cuando se realiza un crimen, muchas veces la información queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que los computadores guardan la información de forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben realizar mecanismos diferentes a los tradicionales. Es de aquí que surge el estudio de la computación forense como una ciencia relativamente nueva.

En el análisis forense se debe realizar ciertos procedimientos que están enfocados a garantizar la integridad del proceso, hay que tener en cuenta que no únicamente se trata de riesgos que genera un atacante, sino de la importancia de poder examinar detalladamente la información que sea relevante y pueda ser almacenada, escondida, cifrada o suprimida en un dispositivo móvil, como llamadas realizadas, perdidas, imágenes, videos, mensajes etc, por medio de estos se logrará encontrar evidencia encontrar al sospechoso o las personas afectadas.

“

Traer a la memoria: La informática forense tiene doble función: preventiva y probatoria. Permite investigar los sistemas informáticos con el fin de prevenir atentados contra su seguridad e integridad, y probar hechos u omisiones cuando estos sistemas han sido vulnerados.

”

4.3 TEMA 3 PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES

La información es el activo más importante en las organizaciones. **La Cámara de Comercio de Bogotá** afirma lo siguiente:

La información es el activo más importante en el mundo actual, es por ello que el **17 de octubre de 2012** el Gobierno Nacional expidió la **Ley Estatutaria 1581 de 2012** mediante la cual se dictan disposiciones generales para la protección de datos personales, en ella se regula el derecho fundamental de hábeas data y se señala la importancia en el tratamiento del mismo tal como lo corrobora la Sentencia de la Corte Constitucional **C – 748 de 2011** donde se estableció el control de constitucionalidad de la Ley en mención. La nueva ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión (en adelante tratamiento) por parte de entidades de **naturaleza pública y privada**.

Este derecho como fundamental autónomo, requiere para su efectiva protección mecanismos que lo garanticen, los cuales no sólo han de depender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tengan la capacidad de fijar políticas públicas en la materia, sin injerencias de carácter político para el cumplimiento de esas decisiones.

Dentro de los contenidos mínimos que se desprenden del derecho de hábeas data se encuentra que las personas tienen la facultad de conocer – acceso – la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las mismas donde se encuentra dicha información; tienen además, el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular – salvo las excepciones previstas en la normativa –.

La Ley obliga a todas las entidades públicas y empresas privadas a revisar el uso de los datos personales contenidos en sus sistemas de información y replantear sus políticas de manejo de información y fortalecimiento de sus herramientas, como entidad responsable del tratamiento (persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos) deben definir los fines y medios esenciales para el tratamiento de los datos de los usuarios y/o titulares, incluidos quienes fungen como fuente y usuario, y los deberes que se le adscriben responden a los principios de la administración de datos y a los derechos –intimidad y hábeas data – del titular del dato personal.

Luego de presentar los antecedentes jurídicos, es clave entender que la información hoy en día es el activo más importante que se utiliza en todas las actividades cotidianas, como podemos evidenciar, el flujo de información se ha multiplicado en los últimos años llevando a un crecimiento acelerado del mismo, lo que implica que a mayor información circulando por el mundo globalizado en que nos encontramos se deben proteger velozmente los datos personales.

Certicámara de acuerdo a la **ley 1581 de 2012**. **Decreto 1377 de 2013**, define los siguientes conceptos así:

Datos personales

Lo define como cualquier información concerniente a personas físicas que tengan carácter privado, que esté ligada a su intimidad y que toque temas susceptibles de discriminación, como orientación sexual, religiosa, étnica, entre otros.

Importancia de los datos personales

Radica en que la información personal puede ser utilizada para varios fines, como la comercialización, la vida laboral, e incluso para cometer delitos, ya que su identidad puede ser suplantada si es que se tiene acceso a la información adecuada.

