UTPL
La Universidad Católica de Loja

Vicerrectorado de Modalidad Abierta y a Distancia

Itinerario II-Derecho Privado: Derecho Informático

Guía didáctica

UTPL

Facultad Ciencias Jurídicas y Políticas

Itinerario II-Derecho Privado: Derecho Informático

Guía didáctica

Carrera	PAO Nivel
Derecho	VI

Autor:

Luis Oswaldo Ordóñez Pineda

DERE_3051

Universidad Técnica Particular de Loja

Itinerario II-Derecho Privado: Derecho Informático

Guía didáctica

Luis Oswaldo Ordóñez Pineda

Diagramación y diseño digital

Ediloja Cía. Ltda.
Marcelino Champagnat s/n y París
edilojacialtda@ediloja.com.ec
www.ediloja.com.ec

ISBN digital -978-9942-47-269-4

Año de edición: abril, 2025

Edición: primera edición

Loja-Ecuador

Índice

1. Datos de información

1.1 Presentación de la asignatura

1.2 Competencias genéricas de la UTPL

- Orientación a la innovación y a la investigación.
- Pensamiento crítico y reflexivo.

1.3 Competencias del perfil profesional

Relaciona fenómenos globales con la realidad jurídica nacional.

1.4 Problemática que aborda la asignatura

El sistema de administración de justicia presenta limitaciones en cuanto a sesgos de género y la implementación de políticas judiciales innovadoras. Además, el ejercicio profesional del abogado se ve afectado por una capacidad analítica y argumentativa reducida, consecuencia de una formación predominantemente positivista.

2. Metodología de aprendizaje

En el proceso de enseñanza-aprendizaje de nuestra asignatura aplicaremos algunos métodos que permitirán desarrollar los resultados de aprendizaje, a partir de un conjunto de procedimientos y recursos destinados a aclarar y comprender cada uno de los contenidos que se proponen. Así, con el objeto de que su aprendizaje sea satisfactorio y exitoso, se plantean las siguientes metodologías:

A. Aprendizaje basado en problemas: Desde los conflictos que plantean las tecnologías de la información y la comunicación en el ejercicio de los derechos de las personas, esta metodología apunta a estudiar estos problemas, a partir del reconocimiento de las distintas fuentes que se aplican en el Derecho Informático. De esta manera, relacionaremos los fenómenos jurídicos globales que, aplicables al mundo de las tecnologías, afectan a la realidad jurídica nacional.
B. Aprendizaje por indagación: Esta metodología permitirá desarrollar la innovación y la investigación de las instituciones jurídicas que se desprenden del Derecho Informático. Así, motivando el pensamiento crítico y reflexivo en los estudiantes, buscaremos reflexionar sobre los cambios y reformas que suscitan las tecnologías en las ciencias jurídicas.
C. Autoaprendizaje: Tomando en cuenta la modalidad de estudios, este método es transversal a todas las actividades que el estudiante debe desarrollar. Por ello, requiere que éste administre correctamente, su tiempo, por cuanto, la mejor manera de aprender es estudiando con responsabilidad, aprovechando los distintos recursos y herramientas que posibilitará el transcurso de esta asignatura, dentro de las actividades de aprendizaje.

Las técnicas que se emplearán se encuentran descritas en las actividades y recursos de aprendizaje del plan docente. Por ello, se sugiere revisar este instrumento, en lo que respecta a la descripción de la secuencia didáctica para el aprendizaje de la asignatura.



3. Orientaciones didácticas por resultados de aprendizaje

Primer bimestre

Resultado de aprendizaje 1:

Comprende los conceptos que se derivan del Derecho Informático.

Para alcanzar este resultado de aprendizaje, se exploran los conceptos fundamentales del Derecho Informático, incluyendo su marco normativo, regulaciones sobre el uso de la información digital y la protección de datos, con el fin de comprender su impacto en el ámbito legal y tecnológico.

Contenidos, recursos y actividades de aprendizaje recomendadas

Recuerde revisar de manera paralela los contenidos con las actividades de aprendizaje recomendadas y actividades de aprendizaje evaluadas.

Semana 1

Estimado estudiante, para comprender la naturaleza del Derecho Informático, principalmente, haremos un análisis teórico de las instituciones jurídicas relacionadas con el Derecho y la Informática. Así, considerando el concepto de transformación digital, abordaremos al “Derecho Informático” como una disciplina de las ciencias jurídicas, en la cual converge el estudio de la Informática Jurídica y el Derecho de la Informática.

A partir de los efectos que produce el desarrollo de las tecnologías de información y comunicación o “TICs” en la sociedad de la información, el Derecho Informático convierte a la Informática en un instrumento y objeto de

estudio. En este marco, se pretende alcanzar este resultado de aprendizaje, mediante el análisis de los distintos recursos de aprendizaje que dispone esta guía didáctica, vinculando, principalmente, el aprendizaje por indagación.

Sin duda, al final de este primer bimestre estará en condiciones de identificar y definir las instituciones jurídicas vinculadas con el Derecho Informático.

Unidad 1. Derecho y Tecnologías de la Información

1.1 Nociones preliminares

Para iniciar el estudio del primer tema planificado, es necesario reflexionar sobre algunas interrogantes. Por ejemplo, ¿Qué relación existe entre el derecho y la tecnología? ¿El derecho está destinado a regular el ámbito tecnológico?

Despejemos estas dudas, a través de la bibliografía básica, en donde encontrará una breve aproximación sobre la relación entre el Derecho y la Informática en la era de la "cuarta revolución". Le propongo analizar estos contenidos.

Una vez revisado dicho tema, se comprende que la sociedad ha experimentado diversos avances sociales, políticos, económicos y tecnológicos. Así, advertimos una nueva etapa denominada "cuarta revolución", la cual nace como producto de los avances experimentados en la "sociedad de la información" en la "era digital", afectando significativamente nuestras formas de comunicar, consumir, innovar y gestionar la información. En este aspecto, "conviene determinar con la mayor precisión posible cuáles son esas notas o características principales del mundo digital" (Riofrío Martínez-Villalba, 2014, p. 19).

El efecto de la transformación digital en el derecho se ha convertido en una de las áreas de estudio más importante de las ciencias jurídicas. Por ello, para designar el modelo de nuestras relaciones interpersonales, mediante el uso e implementación de TICs, alude, reiteradamente, a lo que hemos indicado como cuarta revolución". A partir de esta noción, "la sociedad tecnológica, que tiene

en la informática una de sus más características señas de identidad, plantea, por tanto, al jurista nuevos y complejos problemas" (Pérez-Luño Robledo, 2017, p. 37).

Recuerde, la abreviatura "TICs" es un término que va ligado al concepto de sociedad de la información, el cual alude para designar a las Tecnologías de la Información y Comunicación.

Entre los aspectos novedosos de las tecnologías, que reclaman la atención de los juristas, un lugar destacado ocupa la necesidad de abordar, por ejemplo, áreas relacionadas con los documentos electrónicos, los contratos electrónicos, el régimen jurídico de las bases de datos, el derecho de la *privacy*, los delitos informáticos y otras conductas nacidas del uso de los ordenadores y de las redes de transmisión de datos (Hernández, 2009).

Por ello, para comprender el objeto del Derecho Informático es esencial considerar que las ciencias jurídicas no pueden desentenderse de los avances que experimenta la sociedad, por cuanto, su funcionalidad está encaminada a proteger y garantizar los derechos individuales o colectivos, tanto para el hombre como la comunidad.

El efecto incuestionable de la transformación digital en el derecho se ha convertido en una de las áreas de estudio más importante de las ciencias jurídicas. Los sistemas jurídicos deben encaminarse a regular las tensiones respecto a la garantía de los derechos fundamentales en la era digital. Especialmente, emerge el respeto de la dignidad humana, tomando en cuenta que "se entiende por derechos digitales a los derechos humanos en entornos digitales" (Secretaría General Iberoamericana, 2023, p. 1).

Así, por ejemplo, "la transmisión de datos a través de las fronteras da origen a una nueva problemática jurídica, con repercusiones en el derecho privado y público" (García, 2011, p. 21). En todo caso, advertimos las infinitas posibilidades en la que las TICs buscan trascender y adaptar el ejercicio del derecho en la era digital, lo cual abre nuevas posibilidades y permite mejorar, tanto el acceso a la justicia como la administración pública.

Esta temática es interesante ¿verdad? Entonces, luego de haber abordado algunas cuestiones preliminares sobre la relación entre el Derecho y la Informática, a partir del concepto de transformación digital; lo invito a revisar la Carta Iberoamericana de Principios y Derechos en los entornos digitales.

Luego de la lectura del recurso antes mencionado, es necesario reflexionar sobre algunas interrogantes:

- ¿Cómo puede la cooperación iberoamericana fomentar el desarrollo de capacidades tecnológicas y reducir las brechas digitales, respetando las especificidades y soberanía de los países de la región?
- ¿Qué políticas públicas podrían implementarse para reducir las brechas digitales de género, edad y acceso en Iberoamérica, promoviendo la inclusión digital y la conectividad universal?

Interesantes preguntas ¿verdad? Seguro las propuestas a las mismas serán variadas como, por ejemplo, con respecto a la cooperación iberoamericana puede plantearse proyectos adaptados a necesidades y prioridades de cada país, garantizando sobre todo su independencia en la implementación.

También en la lectura que usted haga del recurso conocerá que dentro del ciberespacio, también, existen derechos y obligaciones. Al respecto, considere que la Carta Iberoamericana es un instrumento internacional de carácter declarativo y no vinculante, el cual pone de manifiesto el respeto de los derechos digitales, colocando a la persona en el centro de la transformación digital.

Si bien, se ha determinado la relación jurídica entre el derecho y las TICs, ahora es momento de conocer cuál es la rama de las ciencias jurídicas que se encarga de identificar estas conexiones. Vea a continuación:

1.2 Derecho Informático

Para comentar este apartado relativo a la esencia del "Derecho informático" dé lectura detenida a la bibliografía básica de la asignatura en el tema "Aproximaciones al derecho informático y los avances de las tecnologías de la información".

Luego de este análisis, habrá identificado la naturaleza jurídica del Derecho Informático. Ahora, realicemos algunas aproximaciones, sobre esta rama de las ciencias jurídicas.

En sentido general, entendemos que el Derecho puede concebirse como una "rama o especialidad de la disciplina jurídica dedicada al estudio de una parte o sector del ordenamiento jurídico" (RAE, 2024); y, que, además, la Informática constituye un "conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras" (RAE, 2024).

En principio, el efecto de las tecnologías es evidente, tomando en consideración las diversas dimensiones en las que se desarrollan las actividades del hombre, principalmente, mediante el apoyo de la informática y el empleo de la información.

Precisamente, en la era de la información digital, entendemos que una disciplina encargada de abordar la relación entre Derecho y la Informática es el Derecho Informático, por cuanto, esta rama de las ciencias jurídicas responde "a los problemas que la informática aporta como fenómeno multifacético" (García, 2011, p. 97).

En estos términos, nos parece que el siguiente vídeo permitirá aclarar las perspectivas relacionadas con el Derecho Informático. Se trata de un comentario desarrollado por el profesor Julio Téllez Valdés.

Muy llamativo ¿verdad? Desde esta perspectiva, Téllez (2004) entiende que el Derecho Informático es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática), (p.6).

En este contexto, en la era de las tecnologías emergentes o disruptivas es crucial reconocer la importancia del derecho informático, como una disciplina transformadora e interdisciplinaria de las ciencias jurídicas. Por ello, puede decirse que el derecho informático "no es más que una disciplina que se encarga de estudiar y regular las nuevas relaciones jurídicas que la informática y las TIC permiten en el mundo actual" (Pimentel Calderón & Cano, 2007, p. 7).

De las definiciones señaladas, concluimos que, por una parte, el Derecho Informático incluye un segmento teórico o normativo destinado a regular el uso de las TICs; y, por otra parte, un segmento práctico orientado a vincular la aplicación de las TICs en la actividad jurídica.

Nótese que las TICs plantean una labor impostergable a las ciencias jurídicas, por cuanto, "la influencia que aquélla está teniendo en el desarrollo y modernización de la sociedad ha llegado para quedarse y afecta a las empresas, pero, también, a los poderes públicos y a la sociedad en general" (De la Serna, 2021, p. 4). Por ello, el siguiente tema pondrá en evidencia cómo la informática afecta el desarrollo y modernización de la sociedad, particularmente, la administración pública.

¿Le ha parecido interesante?, seguro que sí. Ahora lo invito a revisar el siguiente tema.

1.3 Gobierno electrónico y Transparencia

¿Sabía que el concepto de administración pública digital está relacionado con el gobierno electrónico y la transparencia? En efecto, en el ámbito iberoamericano destacamos la trascendencia de la Carta Iberoamericana de Gobierno Electrónico de 2007, que entiende a las expresiones gobierno electrónico y administración digital como sinónimas.

Así, para identificar la naturaleza del "gobierno electrónico" y su relación con el principio de transparencia se sugiere revisar los temas previstos en la bibliografía básica de la asignatura, bajo el tema "Gobierno electrónico, administración pública y protección de datos personales en Ecuador".

A partir del análisis indicado, en principio, se desprende que "la digitalización de las administraciones, la interoperabilidad, la implementación telemática de procesos, el uso seguro de datos personales y un sistema de identificación digital fiable contribuyen a mejorar la calidad de los servicios públicos y de la eficiencia del Estado" (Secretaría General Iberoamericana, 2023, p. 14).

Sobre esta base, en nuestra región, destacamos la forma en la que Uruguay ha llegado a consolidar un modelo de gobierno electrónico, garantizando la seguridad jurídica en la transformación digital. Ha sido reconocido por el "Índice de Gobierno Digital de Naciones Unidas" (E-government Survey) como el país con mayor crecimiento de las Américas entre 2022 y 2024.

Por ello, a continuación, lo invito a revisar dos referencias que dan cuenta de este modelo:

- Transformación digital en Uruguay
- Posición de Uruguay en el índice global de gobierno digital

En este orden, resaltamos que el gobierno electrónico, también llamado *e-government,* "es un concepto de gestión que fusiona el empleo adecuado y acentuado de las tecnologías de la información y comunicación, con modalidades de gestión y administración, como una nueva forma de gobierno" (Téllez, 2008, p. 35).

La Ley Orgánica para la Transformación Digital y Audiovisual pone de manifiesto que uno de sus ejes es el gobierno digital, mediante la simplificación de trámites, la participación ciudadana por medios electrónicos, el gobierno de TIC y la identidad digital.

Por otra parte, tome en consideración que la Carta Iberoamericana de Gobierno Electrónico de 2007 reconoce como principios de la administración electrónica los siguientes:

1. Igualdad
2. Legalidad
3. Conservación
4. Transparencia y accesibilidad
5. Proporcionalidad
6. Responsabilidad; y,
7. Adecuación tecnológica

Particularmente, atendiendo el principio de transparencia, la Carta Iberoamericana de Principios y Derechos en entornos digitales precisa la importancia de fomentar "la transparencia, el acceso a la información pública y la rendición de cuentas de los gobiernos a través de las TIC, para promover y fortalecer una transformación digital de la sociedad" (Secretaría General Iberoamericana, 2023, p. 15). En este sentido, es importante destacar que la Ley Orgánica de Transparencia y Acceso a la Información Pública de Ecuador distingue cuatro categorías relacionadas con la transparencia. Para identificarlas, revisemos la siguiente infografía.

Categorías de Transparencia según la LOTAIP de Ecuador

Muy interesante la conceptualización que realiza dicha Ley, ¿verdad? En este sentido, hemos aclarado que las categorías relacionadas con la transparencia son la: activa, pasiva, colaborativa; y, focalizada. Al respecto, el siguiente vídeo de la Corte Constitucional de Ecuador le permitirá aclarar dichas categorías, particularmente, la transparencia pasiva.

Actividades de aprendizaje recomendadas

Es momento de aplicar su conocimiento a través de las actividades que se han planteado a continuación:

1. En la bibliografía básica, usted encontrará varias referencias a la "Carta Iberoamericana de Principios y Derechos en entornos digitales". La revisión de este documento le permitirá identificar la importancia de respetar los derechos y libertades en entornos digitales.

   Considerando este documento, además, se advierten importantes principios relacionados con la administración pública digital y, en todo caso, con el tratamiento de datos personales e identidad digital. Naturalmente, son temas que abordaremos a lo largo de este primer bimestre.

   En este orden, podría preguntarse si, ¿la Carta Iberoamericana es un instrumento internacional aplicable en nuestro país?

2. La doctrina y comunidad internacional advierten la aparición de los denominados "derechos digitales". Al respecto, le sugiero revisar el siguiente documento: La cuarta ola de derechos humanos: Los derechos digitales, en donde se debate la justiciabilidad de los derechos y libertades en los entornos digitales.

De la revisión de este documento, seguramente, nos preguntaremos, ¿se respetan los derechos digitales de las personas en Ecuador?

Semana 2

Unidad 1. Derecho y Tecnologías de la Información

1.4 Informática Jurídica

Para iniciar el estudio de este tema, demos una lectura a la bibliografía básica acerca de la Informática Jurídica. Por tanto, como una primera actividad relacionada con este tema, se sugiere revisar las partes que, a su criterio, sean las más trascendentales.

¿Le pareció importante? Estoy seguro que sí. Al respecto, destacamos que la Informática Jurídica se relaciona con la Cibernética, por cuanto, ésta tiene "el arte de construir, manejar aparatos y máquinas que mediante procedimientos electrónicos efectúan automáticamente cálculos complicados y otras operaciones similares (…) Tanto la informática como la cibernética tratan la información, por lo que la informática es un subconjunto o una parte de la cibernética" (García, 2011, p. 98). Por ello, apuntamos que, una de las líneas de investigación derivada del binomio derecho e informática es "la aplicación de la informática en el tratamiento de la información jurídica, conocida como informática jurídica" (Ríos Estavillo, 1997, p. 45).

En este orden de ideas, particularmente, el profesor Julio Téllez Valdés aborda la relación de los conceptos de cibernética, informática jurídica y ciberjusticia. Lo invito a revisar esta conferencia.

Ahora bien, de la revisión de las definiciones señaladas en la bibliografía básica, la doctrina aclara que la Informática Jurídica es "el conjunto de estudios e instrumentos derivados de la aplicación de la informática al derecho o, más precisamente, a los procesos de creación, aplicación y conocimiento del derecho" (Fix-Fierro, 1997, p. 56). En este sentido, la Informática Jurídica se evidencia en un ámbito, eminentemente, práctico

cuando el jurista (jueces, secretarios, oficiales mayores, abogados) utilizan las nuevas tecnologías como herramienta para procesar, automatizar, organizar y sistematizar información de contenido jurídico (Páez, 2015, p. 1).

Considerando que, en la era de la transformación digital es fundamental "perfilar las relaciones entre el derecho y la innovación de tal forma que la sociedad pueda aprovechar las oportunidades que la tecnología le ofrece para mejorar la vida" (De la Serna, 2021, p. 14); precisamente, las perspectivas que ofrece la informática jurídica "han dejado de ser una curiosidad para convertirse en herramienta de trabajo cotidiana e incluso imprescindible" (Fix-Fierro, 1997, p. 39).

Respecto a estas aclaraciones, nótese que siempre hacemos referencia al procesamiento, sistematización, organización o complicación de la información y, no de los datos. Por ello, conviene advertir que la Informática Jurídica "está destinada a trabajar con información, y no meramente con datos, y tal información surge cuando se ha logrado establecer una estructura para los datos" (García, 2011, p. 100).

En suma, puede decirse que, la informática jurídica subyace en el derecho informático, tomando en cuenta que aquella "tiene por objeto la aplicación de la tecnología de la información al derecho. Es una categoría bifronte en la que se entrecruzan una metodología tecnológica con su objeto jurídico que interesa a las distintas ramas o disciplinas tradicionales del derecho". (Pérez-Luño Robledo, 2017, p. 39).

Llegados a este punto, ¿le gustaría conocer las perspectivas o dimensiones que tienen relación con la Informática Jurídica? Para ello, lo invito a revisar el siguiente tema.

1.4.1 Clasificación y fuentes de la Informática Jurídica

Los contenidos relativos a la "clasificación de la informática jurídica" se encuentran, debidamente, ampliados en la bibliografía básica, en donde se detallan sus fuentes o clasificación. Por ello, se sugiere revisar e identificar las distintas dimensiones relacionadas con el tratamiento de la información jurídica.

En este orden, previo a aclarar las clases o perspectivas de la Informática Jurídica (documental; gestión; y, decisional), realicemos un breve resumen de lo que hasta ahora hemos puntualizado. Para ello le invito a revisar la siguiente infografía.

Derecho y Tecnologías de información

Pues bien, luego de haber puntualizado los conceptos que se derivan de la relación entre el Derecho y la Informática, a continuación, abordaremos la clasificación de la Informática Jurídica.

En general, la doctrina clasifica a la Informática Jurídica en: documental; de gestión; y, decisional. No obstante, también se considera la existencia de una Informática Jurídica registral y, metadecisional o metadocumental.

¿Interesante verdad? Ahora, revise algunas apreciaciones sobre esta clasificación.

A. **Informática jurídica documental**

Esta vertiente o rama de la informática jurídica parte del supuesto de "crear un banco de datos jurídicos (o corpus jurídico documentario) relativo a cualquiera de las fuentes del derecho (menos la costumbre) a efecto de interrogarlo con base en criterios propios acordes con esa información y su relevancia jurídica" (Téllez, 2008, p. 17). Por ello, se fundamenta en la creación o alimentación de bases de datos.

Así también, otra manera de describir a la informática jurídica documental es precisando que esta se refiere al "tratamiento automatizado de los documentos jurídicos, principalmente los derivados de la legislación, la jurisprudencia y la doctrina" (Fix-Fierro, 1997, p. 56). Por esta razón, también se denominan "bases de datos".

A modo de ejemplo, algunas referencias relacionadas con repositorios, bibliotecas virtuales, bases o bancos de datos (gratuitas o pagadas) constituyen modelos, en la práctica, de la informática jurídica documental.

En este contexto, ¿podría identificar un ejemplo en la práctica? Para identificar ejemplos de la informática jurídica documental, ingrese en la página de la biblioteca virtual de la UTPL y reconozca qué bases de datos jurídicas existen.

Luego de comprobar dichos ejemplos, usted puede conceptualizar que la informática jurídica documental almacena y ordena grandes cantidades de información jurídica. Naturalmente, tomando en cuenta que, "los grandes saltos sociopolíticos de la humanidad están relacionados con eventos tecnológicos o científicos, mismos que también han tenido fuerte impacto en el desarrollo de la ciencia del derecho" (García, 2011, p. 61). Para los juristas este paradigma exige aprender las diferentes formas de consultar, recuperar y aprovechar la información jurídica en entornos tecnológicos.

Para ilustrar mejor, en la bibliografía básica de la asignatura se describen los elementos estructurales de la organización, la búsqueda y la recuperación de la información jurídica. En este orden, puede advertirse que, en esta vertiente de la informática jurídica, la información debe ser tratada "por medio de la estructuración con la aplicación de la lógica o la argumentación para, posteriormente, mediante los instrumentos lingüísticos apropiados, incorporarla a la computadora" (Ríos Estavillo, 1997, p. 60).

B. **Informática jurídica de gestión**

Esta vertiente se caracteriza por ser, eminentemente, operacional en la gestión de las actividades jurídicas. Es decir, comprende "la utilización de las computadoras en la organización y administración de los órganos encargados de crear y aplicar el derecho" (Fix-Fierro, 1997, p. 57). Por ello, involucra el uso y aplicación de programas y tecnologías de la información y comunicación en todos los ámbitos jurídicos, tanto procesales como administrativos.

Con este antecedente, ¿podría identificar un ejemplo en la práctica?

Para identificar ejemplos de la informática jurídica de gestión, ingrese en la página del Consejo de la Judicatura y reconozca qué programas gestionan la información jurídica.

A partir de estos ejemplos, podemos aclarar que, en la actualidad, esta vertiente adquiere especial importancia, a partir de los principios relativos a la administración pública digital, por cuanto, "la simplificación y digitalización de los procesos y trámites administrativos, tanto internos como en relación con las personas usuarias de los servicios públicos, redunda tanto en la eficiencia de las administraciones públicas como en la facilitación del ejercicio de derechos y cumplimiento de deberes" (Secretaría General Iberoamericana, 2023, p. 14).

En este aspecto, entendiendo que esta dimensión de la informática jurídica tiene un fuerte componente operacional, su esencia conceptualiza la automatización o digitalización de "los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el derecho" (Pérez-Luño Robledo, 2017, p. 39).

Bajo estas consideraciones, se concluye que la informática jurídica de gestión abarca el tratamiento de la información vinculada a la administración cotidiana de las actividades jurídicas, por lo que, también, recibe el nombre de "ofimática" o "burocrática". En todo caso, promueve y fortalece la transformación digital, particularmente, en la administración de justicia.

C. **Informática jurídica decisional**

Esta fuente de la informática jurídica representa la aplicación de sistemas lógicos o programas, a través de la implementación de inteligencia artificial y sistemas jurídicos expertos, facilitando la toma de decisiones en el ámbito jurídico. De esta manera, "permite resolver problemas en un dominio específico mediante la simulación de los razonamientos que los expertos del sistema harían si utilizaran los conocimientos adquiridos" (Téllez, 2008, p. 27).

Así, considerando que esta perspectiva de Informática Jurídica "se halla integrada por los procedimientos dirigidos a la sustitución o reproducción de las actividades del jurista; a proporcionarle decisiones y dictámenes" (Pérez-Luño Robledo, 2017, p. 41), su desarrollo tiene que "estar guiado por un propósito y un criterio jurídico previamente definidos (en el sistema), por ello debemos entender que el lenguaje del derecho lleva en estos procesos de construcción de la información, todos los rasgos que le son propios" (García, 2011, p. 101).

En este orden de ideas, la doctrina entiende que "uno de los sectores más dinámicos y en constante evolución de la Informática jurídica metadocumental o decisional es el que se refiere a la aplicación al Derecho de la inteligencia artificial y los sistemas expertos" (Pérez-Luño Robledo, 2017, p. 41)

Según la RAE (2024), la Inteligencia Artificial (IA) es "una disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico".

Estas cuestiones son muy apasionantes, ¿verdad? Por ello, lo invito a identificar en la bibliografía básica de la asignatura los ejemplos de sistemas expertos y el uso de inteligencia artificial en el Derecho. En esta

revisión, particularmente, llaman la atención los simuladores o sistemas expertos del Ministerio del Trabajo en Ecuador; y, en todo caso, el uso de ChatGPT en la administración de justicia.

Luego de esta revisión, es importante reflexionar que la inteligencia artificial y el poder sobre las tecnologías son del hombre. “En la actualidad no es posible, ni deseable, una suplantación plena del razonamiento jurídico del juez o del abogado por el cálculo informático del ordenador” (Pérez-Luño Robledo, 2017, p. 41). Por ello, se asume que en la actividad de razonamiento de los juristas resulta imposible que una computadora desplace a la persona. En todo caso, “si se lograra la automatización de las inferencias y decisiones judiciales, esto pone en evidencia la importancia de impulsar transformaciones conceptuales de relevancia tanto en la teoría de la decisión judicial, como en la informática” (García, 2011, p. 100).

Recientemente, la Corte Constitucional de Colombia ha reflexionado sobre el uso de IA en la administración de justicia. Por ello, le recomiendo revisar la sentencia T-323/24, la cual señala algunos criterios para el uso de IA en los despachos judiciales.

Naturalmente, estos casos ponen de manifiesto que, si bien el uso de esta herramienta de inteligencia artificial es una cuestión polémica, “la inteligencia artificial puede ser un instrumento más de apoyo en la argumentación y motivación, que incluso sirva para su mejora sin menoscabo del debido proceso” (Asís, 2022, p. 118). En este plano, “es imprescindible impulsar, además, un equilibrio entre las decisiones judiciales y la informática, con miras a la construcción del conocimiento jurídico (García, 2011, p. 100).

Como hemos evidenciado hasta esta parte, la incidencia de la Inteligencia Artificial en el derecho puede parecer un tema muy polémico. Por ello, lo invito a revisar los siguientes temas.

1.5 Inteligencia Artificial y Derecho

¿Sabía que la inteligencia artificial es considerada como una tecnología emergente? Efectivamente, para profundizar este apartado se sugiere revisar la bibliografía básica de la asignatura en el tema “Inteligencia artificial y Derecho”.

De las reflexiones que se señalan, se podrá advertir que una referencia importante a este tema es la “Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO”.

Precisamente, entendiendo que un Sistema de Inteligencia Artificial es un sistema basado en “una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales” (Reglamento UE, 2024); la Recomendación de la UNESCO (2022) reconoce que la IA puede suscitar, por ejemplo, “preocupaciones éticas fundamentales, por ejemplo, en relación con los sesgos que pueden incorporar y exacerbar, lo que puede llegar a provocar discriminación, desigualdad, brechas digitales y exclusión y suponer una amenaza para la diversidad cultural, social y biológica” (p. 5)

En este orden, surgen serios desafíos tanto éticos como legales por la forma en la que la IA pueda llegar a afectar los derechos y libertades de las personas. Así, desde la perspectiva iberoamericana se ha manifestado la condición de “abordar conjuntamente las cuestiones asociadas a las tecnologías emergentes, así como su uso seguro, ético y responsable” (Secretaría General Iberoamericana, 2023, p. 18).