Protección de datos

Son todas las medidas que se toman, tanto a nivel técnico como jurídico, para garantizar que la información de los usuarios de una compañía, entidad o de cualquier base de datos, esté segura de cualquier ataque o intento de acceder a esta, por parte de personas no autorizadas.

Medidas se deben tomar para una efectiva protección de datos

Las medidas que se deben adoptar frente a la protección de datos dependen de la posición que se ocupe frente a la información, ya que puede estar a cargo de una persona física titular de la información; por otro lado, puede ser una persona natural o jurídica como encargada del tratamiento de datos y/o responsable del mismo.

¿Quién es el titular de la información?

Es la persona física cuyos datos son objeto de tratamiento.

Si usted es titular de la información debe:

-  Tener claridad de dónde se encuentran sus datos personales actualmente.
-  Saber quién custodia sus datos personales.
-  Conocer qué personas tienen acceso a su información personal.
-  Conocer los mecanismos legales con que puede defender sus derechos de información ante las entidades ya sean públicas o privadas.
-  Identificar sus bases de datos.
-  Entender que su información constituye un derecho y sobre ella usted tiene el poder

¿Quién es el responsable del tratamiento?

Es la persona natural o jurídica que decide sobre la base de datos o el tratamiento de datos, ya sea por si sola o en sociedad con otros.

Importante: si su empresa, realiza actividades como responsable del tratamiento de datos personales debe acondicionar e implementar los siguientes mecanismos:

- El aviso de privacidad.
- El procedimiento para obtener la autorización del titular previo al inicio del tratamiento.
- Herramientas que garanticen condiciones de seguridad adecuadas para evitar la adulteración, pérdida, consulta, uso o acceso fraudulento sobre la información.
- Medidas tecnológicas para proteger los datos personales y sensibles.
- Manual interno de políticas y procedimientos para cumplir con la Ley sobre protección de datos.
- Elaborar las políticas del tratamiento de la información y suministrarlas al registro nacional de bases de datos, el cual está a cargo de la Superintendencia de Industria y Comercio.

¿En qué consisten las sanciones?

Las sanciones para los encargados y los responsables del tratamiento de datos personales que pueden ser la misma persona natural o jurídica de naturaleza privada, están en cabeza de la Superintendencia de Industria y Comercio, y van desde:

- Multas de carácter personal o institucional hasta por 2.000 Salarios Mínimos Mensuales Legales Vigentes.
- Suspensión de las actividades relacionadas con el tratamiento hasta por seis meses.
- Cierre temporal de las operaciones relacionadas con el tratamiento.
- Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos.

“

Para tener en cuenta: la Ley 1581 del 17 de octubre de 2012, en su artículo 28 estableció un plazo de 6 meses para la implementación y adaptación de políticas por parte de las empresas que hagan las veces de encargados y/o responsables del tratamiento de datos.

”

4.3.1 EJERCICIO DE APRENDIZAJE UNIDAD 3 TEMA 4.1

1. La propiedad intelectual abarca dos dimensiones: la propiedad industrial y los derechos de autor. La propiedad industrial es un conjunto de derechos que puede poseer una persona física o una entidad jurídica sobre una invención, un diseño industrial, etc. Los derechos de autor es un conjunto de normas jurídicas y principios que afirman los derechos morales y patrimoniales que la ley concede a los autores por la creación de una obra literaria, artística, musical, científica, o didáctica, esté publicada o inédita. **Con base a lo anterior se puede afirmar que la propiedad industrial se patenta en el siguiente organismo técnico.**

- a. dirección nacional de derechos de autor.
- b. superintendencia de industria y comercio.
- c. resolución institucional.
- d. leyes del congreso reglamentadas por las organizaciones públicas o privadas.

Clave B

2. De acuerdo al concepto de lo que es el Derecho Informático, **los siguientes son algunos derechos fundamentales vulnerados particularmente en el uso de las tecnologías de la información y comunicación.**

- a. los derechos humanos en el ciberespacio
- b. delito informáticos definidos en la ley penal colombiana.
- c. acceso abusivo a un sistema informático
- d. derecho a la intimidad personal, familiar y al buen nombre.