Así también, otra perspectiva de los efectos de la IA puede ser abordada desde el ámbito de la administración pública. Al respecto, la Carta Iberoamericana de Inteligencia Artificial en la Administración Pública (2023) enfatiza en la necesidad de “incorporar de una manera responsable las tecnologías

emergentes en todas las entidades del sector público, así como promover su uso en otros ámbitos sociales, culturales, económicos, políticos, etc., aprovechando sus oportunidades y minimizando sus potenciales riesgos, al mismo tiempo que se preservan los derechos humanos de todas las personas" (p. 5).

Sobre esta base, le invito a revisar la siguiente infografía, donde podrá reflexionar sobre los principios fundamentales de los sistemas de inteligencia artificial, conforme a las recomendaciones de la UNESCO sobre ética en la IA. Además, conocerá los desafíos que supone su implementación en la Administración pública, según lo establecido en la Carta Iberoamericana de Inteligencia Artificial.

Principios y desafíos en el desarrollo de la IA

Como queda expuesto, la IA ejerce influencia, particularmente, en las interacciones humanas y en la toma de decisiones frente a los distintos procesos sociales, económicos, políticos y jurídicos. Así, como hemos señalado en Puertas-Bravo et. al (2024) no se discute las repercusiones positivas y dinámicas que la IA ofrece al desarrollo y al cambio dentro de dichos escenarios. Particularmente, "los avances de la informática moderna han ampliado enormemente la capacidad de detectar patrones subyacentes en los datos. Los algoritmos de IA pueden inferir fácilmente nuevos conocimientos sobre las personas" (Solove, 2024, p. 30).

Interesantes anotaciones. Ahora, tal como ha advertido la Carta Iberoamericana de Inteligencia Artificial en la Administración Pública (2023) un desafío es la garantía "de los derechos de los seres humanos en su interacción con las *neurotecnologías*, estableciendo los controles necesarios de los dispositivos y sistemas utilizados en cada caso, y analizando las consecuencias de la ampliación de capacidades mentales y físicas (transhumanismo)" (p. 12). Por ello, lo animo a reflexionar sobre el siguiente tema.

1.6 Derechos humanos y Neurotecnologías

¿Ha tenido conocimiento de algún instrumento internacional que aborde, particularmente, los conceptos de neurotecnología y derechos humanos? Precisamente, en la bibliografía básica de la asignatura hemos destacado algunas referencias sobre este tema. Por ello, se sugiere revisar estos contenidos que se desarrollan en el primer capítulo de dicha bibliografía.

A partir de esta revisión, notará que en el ámbito internacional trasciende la Declaración de Principios Interamericanos en materia de Neurociencias, Neurotecnologías y Derechos Humanos, elaborada por el Comité Jurídico Interamericano de la OEA, la cual, considerando el desarrollo de tecnologías emergentes, revela la importancia de atender los avances de las neurotecnologías o computación cuántica.

Respecto a este tema, en principio, la Agencia Española de Protección de Datos (2023) advierte que las neurotecnologías "permiten la recolección de datos neurológicos o neurodatos que, en cuanto asociados a personas identificadas o identificables, son datos personales. Con análisis avanzados y uso de Inteligencia Artificial podrían inferir y revelar información asociada a pensamientos, sentimientos o estados de salud, además de perfilar al individuo".

Desde esta perspectiva, se subraya la necesidad de contar con preceptos que protejan "la dignidad, la no discriminación, la identidad, el derecho a la privacidad e intimidad, la salud física y mental, la prohibición de la tortura y los tratos crueles, inhumanos y degradantes, y el acceso a remedios judiciales, entre otros" (OEA, 2023, p. 1). Así, por lo que precede, surgen los denominados neuroderechos, que "pueden definirse como las exigencias y pretensiones éticas que pretenden proteger y preservar la mente y el cerebro de las personas" (Asís, 2022, p. 131).

Como puede evidenciar, se trata de un tema novedoso y, eminentemente, actual en el ámbito del derecho de la informática. Por esta razón, en esta parte, se propone realizar una lectura de la Declaración de Principios Interamericanos en materia de Neurociencias, Neurotecnologías y Derechos Humanos. Habiendo revisado este documento, llama la atención el principio relativo a que los datos neuronales son datos sensibles.

Por ello, lo invito a revisar las siguientes definiciones y comentarios:

Protección de datos neuronales

A partir de estas referencias relacionadas con datos neuronales y datos sensibles, desde la perspectiva de la Declaración de Principios Interamericanos en materia de Neurociencias, Neurotecnologías y Derechos Humanos, seguramente, le habrá llamado la atención que se invoquen los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales de la OEA.

No se preocupe, más adelante profundizaremos este instrumento, tomando en cuenta su particular conexión con el derecho a la protección de datos personales.

Actividades de aprendizaje recomendadas

Es hora de reforzar los conocimientos adquiridos resolviendo las siguientes actividades:

1. Con el objeto de identificar el marco de la clasificación de la Informática Jurídica, se sugiere revisar el siguiente documento: Informática Jurídica, capítulo tercero, en el cual se describen los principales escenarios que materializan la aplicación de esta vertiente del Derecho Informático.

En el análisis de este documento, se evidencia que la Informática Jurídica presenta algunas vertientes o fuentes, relacionadas con los documentos, la gestión y la toma de decisiones. En este contexto, el problema que se quiere resolver es la necesaria distinción que afecta al Derecho Informático, tanto en relación a la Informática Jurídica como del Derecho de la Informática.

2. Considerando la incidencia de la inteligencia artificial y las neurotecnologías en los derechos y libertades fundamentales de las personas, se sugiere revisar los siguientes vídeos sobre El implante cerebral de Neralink y Neuroderechos y la privacidad mental.

   A partir de estos recursos, precisamente, se resalta la importancia de atender el paradigma de los neuroderechos y la inteligencia artificial, a la luz de los avances de las neurociencias, neurotecnologías y derechos digitales. En esta línea, existen varias interrogantes, que como estudiantes de derecho deberíamos realizarnos. Por ejemplo:

   - ¿Cómo garantizar el consentimiento en sistemas de IA que analizan datos biométricos o cerebrales?
   - ¿Cómo prevenir el uso indebido de interfaces cerebro-computadora que podrían manipular pensamientos o decisiones?
   - ¿Qué mecanismos regulatorios deben crearse para supervisar el desarrollo y la implementación de IA y neurotecnologías?

3. De esta manera, hemos llegado a la parte final de esta unidad. Espero que los temas aquí expuestos hayan sido de su agrado. Ahora es momento de medir su nivel de conocimientos. A continuación, le propongo resolver las siguientes interrogantes.

Autoevaluación 1

A partir de los enunciados que se proponen, escoja la respuesta correcta:

1. La Informática Jurídica consiste en el:

   a. Aseguramiento de datos o evidencias.
   b. Tratamiento de la información jurídica por medios electrónicos.
   c. Análisis de la privacidad informática.

2. La Informática Jurídica se relaciona, especialmente, con la:

   a. Cibernética.
   b. Ciberseguridad.
   c. Cibercriminalidad.

3. El Derecho de la Informática conceptualiza la:

   a. Normativa destinada a regular el uso de las tecnologías.
   b. Profesión jurídica asistida de tecnologías.
   c. Acción de la informática en la actividad de los operadores jurídicos.

4. El fundamento de la informática jurídica documental corresponde a:

   a. Bases de datos.
   b. Software de gestión jurídica.
   c. Inteligencia artificial.

5. El fundamento de la informática jurídica decisional corresponde a:

   a. Neurotecnologías.
   b. Software de gestión jurídica.
   c. Sistemas expertos e inteligencia artificial.

6. En el derecho informático, el derecho de la informática se vincula como un:

   a. Instrumento de aplicación.
   b. Objeto de estudio.
   c. Derecho a acceder a Internet.

7. La informática jurídica documental, entre otras disciplinas, incluye una relación con la:

   a. Informática Registral.
   b. Informática Forense.
   c. Lógica o argumentación.

8. La informática jurídica decisional enfrenta problemas relacionados con la:

   a. Digitalización de trámites administrativos.
   b. Ofimática.
   c. Toma de decisiones.

9. En el gobierno electrónico, una categoría relacionada con la transparencia es la:

   a. Proporcionalidad.
   b. Colaborativa.
   c. Adecuación tecnológica.

10. A partir de los conceptos de neurotecnologías e inteligencia artificial subyace la protección de la:

    a. Privacidad e intimidad.
    b. Rendición de cuentas.
    c. Transparencia pasiva.

Ir al solucionario

¡Ahora, continuemos con la revisión de la siguiente Unidad!

Resultado de aprendizaje 2:

Aplica el Derecho de la Informática en las relaciones jurídicas que se derivan de la sociedad de la información.

Dado el carácter amplio que representa el objeto de estudio del Derecho Informático, abordaremos las distintas áreas o campos que afecta esta rama del Derecho. De tal manera que, mediante un estudio pormenorizado —desde una perspectiva legal, doctrinal y jurisprudencial— del comercio electrónico, firma electrónica, documentos electrónicos, contratación electrónica y protección de datos personales, aplicaremos a la realidad jurídica nacional estas relaciones, a partir de los fenómenos globales que se derivan de la sociedad de la información.

En este marco, se alcanzará este resultado de aprendizaje, mediante el análisis de los distintos recursos de aprendizaje que dispone en esta guía didáctica, vinculando principalmente, el aprendizaje basado en problemas. Sobre esta base, al final de este primer bimestre estará en condiciones de aportar, considerar, argumentar y aplicar, dentro del marco jurídico nacional, el Derecho de la Informática.

Contenidos, recursos y actividades de aprendizaje recomendadas

Semana 3

Unidad 2. Derecho de la Informática: e-commerce, firmas y contratos

2.1 Comercio electrónico

En principio, esta Unidad está dedicada a examinar algunas instituciones jurídicas que se derivan del uso de las TICs, las cuales, naturalmente, se regulan dentro del sistema jurídico ecuatoriano, atendiendo a los principales

instrumentos jurídicos que, en materia internacional, se han creado para fijar criterios uniformes y equilibrar las relaciones jurídicas en la sociedad de la información.

Al respecto, ¿se ha preguntado qué validez jurídica tienen los contratos que se realizan por la vía del comercio electrónico? Por ello, en esta primera parte, desde el Derecho de la Informática, se enfocará el estudio del comercio electrónico y los documentos electrónicos, a la luz de la multidisciplinariedad de la regulación de las tecnologías de la información y comunicación, considerando, naturalmente, el paradigma asociado con la protección de los derechos y libertades fundamentales en los entornos digitales.

Como introducción a este tema, en la bibliografía básica encontrará los antecedentes respecto al desarrollo del denominado "*e-commerce*". Particularmente, una conceptualización importante es la que realiza la "Carta Iberoamericana de Principios y Derechos en los Entornos Digitales", la cual considera que —a partir del principio de economía digital justa, inclusiva y segura— el comercio electrónico debe ofrecer un adecuado "grado de protección de las personas consumidoras y usuarias en los entornos digitales" (Secretaría General Iberoamericana, 2023, p. 17).

En este orden, destacamos la importancia de garantizar el intercambio electrónico de datos (*EDI o electronic data interchange*), el cual, sistematizado en el ámbito del comercio y transacciones electrónicas, "sustituye el soporte papel de los relacionados comercialmente (órdenes de compra, remisión, facturas, listas de precios, etcétera) a través de transacciones electrónicas con formatos normalizados y acordados previamente entre los usuarios del servicio" (García, 2011, p. 58).

Malca (2001) conceptualiza al comercio electrónico como el "uso de las tecnologías de la informática y las telecomunicaciones, que soportan las transacciones de productos o servicios entre las empresas, entre estas y particulares o con el Estado" (pág. 33).

Sobre esta base, el concepto de comercio electrónico emerge como una noción derivada, tanto de la transformación como de la economía digital y, en todo caso, de las problemáticas que subyacen en el derecho de la informática. En estos términos, ahora observe algunas características relacionadas con las ventajas del comercio electrónico, las cuales le permitirán identificar su naturaleza, además, de las posibilidades y los riesgos que supone el uso y la aplicación de este servicio de la sociedad de la información. Preste atención a la siguiente tabla:

Tabla 1
Características del Comercio Electrónico.

	CARACTERÍSTICAS
COMERCIO ELECTRÓNICO	Reduce las barreras de acceso a los mercados actuales.
	Establece nuevas formas, más dinámicas, de cooperación entre empresas.
	Abre oportunidades de explotar mercados nuevos.
	Para el consumidor, amplía su capacidad para acceder a prácticamente cualquier producto.
	Reduce o elimina por completo los intermediarios, por ejemplo, en la venta de productos en soporte electrónico.
	Genera la necesidad de llegar a acuerdos internacionales que armonicen las legislaciones sobre comercio.

Nota. Ordóñez, L., 2025.

¿Le pareció importante este tema? Estoy seguro que sí. Ahora, luego de haber contextualizado la importancia y características del comercio electrónico, a continuación, identificaremos una definición concreta sobre esta institución jurídica, a la luz del ámbito nacional e internacional.

En primer término, reconocemos que en nuestro país la norma que regula las relaciones que se producen dentro del comercio electrónico es la Ley de Comercio de Electrónico, Firmas y Mensajes de Datos —en adelante LCE— aprobada en 2002. Esta norma, en su parte final (Novena Disposición General - Glosario de términos) precisa que el comercio electrónico es "toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información". En este orden, la LCE se presenta como una norma que posibilita a los ciudadanos contar "con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales" (LCE, 2002).

Ahora bien, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) lo define como "la venta o compra de bienes o servicios que se realiza a través de redes informáticas con métodos específicamente diseñados para recibir o colocar pedidos" (OCDE, 2019, pág. 17). Por tanto, el comercio electrónico, también llamado *electronic commerce* o *e-commerce*, supone para el derecho un cambio de paradigma, que exige concretar en los ordenamientos jurídicos unas condiciones y principios básicos orientados a garantizar la seguridad jurídica de las transacciones en los servicios de la sociedad de la información.

De esta manera, se entiende que la LCE se deriva como una herramienta jurídica necesaria e indispensable, que permite establecer un marco de seguridad jurídica, en general, para los negocios que se desarrollen por vía electrónica. Esto, se desprende del objeto de dicha norma, toda vez que se encamina a regular "los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas" (LCE, 2002).

Justamente, en principio, un elemento importante en el marco del comercio electrónico es el intercambio de datos, el cual debe sistematizar ciertos niveles de confianza que atribuyan seguridad, tanto jurídica como técnica, a la

transferencia de datos, mediante formatos electrónicos. De este modo, hacemos referencia a los documentos electrónicos como un instrumento que facilita la economía digital. En estos términos, revisemos el siguiente tema.

2.2 Documentos electrónicos

El contenido relativo a los "documentos electrónicos" se encuentra desarrollado en bibliografía básica, en donde se recalca la importancia de que, tanto en el ámbito público como privado, se debe priorizar el uso de medios telemáticos. Especialmente, aparece el documento electrónico, el cual es una figura que permite "pasar de los medios tradicionales, como documentos en papel, al manejo de información en un alto porcentaje a través de datos electrónicos procesados en herramientas TIC" (Oropeza, 2018, p. 29).

Con este antecedente, debemos preguntarnos ¿qué es un documento electrónico? En principio, la RAE (2024) entiende que un documento electrónico es "todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual". Así, además, la doctrina entiende que es aquel "en que la actividad de una computadora o de una red sólo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes" (Téllez, 2008, p. 292).

Frente a estos supuestos, ¿un documento electrónico tiene el mismo valor jurídico que un documento escrito? Al respecto, es conveniente identificar la trascendencia del principio de equivalencia funcional en el marco de los documentos electrónicos.

Precisamente, en la bibliografía básica se advierte que, al tenor de este principio, el documento electrónico tiene el mismo valor jurídico que un documento escrito, incluso —atendiendo la Guía para la incorporación al derecho interno de la "Ley Modelo sobre Comercio Electrónico", aprobada por la Comisión de las Naciones para el Derecho Mercantil Internacional— se aclara que "puede ofrecer un grado de seguridad equivalente al del papel y, en

la mayoría de los casos, mucha mayor fiabilidad y rapidez, especialmente respecto de la determinación del origen y del contenido de los datos" (LMCE, 1999, p. 21).

En estos términos, frente a las nociones, tanto de transformación digital como de economía digital, que hemos resaltado, el documento electrónico, en principio, tiene que responder, entre otras cuestiones, a las normas de inalterabilidad, autenticidad, fe púbica y seguridad, para que determinada representación o manifestación de la voluntad pueda tener efectos legales. Lógicamente, para ello debe estar amparado en un reconocimiento expreso dentro del ordenamiento jurídico.

Así, atendiendo al Art. 2 de la LCE, se reconoce que los mensajes de datos tienen igual valor jurídico que los documentos escritos. En este escenario, ¿es lo mismo un mensaje de datos que un documento electrónico? Sobre este aspecto, el "Glosario de términos" de la LCE aclara que "serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos".

Recuerde, la LCE describe que un mensaje de datos es "toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio".

Desde otra perspectiva, el documento electrónico vincula, necesariamente, el desarrollo y la estructuración de un sistema de información. Por ello, además, el "Glosario de términos" de la LCE, agrega que un sistema de información es "todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos".

Finalmente, queda por señalar que un ejemplo de documento electrónico encaja en lo que, habitualmente, se conoce como una factura electrónica, por cuanto, atendiendo el "Glosario de términos" de la LCE, la "factura electrónica"

se define como el “conjunto de registros lógicos archivados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos que documentan la transferencia de bienes y servicios”.

Desde esta óptica, “bajo documento electrónico se consideran datos o informaciones que tienen relevancia jurídica, los cuales son transmitidos o registrados por vía electrónica, especialmente a través del procesamiento electrónico de datos, pero también por medio de simples soportes de sonido” (Téllez, 2008, p. 295). Por ello, enfatizamos que “tres son, pues, los elementos que se han de tener en cuenta para su caracterización: Se trata de una cosa material; tiene una finalidad representativa; y, en litigio, se utiliza como medio probatorio” (García, 2011, p. 107).

El art. 52 de la LCE contempla que “los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta Ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba”.

De esta manera, hemos destacado que, por una parte, la validez y reconocimiento del documento electrónico responde al principio de equivalencia funcional. Finalmente, por otra, considerando las exposiciones que se señalan en la bibliografía básica, el documento electrónico puede tener la calidad de medio probatorio, por tanto, “al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje” (LMCE, 1999).

Hasta aquí, hemos considerado la naturaleza de los documentos electrónicos y los elementos que caracterizan su reconocimiento. Ahora, en esta parte, corresponde determinar sus condiciones de validez jurídica. Revise las siguientes anotaciones:

1. El documento electrónico, configurado en un mensaje de datos, tienen igual valor jurídico que los documentos escritos, por tanto, “la adopción de este criterio del equivalente funcional no debe dar lugar a que se impongan

normas de seguridad más estrictas a los usuarios del comercio electrónico (con el consiguiente costo) que las aplicables a la documentación consignada sobre papel" (LMCE, 1999).

2. Al constituirse como un medio probatorio, conforme los dispone la LCE (2002), al presentarse un mensaje de datos dentro de un proceso judicial, se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación, cuando sean requeridos.

Finalmente, es preciso apuntar que el documento electrónico se encuentra íntimamente vinculado con la firma digital, por cuanto, ésta es la que transforma en realidad la posibilidad de obviar el papel escrito por el medio electrónico, firmado un documento con las debidas garantías de integridad y solemnidad. Por ello, se entiende que, al igual que los documentos escritos, un documento electrónico "puede ser atribuido a una persona determinada en calidad de autor mediante una forma digital, clave o llave electrónica" (García, 2011, p. 121).

Actividades de aprendizaje recomendadas

En esta parte continuaremos con su aprendizaje mediante su participación en las actividades que se describen a continuación:

1. Considerando que algunos países, para la elaboración del marco legal sobre comercio electrónico, la Ley Modelo de la CNUDMI sirvió de referencia, en este documento encontrará el texto de la normativa aprobada por la Comisión de las Naciones para el Derecho Mercantil Internacional

   Mediante el análisis de esta Ley Modelo o Guía para la incorporación de las disposiciones relativas al comercio electrónico, en los ordenamientos jurídicos internos, usted podrá comparar y determinar si la LCE, en Ecuador, reúne las condiciones jurídicas para enfrentar esta actividad, en la actualidad.

2. En la obra denominada: Derecho de las nuevas tecnologías - Capítulo tercero (Parte 1), sobre el documento electrónico se aborda la problemática jurídica que se desprende del valor probatorio de los documentos electrónicos. Pese a ser una cuestión que en el derecho comparado se encuentra resuelta; al parecer en nuestro país, tanto en el ámbito público como privado, persisten las dudas sobre la validez probatoria de estos documentos.

En este orden, el caso que intentamos resolver es, si en nuestro ordenamiento jurídico, conjuntamente con la LCE, existen otras disposiciones relativas que aseguren el reconocimiento de los documentos electrónicos. Para este fin, se sugiere revisar algunas normas conexas como: el Código Orgánico de la Función Judicial; el Código Orgánico Integral Penal; y el Código Orgánico General de Procesos.

Contenidos, recursos y actividades de aprendizaje recomendadas

Semana 4

Unidad 2. Derecho de la Informática: e-commerce, firmas y contratos

2.3 Firma electrónica

Como se puede evidenciar, el desarrollo del comercio electrónico ha concretado, tanto en el sector público como privado, la necesidad de establecer parámetros de seguridad. Así, en el marco de la transformación digital, la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales recomienda trabajar en "sistemas de autenticación y uso de firmas digitales que aseguren la integridad de los documentos digitales, dotándolos de mayor seguridad tanto técnica como jurídica" (Secretaría General Iberoamericana, 2023, p. 15).

La idea, en este plano es que "el medio electrónico utilizado para enviar o generar la información, sea un método confiable, ya que, si no lo fuera, la validez de dicha información se vería disminuida" (García, 2011, p. 127). Por

ello, a diferencia de las seguridades que en el mundo físico se exige a todo documento, en el ciberespacio se plantea la necesidad de incorporar ciertas medidas de seguridad, las cuales resultan de la aplicación de la firma electrónica. Es decir, es imprescindible "contar con tecnología que brinde la seguridad física y jurídica, a fin de poder atribuirle a la persona (el emisor), lo que se resuelve con la firma electrónica avanzada, con las llaves pública y privada" (García, 2011, p. 127).

Nótese que la Carta Iberoamericana utiliza el sintagma firma digital para referenciar a la garantía técnica de integridad de los documentos electrónicos o digitales.

De esta manera, en sentido general, se entiende que la firma electrónica es "un conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante" (RAE, 2024). Por ello, esta expresión "alude a cualquier método o símbolo basado en medios electrónicos utilizados o adoptados por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas las funciones de la firma manuscrita" (García, 2011, p. 135).

Como veremos a continuación, uno de los elementos esenciales que verifica la validez de la firma electrónica es la criptografía, por cuanto, "es la ciencia que se ocupa de transformar mensajes, utilizando algoritmos matemáticos, para cifrar datos con el fin de hacerlos incomprensibles para cualquiera que no posea su clave, que debe ser privada, con información secreta" (García, 2011, p. 137). ¡Ánimo! Las siguientes precisiones son importantes para comprender el tema propuesto.

2.3.1 Seguridad y criptografía

Las nociones relacionadas con la firma electrónica se encuentran especificadas en la bibliografía básica de la asignatura. Por ello, se sugiere revisar, detenidamente, estos presupuestos que garantizan su seguridad técnica. Luego de esta revisión, precisamente, destacamos la necesidad de

“generar confianza (…) es especialmente importante debido a que internet es una red abierta y a la sensación de inseguridad (a veces tal vez excesiva) que esto produce en los usuarios” (Téllez, 2008, p. 220).

Al respecto, la bibliografía básica de nuestra asignatura, además, destaca que, por ejemplo, en el marco de la economía digital, se debe propender a “el reconocimiento efectivo de derechos, la tutela judicial efectiva y la prevención del robo de identidad” (Secretaría General Iberoamericana, 2023, p. 15). Así, el uso de la firma electrónica supone atender un criterio flexible, en cuanto al grado de seguridad, por el cual, el método de identificación seleccionado “deberá ser tan fiable como sea apropiado para los fines para los que se consignó o comunicó el mensaje de datos” (LMCE, 1999).

En sentido general, puede decirse que la seguridad se trata de “un concepto asociado a la ausencia de riesgo, pero no resulta posible garantizar que desaparezca totalmente porque el elemento de riesgo siempre está presente con independencia de las diversas medidas que se adopten” (De la Serna, 2021, p. 11). En todo caso, la encriptación implica “la transformación de datos a un formato que no sea legible para quien no tenga la clave para decodificarlo” (Malca, 2001, p. 64).

Por tanto, destacamos en esta parte que, “el uso de la firma electrónica, con la criptografía, el encriptado y su respectivo certificado expedido por una institución autorizada satisface los aspectos de seguridad, tales como integridad de la información, la autenticidad, el no repudio y la autoría del firmante” (García, 2011, p. 149).

La seguridad técnica “se lleva a cabo mediante un conjunto de fórmulas matemáticas complejas denominadas algoritmos de encriptación” (Martínez, Mata, & Rodríguez, 2009, p. 67).

Dicho lo anterior, se advierte que existen sistemas de seguridad simétricos y asimétricos. El primero maneja una sola clave; y, el segundo clave diferentes para el proceso de cifrado y descifrado. En este orden, aclaramos que la criptografía “puede ser simétrica (de clave secreta) y asimétrica (de clave

pública)" (García, 2011, p. 137), en donde, el sistema asimétrico de doble clave representa a una clave privada para el transmisor y una clave pública para el receptor.

Así, se resaltan dos clases o métodos, que se identifican como:

a. criptografía simétrica o de clave secreta (convencional)
b. criptografía asimétrica o de clave pública.

Ahora bien, es preciso señalar que, en lo relativo a los aspectos de seguridad técnica de la firma electrónica, el Reglamento General a la LCE (2002) reconoce que un principio y elemento esencial es un sistema de gestión que permita "la seguridad, confidencialidad, transparencia y no discriminación en la prestación de sus servicios". De este modo, entendemos que se derivan cuatro bloques normativos, a saber:

A. Seguridad técnica.
B. Seguridad Jurídica.
C. Seguridad del consumidor.
D. Seguridad Digital.

Justamente, estos bloques normativos, ponen de manifiesto la importancia de "fomentar entornos digitales seguros y confiables, estableciendo medidas para garantizar la protección de la privacidad de las personas y de los datos personales" (Secretaría General Iberoamericana, 2023, p. 9).

Finalmente, resaltamos que en el proceso de creación y validación de la firma electrónica usted debe identificar la naturaleza de los dispositivos de emisión y comprobación. En este aspecto, el "Glosario de términos" de la LCE determina que los dispositivos de emisión constituyen un "instrumento físico o lógico utilizado por el emisor de un documento para crear mensajes de datos o una firma electrónica". En tanto que, los dispositivos de comprobación son un "instrumento físico o lógico utilizado para la validación y autenticación de mensajes de datos o firma electrónica".

¡Interesante verdad! A partir de las consideraciones que plantea la doctrina sobre el universo de la firma electrónica. Preste atención a las siguientes aclaraciones:

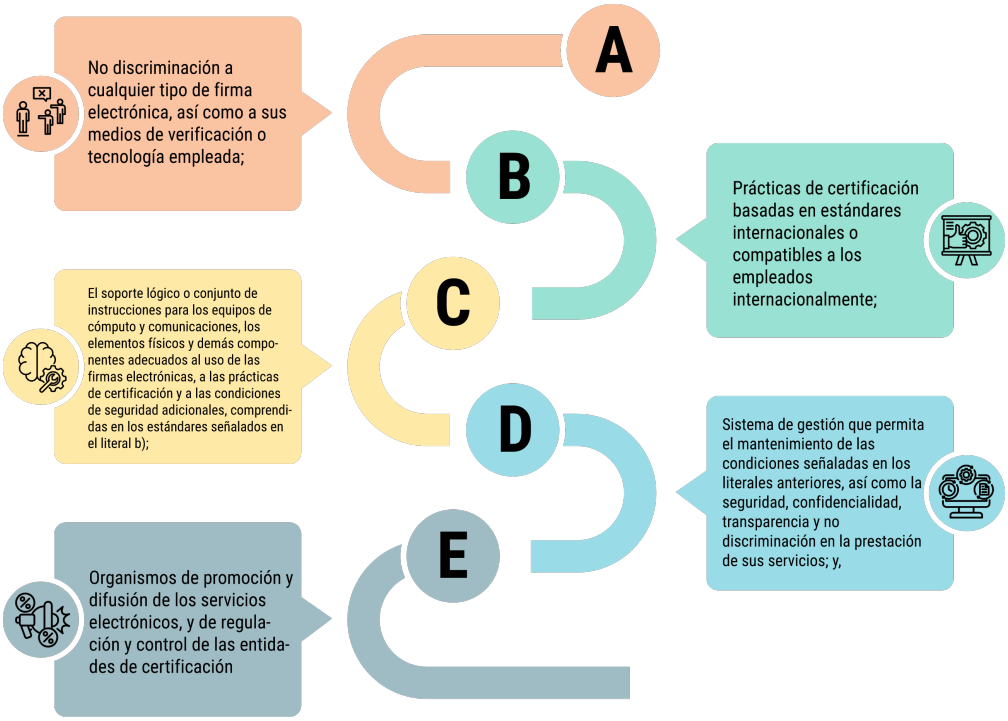
2.3.2 Principios y elementos

El desarrollo de la economía digital y de las transacciones, especialmente, en el ámbito del comercio electrónico, requieren de elementos y principios que garanticen la seguridad, en lo referente a la autenticidad e integridad de la información; y, en todo caso, sobre la identidad de las partes involucradas.