Clave D

3. El derecho de autor se define como un conjunto de normas jurídicas y principios que enuncian los derechos morales y patrimoniales que la ley otorga a los autores. **Con base a lo anterior, los siguientes son tipos de derechos que son contenidos en los derechos de autor.**

- a. los derechos patrimoniales que se pueden negociar y los derechos morales, que son irrenunciables.
- b. los derechos humanos y el derecho a la libertad.
- c. el derecho a la libre expresión y a tener una vivienda adecuada.
- d. el principio de la universalidad de los derechos humanos y el principio de no discriminación.

Clave A

4. Es un derecho exclusivo de un autor para explotar una obra literaria, científica o artística durante un tiempo definido, proviene del derecho anglosajón y se relaciona con el área patrimonial de los derechos de autor. **Con base a lo anterior, esta afirmación hace referencia al siguiente término.**

- a. copyleft
- b. copyright
- c. freeware
- d. adware

Clave B

4.3.2 EJERCICIO DE APRENDIZAJE UNIDAD 3 TEMA 4.2

1. La informática forense se define como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. **Con base a lo anterior, las siguientes son herramientas y técnicas utilizadas en la informática forense.**

- a. freeware, shareware, adware, software libre.
- b. firma digital, copyleft, copyrigt, adware
- c. herramientas de hardware, análisis de discos, evidencia digital, herramientas para la recolección de evidencia.
- d. software libre, software gratuito, software de licenciamientos, herramienta digital.

Clave C

2. Con base al concepto de lo que es la Informática Forense, **para la realizar un adecuado análisis de procesos de informática forense se necesita un grupo interdisciplinario con las siguientes características.**

- a. profesionales expertos en derecho de las TIC y expertos técnicos en metodología forense.
- b. ingenieros de sistemas y expertos en informática general.
- c. profesionales expertos en informática básica y metodologías de aprendizajes.
- d. ingenieros de sistemas y expertos en metodologías de aprendizajes.

Clave A

3. La informática forense tiene doble función. Por una parte, permite investigar los sistemas informáticos con el fin de eludir atentados contra su seguridad e integridad, y demostrar hechos u omisiones cuando estos sistemas han sido vulnerados. Con base a lo anterior, esta doble función de la informática forense se conoce no los siguientes nombres.

- a. flexibilidad y confiabilidad

- b. preventiva y probatoria
- c. integridad y razonabilidad
- d. acusatoria y Acreditadora

Clave B

4.3.3 EJERCICIO DE APRENDIZAJE UNIDAD 3 TEMA 4.3

Estudiantes a repasar.

Defina informática forense.	Es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.
¿Para qué se usa la informática forense?	Sirve para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información.
¿mencione herramientas y técnicas utilizadas en la informática forense	<ul style="list-style-type: none"> • Evidencia digital. • Grabación de medios magnéticos. • Análisis de discos. • Herramientas de investigación forense. • Herramientas para la recolección de evidencia. • Herramientas para el monitoreo y/o control de computadores. • Herramientas de marcado de documentos. • Herramientas de hardware.
¿Cuáles son las funciones principales de la informática forense?	La informática tiene doble función: preventiva y probatoria . Permite investigar los sistemas informáticos con el fin de prevenir atentados contra su seguridad e integridad, y probar hechos y omisiones cuando estos sistemas han sido vulnerados.
¿Qué conocimientos se deben tener para realizar la investigación forense?	Se requiere de un equipo multidisciplinario que incluya profesionales expertos en derecho de las TIC y expertos técnicos en metodología forense. (Pérez, 2011).