De este modo, atendiendo el Reglamento General a la LCE (2002), los principios y elementos que respaldan a la firma electrónica son:

Figura 1

Principios y elementos que respaldan a la firma electrónica



Nota. Tomado de Ley de Comercio Electrónico, Firmas y Mensajes de Datos [Infografía], por Cepweb, 2002. CEPWEB. CC BY 4.0.

Bajo estas consideraciones, particularmente, identificamos que otra de las características que satisface la seguridad en la firma electrónica tiene que ver con el uso del certificado de firma electrónica, avalado por una entidad autorizada. Naturalmente, es una cuestión que abordaremos en el siguiente tema.

Consideraciones finales respecto a la diferencia entre firma electrónica y firma digital

La función de la firma, en sentido general, apunta a que los intervinientes dentro del negocio jurídico puedan signar las condiciones en las que se realiza el documento. Como se ha señalado en la bibliografía básica de la asignatura,

existen diversas clases de firmas electrónicas, y una de ellas es la firma electrónica avanzada o, simplemente, digital, la cual "se crea usando un sistema de criptografía asimétrica o de clave pública, con un certificado expedido por una institución autorizada por la ley" (García, 2011, p. 137). Por tanto, surgen dos conceptos relacionados –firma electrónica y firma digital–, los cuales tienen el mismo objeto, pero distinta naturaleza como veremos a continuación.

A. **Firma electrónica**

Nota. Ordóñez, L., 2021

En la imagen que se propone, existen dos clases de firma, ¿cuál considera usted que representaría a una firma electrónica?

Para responder a la interrogante, revisemos lo que nos manifiesta el art. 13 de la LCE. Al respecto, dicha norma precisa que la firma electrónica "son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados

para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos".

De esta manera, atendiendo la imagen antes propuesta, el gráfico que mejor representa a la definición de firma electrónica es la que se sitúa en la parte derecha, por cuanto, aquella se traduce en cualquier método de envío de mensajes, mediante algún recurso electrónico, con la finalidad de aprobar y reconocer su contenido. Así, se comprende que la firma electrónica es "el término genérico y neutral para referirse al universo de tecnologías mediante las cuales una persona puede firmar un mensaje de datos" (Téllez, 2008, p. 234).

Considere entonces que, la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre firmas electrónicas describe que la firma electrónica responde al "creciente empleo de técnicas de autenticación electrónica en sustitución de las firmas manuscritas y de otros procedimientos tradicionales de autenticación". Por ello, se entiende que el universo de firmas, a través, de métodos técnicos de encriptación refiere a la expresión "firma electrónica"; en tanto que, la firma digital se considera como un tipo o especie de firma que se encuentra incluida dentro de ese género.

Con el objeto de ampliar el estudio de este tema, es fundamental analizar las disposiciones legales del Capítulo 1, Título 2, de la LCE en relación a la Firma Electrónica. Dentro de esta revisión, podrá determinar temas importantes como los requisitos y efectos de la firma electrónica, las obligaciones del titular de la firma; y la duración y la extinción de la misma.

B. **Firma digital**

La firma digital (firma electrónica avanzada) constituye la transformación de un mensaje utilizando un sistema de cifrado asimétrico. De este modo, Téllez (2008) aclara que la firma digital es "el nombre que se da a cierto tipo

de firma electrónica basada en el uso de criptografía, entre las cuales la más comúnmente usada es la llamada criptografía asimétrica o de llave pública" (p. 235).

Las legislaciones reconocen el género de la firma electrónica; y, luego eligen una especie que denominan "firma electrónica avanzada" o "firma digital".

Así, como usted puede identificar en la bibliografía básica de la asignatura, en la firma digital se utilizan una "serie de datos, generados por un método criptográfico, que garantiza la autenticidad de un mensaje o pedido comercial" (RAE, 2024). Por consiguiente, "mediante el uso de la clave pública del destinatario, el remitente puede estar seguro que sólo el destinatario, poseedor de la clave privada correspondiente, podrá descifrar su mensaje" (García, 2011, p. 139).

En este marco, entre las ventajas de la firma digital encontramos las siguientes:

- Control de integridad de la información.
- Validación de la identificación.
- No repudio o irrefutabilidad.
- Privacidad.

A partir de estas ventajas, la firma digital garantiza que los documentos electrónicos no puedan ser modificados, suplantados por otros firmantes y se les atribuye un carácter probatorio.

Para cerrar este apartado, lo invito a revisar la siguiente infografía que da cuenta de las diferencias entre la firma electrónica y la firma digital.

Diferencias entre firma electrónica y firma digital

Actividades de aprendizaje recomendadas

Finalmente, lo invito a reforzar sus conocimientos, participando en las actividades que se detallan a continuación:

1. En la obra que hemos enunciado anteriormente, sobre el Derecho de las nuevas tecnologías - Capítulo tercero (Parte 2) se describen varios temas relacionados con la firma electrónica, desde la perspectiva de la seguridad técnica y jurídica. Particularmente, se ejemplifica, tanto la criptografía simétrica como asimétrica. Por ello, atendiendo dichos ejemplos, se sugiere identificar las características de cada proceso, así como subrayar las ideas principales que subyacen en torno a la vinculación con la firma digital.
2. Tomando en cuenta que en la bibliografía básica se describe cómo funciona el proceso de firma digital, a partir del siguiente vídeo relativo a las características y ventajas de la firma, le propongo construir un caso que identifique cada fase de este proceso.

Contenidos, recursos y actividades de aprendizaje recomendadas

Semana 5

Unidad 2. Derecho de la Informática: e-commerce, firmas y contratos

2.4 Certificados electrónicos y entidades de certificación

Como se ha destacado en los temas que hemos estudiado hasta esta parte, tanto los certificados electrónicos como las entidades de certificación, son dos presupuestos vinculados con la garantía de la seguridad e integridad de los mensajes de datos y, en suma, de los documentos electrónicos. Por ello, atendiendo la bibliografía básica de la asignatura, revise las siguientes anotaciones.

A. **Certificados electrónicos**

Según la LCE, el certificado de firma electrónica "es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad". De este modo, el certificado de firma electrónica constituye en sí mismo un documento electrónico "generado y firmado digitalmente por una entidad de certificación, la cual vincula claves con una persona determinada confirmando su identidad" (Malca, 2001, p. 68).

El certificado constituye un documento electrónico que contiene información vinculada, tanto a la identidad del firmante como de la entidad de certificación.

Para comprender mejor, García (2011) describe que un sistema de certificación de clave pública determina la intervención de los siguientes sujetos:

- Titular del certificado.
- Usuario o persona que confía en el certificado.
- Entidad de certificación (p. 163).

Respecto a este señalamiento, la bibliografía básica de la asignatura advierte que para garantizar la seguridad y demostrar el vínculo entre el documento electrónico y la identidad del firmante, "la práctica actual invita a introducir la clave pública de un individuo en un certificado digital junto con información relativa a la clave (por ejemplo, la fecha de vencimiento) y al propietario de dicha clave (nombre, etc.)" (Téllez, 2008, p. 231). En todo caso, se requiere de "una tercera parte de confianza", es decir, de una entidad de certificación.

Ahora bien, dentro de las definiciones del "Glosario de términos", la LCE precisa que el emisor es la "persona que origina un mensaje de datos"; el destinatario es la "persona a quien va dirigido el mensaje de datos" y el signatario es la "persona que posee los datos de creación de la firma electrónica, quien, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica".

En este orden, usted debe identificar que el certificado de firma otorga ciertas características y garantías de seguridad, tanto técnicas como jurídicas. Así pues, en la bibliografía básica de la asignatura se identifican las siguientes: autenticación de las partes; integridad del mensaje; la confidencialidad de la información; y, el no repudio (Malca, 2001, p. 70).

Con el objeto de ampliar el estudio de este tema, se sugiere revisar las disposiciones legales del Capítulo 2, Título 2, de la LCE en relación a los certificados de firma electrónica. Dentro de esta revisión, podrá determinar temas importantes como requisitos del certificado; su duración, extinción, suspensión y revocatoria; además de reconocimiento internacional de certificados de firma.

B. **Entidades de certificación**

En primer término, la LCE señala que las entidades de certificación son "empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica". En este sentido, en el marco del proceso de certificación electrónica, se advierte que "la criptografía necesita de una tercera parte de confianza, una entidad de certificación que debe realizar tal asociación vinculando una persona debidamente identificada con un par de claves determinadas" (García, 2011, p. 161).

Recuerde, las entidades de certificación se identifican con el término tercero de confianza, (*trusted third party o TTP*).

En este orden de ideas, se añade que el organismo de regulación, autorización y registro de las entidades de certificación es la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL)[1].

La página web de la ARCOTEL hace referencia a las entidades de certificación y terceros vinculados que se encuentran registradas y autorizadas para la emisión de certificados electrónicos.

Nótese la referencia hacia los “terceros vinculados”, dentro de las entidades de certificación. Esto quiere decir que son personas jurídicas que ofrecen servicios de certificación, al igual que las entidades, propiamente dichas. Conforme a la LCE, respecto a la prestación de servicios de certificación por parte de terceros, “los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información”.

Con el objeto de ampliar este tema, se sugiere revisar las disposiciones legales del Capítulo 3, Título 2, de la LCE en relación a las entidades de certificación. Dentro de esta revisión, habrá determinados temas importantes como obligaciones y responsabilidades de las entidades de certificación; protección de datos, prestación de servicios de certificaciones por terceros vinculados, además de terminación contractual y notificación de cesiones de actividades.

2.5 Contratos informáticos

A. **Nociones preliminares**

Otro tema que es necesario analizar está relacionado a los contratos informáticos, ¿será que usar la tecnología como parte de la contratación conlleva a ilegalidades o invalidez? Verifiquemos estos aspectos entre otros, a través, de la lectura de la bibliografía básica. A partir de estos contenidos, usted podrá encontrar una aproximación al concepto de los contratos informáticos e identificar sus elementos jurídicos y tecnológicos. De esta manera, se sugiere revisar las siguientes apreciaciones.

Como queda anotado, las tecnologías de la información y comunicación permiten beneficiar, entre otras actividades, el comercio electrónico, mediante la contratación de bienes y servicios de la sociedad de la información. Así, a partir de los conceptos de transformación digital y del *e-commerce,* evidenciamos “una ascendente comercialización de los bienes y

servicios derivados de dicha tecnología, regulados mediante figuras jurídicas recientes como los llamados contratos informáticos" (Téllez, 2008, p. 133).

En estos términos, desde la teoría general del derecho contractual, entendemos que los contratos informáticos surgen como un elemento fundamental para afirmar la voluntad de las partes, mediante las reglas y condiciones establecidas para el comercio electrónico o "*e-commerce*". Por esta razón, el impacto de internet y del comercio electrónico en las relaciones contractuales es una cuestión que no pasa desapercibida por el derecho de la informática.

Fundamentalmente, conforme a los contenidos señalados en la bibliografía básica, el contrato informático se define como "un acuerdo de voluntades que establece relaciones jurídicas entre las partes, que tiene por objeto regular la creación y transmisión de derechos y obligaciones derivados de los bienes y servicios informáticos" (Aguilar, 2017, p. 134).

Para ilustrar mejor, las características de dichos contratos hacen referencia, por ejemplo, a su complejidad y carácter atípico.

Precisamente, la bibliografía básica advierte que la evolución de las TIC "ha dado lugar a un incremento exponencial de los volúmenes de información intercambiados, las velocidades de intercambio, la complejidad relacional, entre otras cosas, de lo cual se desprende la contratación electrónica y el comercio electrónico, dentro del ámbito de la economía digital" (Faliero, 2020).

Atendiendo a Téllez (2008) el contrato informático, esencialmente, es sui generis, ya que puede tener en sus cláusulas múltiples normas legales de distintas áreas del derecho.

Así, de la misma manera que en los contratos tradicionales, se entiende que de un contrato informático se desprenden principios y elementos o solemnidades esenciales, por cuanto, de ese acuerdo de voluntades

celebrado entre las partes –generalmente proveedor, distribuidor o diseñador como el usuario, cliente o adquirente– se crean y transmiten derechos y obligaciones (Ríos Estavillo, 1997).

Naturalmente, esto nos lleva a reflexionar sobre la validez de este tipo de contratos. Al respecto, corresponde advertir que la LCE establece que "los contratos podrán ser instrumentados mediante mensajes de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos".

Desde otra perspectiva, otro aspecto que debe destacarse es que, los contratos informáticos, al vincular un acuerdo de voluntades, requieren establecer reglas sobre la resolución de conflictos, ante la falta de cumplimiento. Precisamente, el art. 47 de la LCE, respecto a la jurisdicción señala que "en caso de controversias las partes se someterán a la jurisdicción estipulada en el contrato".

Tomando en cuenta que se trata de una novedosa, el contrato informático "categoría contractual (tanto en lo técnico como en lo jurídico) amerita un tratamiento pormenorizado" (Téllez, 2008, p. 133).

Interesante tema, verdad. Ahora revise las clases de contratos informáticos.

B. **Clasificación**

Según Ríos (1997) se distinguen los siguientes contratos informáticos:

1. Equipamiento.
2. Software.
3. *Leasing*.
4. Servicios.
5. Venta.
6. Locación.
7. Prestación intelectual.

Por constituir un tipo de contratación relacionada con los servicios de la sociedad de la información, aparecen varios principios y elementos constitutivos nuevos que, a priori, no se han señalado en las legislaciones. De este modo, como advierte Aguilar (2017), "el tipo de contrato dependerá de la materia objeto del mismo, si se trata de bienes, suministros, programas y servicios informáticos, por lo tanto, derivado de lo anterior se desprenderán múltiples contratos" (p. 135).