<p>¿Cuál es la finalidad de la informática forense?</p>	<p>La finalidad es detectar evidencias de la vulneración de los sistemas, por tanto sirve para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de la información.</p>
<p>¿En qué momentos es necesario hacer uso de la informática forense y porque es necesario acudir a ella?</p>	<p>Cuando la seguridad de la empresa ya ha sido vulnerada, es necesaria para realizar un adecuado análisis.</p>
<p>¿Que facilita las metodologías utilizadas para la informática forense?</p>	<p>La gestión de la información.</p>

5 PISTAS DE APRENDIZAJE

Tener en cuenta: El Derecho puede entenderse como sistema jurídico, como ordenamiento jurisdiccional o desde la perspectiva de los “derechos”.

Tenga presente: La informática jurídica es la informática aplicada al derecho; el derecho informático es el derecho aplicado a la informática.

Traer a la memoria: Al considerarse la informática como objeto del derecho, estamos en el terreno del derecho informático.

Tener en cuenta: En la denominada “Sociedad Tecnológica” y particularmente en el llamado “Ciberespacio”, se presentan nuevos contextos para la garantía de los derechos humanos, de esta forma, los hechos sociales trazan nuevos caminos para el derecho.

Tenga presente: En la denominada “Sociedad Tecnológica” y particularmente en el llamado “Ciberespacio”, se presentan nuevos contextos para la garantía de los derechos humanos, de esta forma, los hechos sociales trazan nuevos caminos para el derecho.

Tener en cuenta que: El delito informático se puede presentar por el uso de la informática como medio o como fin. Ejemplo del primer caso es la suplantación de sitios web para obtener datos personales; del segundo, el daño informático.

Tener en cuenta: La informática forense tiene doble función: preventiva y probatoria. Permite investigar los sistemas informáticos con el fin de prevenir atentados contra su seguridad e integridad, y probar hechos u omisiones cuando estos sistemas han sido vulnerados.

Tenga presente: Los derechos de autor tienen dos contenidos; los derechos patrimoniales, que se pueden negociar, y los derechos morales, que son irrenunciables.

Tener en cuenta: El comercio electrónico es uno de los más grandes desarrollos de las TIC. En Colombia la Ley de Comercio Electrónico es la Ley 527 de 1999.

Traer a la memoria: La firma digital es un instrumento que garantiza tanto la autenticidad de un documento como la integridad del mismo; y tiene los mismos efectos que la firma escrita.

6 GLOSARIO

ADWARE: es software gratuito al que se le incorpora normalmente publicidad.

COPYLEFT: es un concepto establecido por el movimiento GNU (acrónimo de GNU No es Unix), líder del Linux, que se refiere a un método para hacer software libre o de código abierto, que exige que todas las versiones del mismo sean también libres.

COPYRIGHT: proviene del derecho anglosajón, y se relaciona con el área patrimonial de los derechos de autor

DELITO INFORMÁTICO: conducta ilícita que utiliza la informática como medio o como fin.

DERECHO INFORMÁTICO: Es el estudio de las tecnologías de la información y comunicación desde dos ejes, el primero de ellos estudia la tecnología como objeto del Derecho, y estudia la tecnología como instrumento del Derecho". (ACODITIC, 2010).

FREEWARE: es todo software que se distribuye gratuitamente bajo licencia GPL (General Public License).

INFORMÁTICA FORENSE: consiste en la investigación de los sistemas de información con el fin de detectar evidencias de la vulneración de los sistemas, por tanto, sirve para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información.

INFORMÁTICA JURÍDICA: es una técnica que tiene por objeto el estudio e investigación de los conocimientos aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica, necesaria para lograr dicha recuperación.

INGENIERÍA SOCIAL: conjunto de habilidades, técnicas, artilugios, tretas y engaños usados por cibercriminales para engañar a sus víctimas, de tal manera que revelen contraseñas u otra información que sirva para defraudarlas económicamente.

PROPIEDAD INTELECTUAL: abarca dos dimensiones: a) La propiedad industrial (que se patenta) y b) Los derechos de autor (que se registran).