En todo caso, la doctrina conviene vincular dichos elementos, a la luz de los contratos tradicionales para establecer su existencia y validez. A continuación, atendiendo a Aguilar (2017) se señalan los siguientes elementos:

- **De validez:** capacidad, ausencia de vicios, licitud; y, formalidad.
- **De existencia:** consentimiento, objeto; y, solemnidad.

En la bibliografía básica se realiza un interesante análisis de cada uno de estos elementos. Le sugiero revisarlos a fin de contextualizar su naturaleza.

Ahora bien, por tratarse de nuevas formas de contratación, esta manifestación de los contratos tradicionales presenta una serie de principios muy particulares, los cuales se describen a continuación. Preste atención a la siguiente tabla.

Tabla 2
Principios de los contratos informáticos

CONTRATOS INFORMÁTICOS	
PRINCIPIOS	Equivalencia funcional.
	Inalterabilidad del derecho preexistente.
	Neutralidad tecnológica.
	Buena fe.
	Autonomía de la voluntad.

Nota. Ordóñez, L., 2021

Luego de haber revisado esta parte. A continuación, le propongo revisar la siguiente tabla, en donde se identifican algunas características de los Smart Contracts, como una nueva clase de contrato informático. Preste atención.

Tabla 3
Smart Contracts

Smart Contracts	
CARACTERÍSTICAS	Algoritmos que se almacenan en una *blockchain*.
	Ejecutan decisiones automatizadas.
	Se ejecutan sin intervención humana.

Nota. Ordóñez, L., 2021

Así, el *smart contract* se define como un contrato inteligente "diseñados a base de lenguaje de programación, en software, que permiten el cumplimiento automatizado y la ejecución de un contrato" (Faliero, 2020). Así, tal como agrega la AEPD (2022), son ejemplos de aquellos los "servicios automáticos

de apuestas, de compraventa, de notaría, certificaciones de documentos, financieros, inversiones en activos digitales, verificación de identidades digitales".

Como se puede identificar, es evidente que la esencia de los contratos informáticos está determinada por el objeto que da forma al negocio jurídico, siempre que este implique la participación de las tecnologías de la información y comunicación.

[1] Las referencias de la LCE y su Reglamento, en relación al organismo de regulación, si bien invocan al CONATEL, debe entenderse que se trata de la ARCOTEL.

Actividades de aprendizaje recomendadas

Continúe con el aprendizaje mediante la participación en las siguientes actividades:

1. El banco central del Ecuador es una entidad de certificación, debidamente acreditada. Ingresando en el enlace de referencia, usted podrá identificar su misión y visión en esta clase de servicios electrónicos. En todo caso, además, revisará las políticas de seguridad técnica y jurídica que tienen relación con esta entidad de certificación de la información.

   El objeto de esta actividad se dirige a evidenciar cómo, en la práctica, funciona el proceso de certificación de la información.

2. En relación a la naturaleza de los contratos informáticos, la doctrina ha identificado, entre otros, elementos específicos como el secreto y la confidencialidad. Por ello, mediante la revisión de Contratos informáticos, capítulo II usted podrá identificar estos elementos.

Lo que se pretende, a través de esta actividad es reconocer las características, principios y elementos que deben observarse, al momento de redactar un contrato informático. En todo caso, ¿pudo identificar a qué se refieren las cláusulas diversas como parte de los contratos informáticos?

3. Pues bien, ha llegado a la parte final de esta Unidad. Espero que los temas expuestos hayan sido de su interés. Ahora, ¿quiere medir su nivel de conocimiento? ¡Estoy seguro que sí! A continuación, le propongo resolver las siguientes interrogantes:

Autoevaluación 2

A partir de los enunciados que se proponen, escoja la respuesta correcta:

1. Un modelo de ordenamiento jurídico para el comercio electrónico es la:

   a. Ley modelo de la CNUDMI.
   b. Normativa de la RAE.
   c. Directiva de la OCDE.

2. El comercio electrónico es un objeto de estudio de:

   a. El derecho Informático.
   b. El derecho de la Informática.
   c. La informática jurídica.

3. Un área de protección del comercio electrónico es el:

   a. Consumidor.
   b. E-commerce.
   c. Electronic commerce.

4. En Ecuador, la normativa que regula el comercio electrónico es la:

   a. Constitución.
   b. Ley de Protección de Datos Personales.

c. Ley de Comercio Electrónico, Firmas y Mensajes de Datos.

5. Un ejemplo de contrato informático es el de:

a. Electronic data interchange.
b. Trusted third party.
c. Leasing.

6. El documento electrónico hace referencia a todo contenido:

a. Almacenado en formato electrónico.
b. En formato de firma ológrafa.
c. Impreso para ser validado.

7. Un principio aplicable a la validez del documento electrónico es el de:

a. Smart Contract.
b. Equivalencia funcional.
c. Blockchain.

8. La firma digital es un:

a. Término genérico y neutral de las firmas que utilizan TICs.
b. Tipo de firma electrónica basada en la criptografía.
c. Documento en formato físico que se puede digitalizar.

9. Las entidades de certificación, también se conocen como una:

a. Firma Digital.
b. Firma electrónica.
c. Tercera parte de confianza.

10. Un principio de los contratos informáticos es la:

a. Neutralidad tecnológica.
b. Locación.
c. Prestación intelectual.

Ir al solucionario

Contenidos, recursos y actividades de aprendizaje recomendadas

Semana 6

Unidad 3. Protección de datos personales

3.1 Naturaleza del derecho a la protección de datos

Para aclarar el contenido del derecho fundamental a la protección de datos personales, es necesario que acuda a la bibliografía básica y complementaria y revise, detenidamente, tanto el marco legal de protección como las consideraciones que hace la doctrina, respecto a esta libertad informática.

Luego de revisar las precisiones señaladas, puntualizamos que Puccinelli (2004) nos recuerda que, frente a la aparición del poder informático, estamos ante un derecho con contenidos diferenciales, que se constituye por "la suma de principios, derechos y garantías establecidos en favor de las personas que pudieran verse perjudicadas por el tratamiento de los datos de carácter personal a ella referidos" (p. 2).

Este tema es muy interesante, ¿verdad? Ahora, como usted identificará, particularmente, en la bibliografía básica de la asignatura, el derecho a la protección de datos es un derecho que se encuentra muy vinculado con la protección de la intimidad y la privacidad de las personas. Por ello, a partir del ámbito de la sociedad del espectáculo, lo invito a revisar el texto El valor de la información personal, en donde se analiza el valor que representa la información personal.

De la revisión de este documento, usted indicará los efectos que produce la pérdida de la privacidad, a consecuencia de los avances tecnológicos. Por ello, la protección de la intimidad y privacidad, mediante el derecho a la protección

de datos, adquieren especial importancia, a través del reconocimiento de derechos como la intimidad informática, autodeterminación informativa o protección de datos personales.

Ahora bien, sobre la definición de datos de carácter personal, la doctrina, la jurisprudencia y la legislación, en el ámbito internacional, coinciden en precisar que constituye cualquier información concerniente a una persona que la identifique o la puede hacer identificable y que en todo caso pueda "facilitar la configuración de un perfil, aunque no pertenezcan al reducto de la intimidad de la persona" (Troncoso, 2010, p. 133). Así, por ejemplo, encontramos "los datos sobre los gustos o aficiones de las personas e, incluso, aquellos que puedan parecer irrelevantes para incidir en la dignidad como el color de pelo o el número de pie que se calza" (De la Serna, 2011, p. 9).

Desde esta perspectiva, la Ley Orgánica de Protección de Datos Personales –aprobada en mayo de 2021– define que un dato personal es aquel que "identifica o hace identificable a una persona natural, directa o indirectamente" –art. 4–; distinguiéndose dentro de esta categoría: los datos biométricos, genéticos, crediticios, relativos a la salud; y, los datos sensibles.

El objeto y finalidad de la Ley Orgánica de Protección de Datos Personales es "garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección".

En todo caso, además, debe tomarse en consideración que dicha Ley, a partir del principio de juridicidad, dispone que "los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la Constitución, los instrumentos internacionales, la presente Ley, su Reglamento y la demás normativa y jurisprudencia aplicable"–art. 10–. Así, para ampliar esta parte, le sugiero revisar la siguiente infografía que está relacionado con los principios que enmarcan la Ley Orgánica de protección de datos personales.

Principios de la Ley Orgánica de Protección de Datos Personales

Con el objeto de profundizar el estudio de este derecho fundamental, le sugiero revisar el articulo "La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración", en donde se estudia la evolución de la protección de datos, en el contexto de la Comunidad Andina.

De la revisión de este documento, queda evidenciado que existen notables diferencias entre los países que han recibido reconocimiento internacional, en relación con otros que, aún, empiezan o se encuentran en proceso de consolidar un modelo adecuado en el régimen sectorial. Por consiguiente, sobre la base de los Principios y estudios realizados por la OEA, y la experiencia incorporada por Argentina, Uruguay y Perú–, la necesidad de crear un marco interamericano para la regulación de los datos personales es, estrictamente, necesaria en virtud de proteger integralmente el tratamiento de la información personal en el marco de una sociedad globalizada.

Bajo las consideraciones anotadas la regulación de este derecho, desde el ámbito constitucional permite ejercer su protección tanto por su reconocimiento como un derecho fundamental como a través de mecanismos jurídicos que efectivicen su protección. Al respecto, analice el siguiente tema.

3.2 Precisiones desde el derecho constitucional

Sobre este tema, se debe apuntar que el derecho fundamental a la protección de datos tiene un reconocimiento global, tanto en los tratados y acuerdos internacionales como en las Constituciones de distintos países, a partir de los efectos que las tecnologías ocasionan en la privacidad e intimidad de las personas.

Esto se ha traducido en un desarrollo legislativo de este derecho fundamental tendente a regular el tratamiento de la información personal, tanto en el ámbito público como privado.

En el caso de Ecuador, el surgimiento del derecho a la autodeterminación informativa se enmarca en los principios consagrados dentro de la teoría del neoconstitucionalismo andino, enmarcado, fundamentalmente, en la constitucionalización de nuevos derechos y libertades.

Así, la Constitución de 2008 reconoció, por primera vez en su art. 66.19, este derecho fundamental como una libertad que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley".

También, este derecho se conecta con el derecho a guardar reserva sobre las convicciones, por el cual "en ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica". Naturalmente, este derecho previsto en el art. 66.11, garantiza aquellos datos personales que se consideran como información sensible o especialmente protegida.

En este marco, se aprecia que el derecho a la protección de datos se constituye como un instituto de garantía de otros derechos fundamentales, en donde pueden afectarse, por ejemplo, derechos relacionados con la intimidad, la privacidad, la honra, las convicciones y el propio desarrollo de la personalidad. Frente a estas intromisiones, la garantía jurisdiccional del hábeas data, prevista en el art. 92 de la Constitución, tutela el ejercicio de los derechos ARCO además de todos aquellos derechos que puedan afectarse, a partir del uso ilegítimo de la información de carácter personal.

Como se sabe, existen varias problemáticas derivadas de los avances tecnológicos, que se traducen en necesidades al momento de garantizar este derecho fundamental, a partir del tratamiento de la información, sea en el ámbito público o privado. Por ello, asumiendo la importancia del Delegado de

Protección de Datos Personales en nuestro ordenamiento jurídico, lo invito a continuar con la revisión de la siguiente figura en donde se muestran los casos en los que se designará un delegado.

Figura 2

Delegado de protección de datos personales

Nota. Tomado de Ley Orgánica de Protección de Datos Personales [Infografía], por Asamblea Nacional, 2021. Registro Oficial Suplemento 459 de 26-may.-2021. CC BY 4.0

La Autoridad de Protección de Datos Personales podrá definir nuevas condiciones en las que deba designarse un delegado de protección de datos personales y emitirá, a dicho efecto, las directrices suficientes para su designación.

Actividades de aprendizaje recomendadas

Llegados a este punto, lo invito a continuar con el aprendizaje mediante la participación en las siguientes actividades.

1. Tanto la doctrina como la jurisprudencia internacional han destacado que uno de los pilares del ordenamiento jurídico en materia de protección de datos personales es la autoridad de control. En nuestro país, dicha autoridad la ejerce la Superintendencia de Protección de Datos Personales.

   Por ello, en el siguiente documento relacionado con las "Autoridades de control independientes", usted podrá identificar, tanto las garantías sustanciales como formales de independencia que deben acreditar las autoridades de protección de datos personales.

2. Un principio importante y que forma parte de la Ley Orgánica de Protección de Datos Personales es el de seguridad, por el cual se deben implementar todas las medidas de seguridad adecuadas, tanto técnicas como organizativas, para proteger los datos personales frente a cualquier riesgo. En este orden, el siguiente documento titulado: "Del principio de seguridad de los datos al derecho a la seguridad digital" usted podrá identificar las condiciones que plantea el derecho a la protección de datos, desde el ámbito de la seguridad.

Semana 7

Unidad 3. Protección de datos personales

3.3 Protección de datos personales y hábeas data

Una de las cuestiones más importantes que se precisan destacar es que la protección de datos personales se hace efectiva, por medio de la garantía jurisdiccional del *hábeas data*. Así, doctrinariamente, el *hábeas data* protege la integridad de las personas, frente a informaciones referidas a su personalidad; donde prima la intimidad, la privacidad y su entorno familiar.

Del mismo modo, debe considerarse que el derecho fundamental a la protección de datos personales, materializado a través de la garantía jurisdiccional del *hábeas data*, se ejerce mediante la tutela de los denominados "derechos ARCO", es decir: acceso, rectificación, cancelación u oposición.

A partir de este tema, en el artículo relacionado con: "El hábeas data como garantía procesal, frente a las tecnologías de la información y comunicación", abordamos la importancia de esta garantía jurisdiccional, en la era de la transformación digital.

Como pudo identificar, el *hábeas data* no significa, únicamente, una garantía procesal constitucional de acceso a la información de carácter personal. Además, representa un mecanismo de control y de garantía procesal frente al tratamiento de la información en la era de las nuevas tecnologías. Por tanto, respecto a los responsables del tratamiento de la información, esta garantía exige en la era digital la adopción de medidas preventivas y proactivas de seguridad que aseguren la tutela de los bienes jurídicos que compone este denominado instituto de garantía.

Por otra parte, en los últimos años, el ejercicio del derecho fundamental a la protección de datos personales, a partir de los derechos ARCO, especial importancia tiene el surgimiento de un nuevo derecho denominado "derecho al

olvido". En este sentido, lo invito a revisar el siguiente estudio: Reflexiones en torno al derecho al olvido, el cual plantea varias reflexiones, en torno a la protección de los derechos fundamentales en la sociedad de la información.