SHAREWARE: Es un software que se distribuye con limitaciones, como versión de demostración evaluación.

PROTECCIÓN JURÍDICA DE LOS DATOS: la información como el activo más importante de las organizaciones.

7 BIBLIOGRAFÍA

- ACODITIC (Asociación Colombiana de Derecho Informático y de las Nuevas Tecnologías de la Información y las Comunicaciones). (2010). Recuperado el 18 de agosto de 2011, del sitio web: http://www.acoditic.org/main/index.php?option=com_content&view=article&id=54&Itemid=53
- AULACLIC. (2005). Recuperado el 19 de agosto de 2011, del sitio web: <http://www.aulaclic.es/articulos/licencias.html>
- Cámara de Comercio de Bogotá (2013). ABC para proteger los datos personales. Ley 1581 de 2012. Decreto 1377 de 2013. Recuperado de http://colombiadigital.net/publicaciones_ccd/anexos/certicamara_proteccion_datos_ago28.pdf
- Canedo, Alex. (2010). Revista Pensamiento Americano. N°4. Pág. 81-88. Recuperado de: <https://scholar.google.es/scholar?hl=es&q=la+informatica+forense+y+los+delitos+informaticos&btnG=&lr=>
- Chopan (2010). El aprendizaje a partir de dos ABP y el estudio de caso. Recuperado de <http://bchopan.blogspot.com.co/2010/09/el-aprendizaje-partir-de-los-abp-y-el.html>
- Cobo, J. (2009). El concepto de tecnología de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento. Recuperado de <http://www.ehu.eus/ojs/index.php/Zer/article/view/2636/2184>
- EcuRed, conocimiento de todos y para todos (2015). Derecho informático, Informatización del derecho. Recuperado de http://www.ecured.cu/Derecho_inform%C3%A1tico
- El espectador (2015). Sociedad del conocimiento. Recuperado de <http://www.elespectador.com/noticias/educacion/los-retos-de-sociedad-del-conocimiento-colombia-articulo-550902>
- Firma digital. Recuperado el 15 de agosto de 2011, del sitio web: http://www.kimaldi.com/area_de_conocimiento/firma_digital/conceptos_relacionados_con_la_firma_digital
- Guerrero, Paiva. (2009). Revista de Información Tecnología y Sociedad. N°3. Pág 105- 107. Recuperado de: http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442009000200025&script=sci_arttext&tlng=es
- Jiménez, D. (2010). Fundamentos de Derecho. El derecho como un sistema de normas. Recuperado de <http://fundamentosdederechouag.blogspot.com.co/2010/08/el-derecho-como-un-sistema-de-normas.html>
- López, H. et al. Informática forense: generalidades, aspectos técnicos y herramientas. Recuperado el 20 de agosto de 2011, del sitio web: http://gluc.unicauca.edu.co/index.php/P%C3%A1gina_principal

- Mintic. Recuperado de <http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf>
- Pérez, E. (2011). ¿Qué es la informática forense? Recuperado el 18 de agosto de 2011, del sitio web: <http://www.microsoft.com/es-es/business/>
- Petrella.(2007). Negocios electrónicos. Recuperado de <http://www.fing.edu.uy/catedras/disi/DISI/pdf/NEGOCIOS%20ELECTRONICOS.pdf>
- Servicio de Innovación Educativa Universidad Politécnica de Madrid. Recuperado de <http://maristas.org.mx/portal/sites/default/files/AprendizajeProblemas.pdf>
- Tato, N. (2010). El Derecho Informático como una nueva rama del derecho. Recuperado de http://www.nicolastato.com.ar/esp/index.php?option=com_content&view=article&id=6:artderechoinformaticonuevarama&catid=10:catgderechoinf&Itemid=7
- Torres, R. (2005). Sociedad de la Información / Sociedad del Conocimiento. Recuperado de <http://www.ub.edu/prometheus21/articulos/obsciberprome/socinfocon.pdf>