De lo anotado en esta parte, usted puede evidenciar que el *hábeas data* permite solicitar acceso a la información personal y requerir el contenido de la misma con el objeto de tomar conocimiento sobre los fines de uso y exigir su rectificación cuando resulta errónea o afecta a los derechos del titular de la información.

Finalmente, tomando en cuenta que el derecho a la protección de datos presenta una regulación, dentro del ordenamiento jurídico secundario. Se sugiere revisar la bibliografía básica y complementaria de la asignatura, por cuanto, en los contenidos pertinentes, se realiza un análisis de varias normas que se relacionan con la protección de datos.

3.4 Protección de datos personales en la jurisprudencia de Ecuador

Como hemos identificado hasta esta parte, uno de los derechos que emerge de la evolución de las TIC y de la transformación digital, precisamente, es el derecho fundamental a la protección de datos personales. Así, en el derecho constitucional ecuatoriano, la protección de datos personales se ha desarrollado en tres etapas: primero, la protección constitucional, a través, del *hábeas data*; segundo, la regulación de la información personal y la intimidad mediante leyes sectoriales; y, tercero, el reconocimiento de un derecho fundamental a la protección de datos personales en la Constitución de 2008. En todo caso, desde la promulgación de la Ley Orgánica de Protección de Datos y su Reglamento, atravesamos por una cuarta etapa.

Naturalmente, en las primeras tres etapas la Corte Constitucional de Ecuador -en adelante CCE- ha tenido gran incidencia. Así, habiendo identificado que la jurisprudencia de la CCE es una fuente primaria del derecho en el marco del paradigma del neoconstitucionalismo o constitucionalismo contemporáneo,

que desarrolla el Estado constitucional de derechos y justicia; atender sus precedentes es fundamental en el marco de garantizar la seguridad jurídica del derecho a la protección de datos personales.

En la bibliografía básica se aborda cómo la jurisprudencia de la CCE ha incidido en los distintos ámbitos sectoriales o secundarios que desarrollan el derecho a la protección de datos personales. Por ello, se sugiere ampliar esta perspectiva en dichos contenidos.

En todo caso, queremos resaltar dos sentencias de la CCE que, en nuestro concepto, involucran aspectos fundamentales con la naturaleza de este derecho fundamental. La primera relacionada con el ámbito de la administración pública; y, la segunda con la protección de la intimidad y otros derechos conexos. Veamos las siguientes reflexiones.

i. **En el ámbito de la administración pública**

En la Sentencia 19-9-SEP-CC (Caso No. 14-9-EP), la CCE describe algunos principios importantes que deben observarse en el tratamiento de datos. En todo caso, consideramos que el concepto de *manejo responsable* podría equipararse al principio de responsabilidad proactiva descrito en la LOPDE.

Al respecto, este precedente destaca que, en el tratamiento de datos personales "corresponde también un manejo responsable de la misma, debido a que cualquier acción u omisión en su tratamiento por parte de los servidores públicos responsables puede generar una violación a derechos fundamentales de las personas". En todo caso, desde la perspectiva del principio de eficacia directa, advierte que "los servidores públicos no deben olvidar que entre los fines esenciales del Estado están los de servir la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución".

ii. **En el ámbito de la protección de la intimidad y otros derechos conexos**

En la Sentencia 2064-14-EP/21 (Caso No. 2064-14-EP), la CCE realiza importantes precisiones sobre el contenido del derecho fundamental a la protección de datos personales, en el ámbito de la era digital. En nuestro concepto, se trata del precedente más completo en esta materia, no solamente por su extensión, sino además por la forma en la que aborda los distintos conceptos que emergen del plexo de garantías que comprende el derecho a la autodeterminación informativa.

Particularmente, frente a la conexión con el derecho a la protección de datos personales, la CCE destaca que la intimidad:

En principio se puede abordar el marco de protección de este derecho, partiendo de la idea de que hay ciertos comportamientos del sujeto que exclusivamente podrían llegar al conocimiento de un tercero, si es que dicho sujeto así lo autoriza. En este sentido, se podría utilizar como ejemplo de lo anterior, a las relaciones familiares, a las costumbres, a las prácticas sexuales, a las creencias religiosas, a la salud, al domicilio, a los espacios para la utilización de datos a nivel informático y a los secretos profesionales de una persona.

En esta línea, la CCE advierte la importancia de la denominada expectativa razonable de la privacidad, la cual surge como consecuencia del desarrollo jurisprudencial del derecho a la intimidad y privacidad efectuado por la Corte Suprema de los Estados Unidos de América en el caso United States vs. Katz.

En este orden de ideas, la CCE identifica dos elementos para considerar que una persona tiene una expectativa razonable de privacidad; es decir, un elemento objetivo y otro subjetivo. Por tanto, como señala esta Corte:

> El elemento subjetivo consiste en que quien alegue violación al derecho a su intimidad, pueda considerar válidamente que su actividad, comportamiento o esfera está protegida de posibles injerencias. Por su

parte, el elemento objetivo consiste en que la sociedad pueda asumir que esta expectativa es razonable; es decir, que sea posible concluir que es oponible a terceros.

Respecto a este caso, es preciso señalar que la CCE aborda esta resolución como parte de un "*Hábeas data* para impedir la divulgación de fotos íntimas". Por ello, para contextualizar este precedente, lo invito a revisar el video antes indicado.

Actividades de aprendizaje recomendadas

Continúe con el aprendizaje mediante el desarrollo de las siguientes actividades:

1. En la era digital, la protección de la privacidad de los menores es uno de los debates que requieren especial atención. La sobreexposición de información personal de los menores en internet y redes sociales advierte una serie de riesgos para su privacidad, integridad, propia imagen y desarrollo de la personalidad. Desde esta perspectiva, le propongo revisar el siguiente artículo Amenazas a la privacidad de los menores de edad a partir del Sharenting, en donde se identifican algunos de los riesgos en la privacidad de los menores en la red.
2. Luego de este análisis, resuelva las siguientes interrogantes:

   - ¿Qué entiende por *Sharenting*?
   - La familia, ¿tiene algún deber relacionado con la protección de los datos de los menores?

3. Pues bien, una vez que ha llegado a la parte final de esta unidad, espero que las explicaciones expuestas hayan sido lo suficientemente claras. Ahora, le propongo medir su nivel de conocimiento. A continuación, resuelva las siguientes interrogantes:

Autoevaluación 3

A partir de los enunciados que se proponen, escoja la respuesta correcta:

1. Frente al poder informático, ¿cuál es el objeto del derecho a la protección de datos personales?

   a. La posibilidad de que el Estado controle todos los datos personales de los ciudadanos.
   b. La suma de principios, derechos y garantías en favor de las personas perjudicadas por el tratamiento de datos.
   c. Un mecanismo exclusivo para el beneficio de empresas tecnológicas en la gestión de información.

2. Son bienes jurídicos que están, estrechamente, vinculados con el derecho a la protección de datos:

   a. Seguridad jurídica.
   b. Seguridad técnica.
   c. La intimidad y la privacidad de las personas.

3. ¿Qué caracteriza a un dato personal?:

   a. Cualquier información que identifica o hace identificable a una persona natural.
   b. Está exclusivamente relacionado con actividades comerciales.
   c. Es información que solo se utiliza en investigaciones estadísticas.

4. ¿Cuál es el objeto y finalidad de la Ley Orgánica de Protección de Datos Personales?

   a. Garantizar el ejercicio del derecho a la autodeterminación informativa, incluyendo el acceso y la decisión sobre ellos.
   b. Promover el intercambio libre de datos personales.
   c. Limitar el acceso de las personas a su propia información personal.

5. Atendiendo el principio de juridicidad previsto en la Ley Orgánica de Protección de Datos Personales, los datos personales deben tratarse:

   a. Exclusivamente siguiendo las políticas de las empresas que gestionan los datos.
   b. Sin considerar los instrumentos internacionales.
   c. Con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidos en la Constitución, los instrumentos internacionales y demás normativa aplicable.

6. Atendiendo los principios de la Ley Orgánica de Protección de Datos Personales, es una función que debe cumplir la Autoridad de Protección de Datos:

   a. Centralizar toda la información personal en una base de datos estatal para su monitoreo.
   b. Ejercer un control independiente, imparcial y autónomo, además de realizar acciones de investigación y sanción.
   c. Delegar exclusivamente en las empresas privadas la prevención y sanción de infracciones de datos.

7. ¿En qué paradigma se fundamenta el surgimiento del derecho a la protección de datos en Ecuador?

   a. En el desarrollo de políticas económicas internacionales enfocadas en el comercio digital.
   b. En la teoría del neoconstitucionalismo andino.
   c. En la implementación de reglamentos administrativos sin base constitucional.

8. Como un derecho autónomo, la protección de datos personales fue reconocida por primera vez en el año:

   a. 2021.
   b. 1998.
   c. 2008.

9. Representan los derechos que se tutelan, mediante la garantía jurisdiccional del hábeas data:

   a. Los derechos ARCO: acceso, rectificación, cancelación u oposición.
   b. Los derechos de propiedad intelectual sobre bases de datos personales.
   c. Los derechos exclusivamente relacionados con el comercio electrónico.

10. La Constitución garantiza el derecho a la protección de datos personales como un derecho de:

   a. La naturaleza.
   b. Libertad.
   c. Participación.

Ir al solucionario

Resultados de aprendizaje 1 y 2:

- Comprende los conceptos que se derivan del Derecho Informático.
- Aplica el Derecho de la Informática en las relaciones jurídicas que se derivan de la sociedad de la información.

Contenidos, recursos y actividades de aprendizaje recomendadas

Semana 8

Actividades finales del bimestre

Dentro de esta semana académica se propone hacer una nueva revisión de los contenidos abordados en esta guía didáctica, de conformidad a la planificación señalada en el plan docente de la asignatura.

Cada uno de los recursos doctrinarios, autoevaluaciones de cada unidad y actividades recomendadas, le permitirán ampliar y comprender de mejor manera las instituciones jurídicas que quedan expuestas.

Así también, en cada una de las actividades de colaboraciones, cuestionarios en línea y actividades del componente práctico- experimental, le permitirán vincular los contenidos que se explican en la bibliografía básica. En todo caso, el siguiente vídeo de retroalimentación de contenidos le permitirá recapitular los contenidos más esenciales del primer bimestre.

Resumen del primer bimestre

Estoy seguro que la suma de todas estas actividades, le permitirán desarrollar, adecuadamente, su evaluación en línea.

Segundo bimestre

Resultado de aprendizaje 3:

Comprende la técnica digital forense en los procedimientos de investigación penal de los delitos informáticos

Para comprender la naturaleza de la Informática Forense se hará una revisión de los procesos de identificación, almacenamiento, protección y documentación de los elementos o vestigios que se pueden recabar dentro de un escenario, en el cual se requiera la aplicación de técnicas digitales forenses.

En este marco, se pretende alcanzar este resultado de aprendizaje, mediante el análisis de los distintos recursos de aprendizaje que dispone en esta guía didáctica, vinculando, principalmente, el aprendizaje por indagación.

Sin duda, al final de esta unidad estará en condiciones de identificar a la "Técnica Digital Forense" o "Cómputo Forense" como un sinónimo de la Informática Forense.

Contenidos, recursos y actividades de aprendizaje recomendadas

Recuerde revisar de manera paralela los contenidos con las actividades de aprendizaje recomendadas y actividades de aprendizaje evaluadas.

Semana 9

Unidad 4. Informática Forense

4.1 Definiciones

Como punto de partida en este tema, la bibliografía básica y complementaria de la asignatura realiza una aproximación sobre la conceptualización de la informática forense. Así, en primer término, identificamos que otra forma de hacer referencia a esta disciplina, desde la perspectiva del Código Orgánico Integral Penal, es llamándola "técnica digital forense". Por tanto, constituye otra de las áreas que tiene especial interés para el derecho de la informática, la cual está especialmente relacionada con el estudio del derecho penal informático. Le propongo analizar esta parte. Ahora, preste atención a las siguientes anotaciones.

Sobre la Informática Forense, en principio se destaca que, uno de los compromisos que plantea el escenario de la modernidad es "promover estrategias y políticas iberoamericanas en relación con la prevención e investigación de los ciberdelitos que incluyan el desarrollo de capacidades y la creación y fortalecimiento de las redes de asistencia y cooperación iberoamericana" (Secretaría General Iberoamericana, 2023, p. 9).

Desde esta perspectiva, se advierte que la Informática Forense constituye "una rama de las ciencias forenses que se encarga de adquirir, analizar, preservar y presentar datos que han sido procesados electrónicamente, y almacenados en un medio digital. Es el uso de las Tecnologías de la Información para recuperar evidencia digital" (Di Iorio et al., 2017, p. 80).

En consecuencia, la informática forense, esencialmente, está guiada por la intervención de las ciencias forenses que, mediante un método científico, emplea técnicas especializadas dirigidas a la identificación, observación y análisis de evidencias o vestigios derivados de una infracción, conducta ilícita o de cualquier procedimiento judicial que requiera la utilización de herramientas, mediadas por el uso de tecnologías de la información y comunicación.

En este orden de ideas, desde el ámbito del derecho penal informático, la informática forense se considera una disciplina derivada de la criminalística, en tanto que se configura como una ciencia forense destinada a la obtención de elementos probatorios que permitan inferir la posible comisión de una infracción informática. Su objetivo principal radica en incorporar dichos elementos como pruebas en el proceso penal, a través de los procedimientos y diligencias previstos en la normativa penal aplicable.

Ahora bien, frente a la conceptualización de la informática forense, "varios términos, por ejemplo, *computer forensics, cyber forensics, media analysis y network forensics*, se utilizan para referirse al proceso de adquisición, conservación, examen análisis y presentación de pruebas digitales" (Pollitt et al., 2004, p. 394).

Respecto al origen del término "informática forense" y otras definiciones sobre su naturaleza se sugiere revisar los contenidos previstos en la bibliografía básica. Así, estoy seguro que identificará que su principal característica está relacionada con "adquirir, analizar, preservar y presentar datos que han sido procesados electrónicamente en un medio computacional" (Di Iorio, 2016, p. 64).

Bajo estas consideraciones, ¿se ha preguntado en qué escenarios o contextos se puede aplicar técnicas digitales forenses? Preste atención al siguiente tema.

4.2 Objetivos y estándares

Considerando las definiciones que anteceden, puede decirse que el principal objetivo de la informática forense es precautelar la evidencia de una infracción informática, desde una perspectiva estrictamente técnica, es decir, "salvar y examinar medios informáticos, así como, conseguir argumentos y evidenciar una infracción informática, con el fin de presentar estas mismas, ante un tribunal" (Bustamante, 2020, p. 72).

En todo caso, Páez (2015) precisa que, entre los objetivos de la Informática Forense se destacan:

- Compensación de daños.
- Persecución y procesamiento judicial.
- Creación y aplicación de medidas de prevención.

Además, considerando el mismo criterio de Páez (2015), se hace referencia a varios usos o aplicaciones relacionados a la informática forense en distintos ámbitos, preste atención a la siguiente infografía donde se detallan algunos de estos.

Usos – aplicaciones de la informática forense

Luego de estas revisiones, naturalmente, coincidimos en que el desarrollo de la Informática Forense "ha trabajado sobre su principal objeto de estudio: la evidencia digital" (Di Iorio et al., 2017, p. 80).

Por otra parte, desde el ámbito normativo, advertimos que el Código Orgánico Integral Penal –a partir de lo dispuesto en el numeral 1 del Art. 500– determina las reglas de investigación que deben ejecutarse, en cuanto a la aplicación de las técnicas digitales forenses.

No obstante, la aplicación de estas técnicas se encuentra vinculada tanto al ámbito penal como a los procesos civiles y a ciertas diligencias preparatorias que le preceden.

Dicha norma, como hemos precisado, vincula a la informática forense como una rama de las ciencias forenses, las cuales "siempre están en constante cambio, siempre buscando nuevos métodos y procesos para encontrar y fijar las evidencias de cualquier tipo. Creando nuevos estándares y políticas" (Acurio del Pino, 2009, p. 8).

A continuación, se sugiere revisar los contenidos de la bibliografía básica con el objeto de identificar los estándares y principios internacionales que plantea la IOCE.

Actividad de aprendizaje recomendada

Continúe con el aprendizaje mediante el desarrollo de la siguiente actividad:

Habiendo destacado el vínculo entre la Informática Forense y los procesos de transformación digital, este paradigma demanda de la administración de justicia la modernización, como elementos para procesar los trámites o las causas relacionadas con la aplicación de la Informática Forense. En este marco, le sugiero revisar el siguiente estudio: Informática forense al servicio de una justicia moderna, en donde, a partir de la experiencia internacional se destacan e identifican algunas respuestas.

Lo que pretendemos con esta actividad es, en primer término, que evalúe, desde su experiencia o conocimiento, el estado de modernización de la administración de justicia en Ecuador, respecto a la incorporación de procesos tecnológicos en la sustanciación de los procesos judiciales.

Bajo estas consideraciones, y luego de haber identificado la naturaleza conceptual y legal de la Informática Forense, es preciso avanzar en este estudio con el análisis de los modelos técnicos que se prevén dentro de las técnicas digitales forenses.

Semana 10

Unidad 4. Informática Forense

4.3 Metodologías de investigación forense

Como hemos singularizado hasta esta parte, la investigación forense contemporánea se distingue por su estrecha vinculación con el empleo de las tecnologías de la información y la comunicación, lo cual ha desembocado en un notable avance en la eficiencia y precisión de los procedimientos de investigación.

En este contexto, la Informática Forense se fundamenta en una serie de modelos y procedimientos técnicos, articulados bajo una metodología estándar, cuyo propósito es garantizar la correcta ejecución de las investigaciones judiciales.

Para profundizar el estudio de este apartado, tome en consideración que, en la bibliografía básica se hace referencia a los principales modelos de investigación forense, así como una descripción de algunos de ellos. Por tanto, podrá reconocer que, frente al aseguramiento de la evidencia digital, las metodologías de investigación forense buscan establecer “bases sólidas para el juzgamiento y la validez delante del fuero judicial, por esta razón, es necesario que se eviten suplantaciones, transformaciones, variaciones y falsificaciones” (Bustamante, 2020, p. 72).

Como examinaremos a continuación, dichos modelos, como parte teórica de las técnicas de investigación forense, se apoyan en ciertas metodologías que, en la parte práctica, establecen el proceso o las fases que se deben ejecutar, a partir de la aplicación de los distintos procedimientos. Preste atención a la siguiente tabla:

Tabla 4
Metodologías de la Informática Forense.

	INFORMÁTICA FORENSE / TÉCNICA DIGITAL FORENSE
METODOLOGÍAS	Estándares internacionales para los procedimientos relativos a la evidencia digital de la IOCE.
	Estrategias y metodologías de investigación forense, aplicables a los escenarios informáticos del RFC 3227.
	Guía para las fuerzas y cuerpos de seguridad, relacionada con el examen forense de evidencias digitales, del Departamento de Justicia de Estados Unidos.

Nota. Ordóñez, L., 2025

Estas metodologías son estándares internacionales de algunos grupos de interés en relación a los modelos de control interno sobre sistemas de seguridad para el tratamiento de la evidencia digital. Por ello, la bibliografía básica realiza una amplia explicación. Le sugiero revisar esta parte, con el objeto de precisar las características de cada modelo y sistema de seguridad.

Esta parte, a pesar de contener una serie de terminología de carácter técnica, es preciso estudiarlas, por cuanto, nuestra materia se desenvuelve entre la relación del derecho y la informática.

Actividad de aprendizaje recomendada

Continuemos con el aprendizaje mediante su participación en la actividad que se describe a continuación:

En la era digital, la comisión de infracciones, a través de medios informáticos se considera, más que una realidad, una necesidad que debe ser superada desde el ejercicio profesional. Así, este estudio sobre: El

rasgo digital del delito, le permitirá comparar las normas y metodologías que pueden ser utilizadas en la examinación de datos, en medios digitales.

Lo que pretendemos con esta actividad es que identifique las metodologías que pueden vincularse en estos casos, con el objeto de determinar el alcance de la Informática Forense en la investigación de los delitos informáticos.

A partir de esta revisión, se entienden los fundamentos teóricos, técnicos o informáticos que se aplican en la investigación por lo que es necesario revisar, a continuación, las actuaciones que desde el ámbito legal se prevén para el aseguramiento de la prueba. Al efecto, revise el siguiente tema.

Contenidos, recursos y actividades de aprendizaje recomendadas

Semana 11

Unidad 4. Informática Forense

4.4 Actuaciones y técnicas especiales de investigación

Como introducción a este tema, es preciso anotar que en nuestro país se ha promovido con mucha precisión la incorporación de las tecnologías de la información y comunicación en los procesos de administración de justicia, tanto en el ámbito administrativo como en el desarrollo de principios jurídicos que aseguren la legalidad de la prueba obtenida mediante herramientas tecnológicas.

Si bien los escenarios de las actuaciones especiales de investigación representan una transformación respecto a las prácticas tradicionales para el aseguramiento de la prueba, actualmente, sigue siendo imprescindible

destacar su relevancia. Todo ello, en virtud de que la investigación forense y actuaciones empleadas contribuyan de manera significativa a garantizar la integridad y, en consecuencia, la validez jurídica de las pruebas.

Con respecto a esta última parte, el Código Orgánico Integral Penal describe los principios para el anuncio y práctica de la prueba. En este orden, se sugiere revisar en qué consiste cada uno de estos principios.

En todo caso, considerando que el COIP (2014) reconoce la práctica de "diligencias de reconocimiento del lugar de los hechos en territorio digital, servicios digitales, medios o equipos tecnológicos" (Art. 460.8), dicha normativa advierte los siguientes escenarios: i) actuaciones especiales de investigación en general, ii) actuaciones especiales relativas a contenido digital y iii) técnicas especiales de investigación.

La bibliografía básica de la asignatura, atendiendo el COIP, desarrolla cada uno de estos escenarios. Por ello, se sugiere revisar estos contenidos con detenimiento.

Luego de estas reflexiones precisadas en nuestro COIP, usted habrá identificado que, en los últimos años, la normativa penal ecuatoriana ha tenido un desarrollo importante en lo concerniente a las actuaciones y técnicas especiales de investigación. Particularmente, llama la atención la incorporación del denominado *agente encubierto informático*, que fue incluido en las disposiciones del COIP, a partir de la Ley Orgánica Reformatoria a Varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral en el año 2023.

Con el objeto de precisar las reformas que afectaron el COIP en 2023, en relación a las actuaciones y técnicas especiales de investigación, se sugiere revisar el texto publicado en el Registro Oficial – Suplemento Nro. 279.

En suma, lo que buscan las actuaciones y técnicas especiales de investigación es la preservación de los indicios, la aplicación de la cadena de custodia y la determinación, tanto del nexo causal en el delito como de los criterios para la valoración de la prueba. Por ello, atendiendo a Páez (2015), preste atención al siguiente módulo didáctico:

Actuaciones y técnicas especiales de investigación

Luego de este análisis, se concluye que para que una evidencia recabada en territorio digital pueda adquirir la calidad de prueba legal dentro de un proceso judicial, es indispensable que su obtención, preservación y presentación cumplan con las guías, procedimientos y buenas prácticas que aconsejan los principios y estándares aplicables a la Informática Forense.

Naturalmente, esto garantiza que dichos elementos cuenten con los suficientes criterios legales para asegurar su pertinencia, admisibilidad y eficacia probatoria. En estos términos, puede decirse que el objeto de la informática forense está, especialmente, incardinado con la cadena de custodia, la cual representa una serie de procedimientos técnicos "que garantiza[n] que las muestras y objetos por analizar, que serán expuestos como elementos de prueba en las diferentes etapas del proceso, sean los mismos que se recolectaron en el lugar de los hechos o en puntos relacionados con lo que se investiga" (RAE, 2024).

Es preciso, luego de haber analizado este tema, abordar el procedimiento técnico de investigación forense. Prosiga con su estudio.

4.5 Procedimiento de investigación

Habiendo considerado la estrecha relación entre la informática forense y la cadena de custodia, advertimos la importancia de "instituir procesos adecuados garantizando la eficacia de los métodos empleados al extraer evidencia informática" (Bustamante, 2020, p. 72).

Por una parte, subrayamos que el COIP (2014) determina que la cadena de custodia se aplicará también al contenido digital o evidencia informática, con el objeto de "garantizar su autenticidad, acreditando su identidad y estado original; las condiciones, las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos y se incluirán los cambios hechos en ellos por cada custodio" (Art. 456).

Por ejemplo, en el marco de la investigación y análisis forense de la evidencia o contenido digital en la escena del delito, el COIP (2014) advierte que se debe seguir las siguientes reglas o procedimiento:

- Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura crítica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.
- Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.
- Cuando se recolecta cualquier medio físico que almacena, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto (Art. 500).

Atendiendo los estándares internacionales de la IOCE (1999), "toda actividad relacionada con la incautación, el acceso, el almacenamiento o la transferencia de pruebas digitales debe estar plenamente documentada, conservada y disponible para su revisión.

Por otra parte, en la bibliografía básica, Rodríguez & Doménech (2011) distinguen que, en términos generales, la investigación forense debe atender el procedimiento o pasos que a continuación se detallan. En la siguiente tabla, se resume esta sección.

Tabla 5
Procedimiento / Pasos de la investigación forense.

PROCEDIMIENTO / PASOS DE LA INVESTIGACIÓN FORENSE	
Identificación	Conocimiento y la comprobación del hecho delictivo.
Preparación	Los manuales de operación y los manuales de instrucción deben estar preparados.
Planificación estratégica	Maximiza la recolección de pruebas y minimizar el impacto sobre la víctima.
Aseguramiento de la escena, tanto física como digital	Se pretende evitar la contaminación de las evidencias en territorio digital, tanto por vía física como electrónica
Recogida de evidencias	Implica registrar la escena del delito, recoger y empaquetar adecuadamente las evidencias digitales.
Examen	Se realiza un estudio preliminar de los dispositivos recogidos
Análisis e interpretación	Supone interpretar los datos que se obtenga e interrelacionarlos adecuadamente.
Documentación	Momento final de la investigación forense, que expone, por escrito, los pasos realizados en el análisis, los hallazgos, su interpretación y la conclusión que de ellos se derivan.

Nota. Ordóñez, L., 2021

Finalmente, para ampliar esta parte, se recomienda revisar la bibliografía básica de la asignatura, en donde se expone la naturaleza de cada una de estos pasos y, en suma, del procedimiento aplicable a la investigación forense.

Actividades de aprendizaje recomendadas

Lo invito a reforzar sus conocimientos, participando en las actividades que se describen a continuación:

1. Como pudo evidenciar, uno de los planteamientos de la Informática Forense es la modernización y transformación de los procedimientos de investigación. Particularmente, exige construir e institucionalizar en la administración de justicia mejores condiciones, mediante el apoyo de tecnologías de la información y comunicación. Así, entendemos que un papel importante desarrollará la Unidad Nacional Especializada en Investigación del Ciberdelitos de Ecuador.

   En estos términos, considerando la importancia de dicha unidad, se sugiere identificar la Resolución 34-FGE-2022, por la cual se crea la Unidad de Investigación. Para este fin, es muy importante que ingrese a la base de datos en referencia, mediante la biblioteca virtual de la UTPL, utilizando sus credenciales académicas.

2. Pues bien, ha llegado a la parte final de esta unidad. ¡Espero que los temas aquí expuestos hayan sido de su agrado! Ahora le propongo desarrollar la siguiente actividad:

   Con el objeto de medir su nivel de conocimiento, resuelva las siguientes interrogantes:

Autoevaluación 4

A partir de los enunciados que se proponen, escoja la respuesta correcta:

1. Es otra manera en que se hace referencia a la Informática Forense, según el Código Orgánico Integral Penal:

   a. Técnica digital forense.
   b. Auditoría informática judicial.

c. Seguridad cibernética avanzada.

2. La informática forense se encuentra vinculada científicamente con la:

a. Informática jurídica.
b. Ciencia forense.
c. Regulación de la ofimática.

3. La informática forense tiene especial interés para el derecho informático porque:

a. Regula las licencias de software y hardware en el ámbito penal.
b. Se enfoca únicamente en proteger los derechos de autor digitales.
c. Está vinculada al estudio del derecho penal informático.

4. En el marco de la Informática Forense, la Carta Iberoamericana de principios y derechos en entornos digitales busca promover:

a. Una regulación de plataformas digitales privadas.
b. La creación de leyes que prohíban el uso de tecnología en investigaciones judiciales.
c. Estrategias y políticas iberoamericanas para la prevención e investigación de los ciberdelitos.

5. En el marco de la Informática Forense, la Carta Iberoamericana de principios y derechos en entornos digitales destaca que son aspectos que deben incluirse en las estrategias para combatir los ciberdelitos:

a. La imposición de sanciones automáticas a usuarios de internet.
b. El desarrollo de capacidades y la creación y fortalecimiento de redes de asistencia y cooperación iberoamericana.
c. La limitación de acceso a tecnologías de comunicación en la región.

6. Término que utiliza la doctrina para referirse al proceso de adquisición, conservación, examen, análisis y presentación de pruebas digitales:

   a. Network forensics.
   b. Data recovery.
   c. Data protection.

7. El término cyber forensics, dentro de la informática forense, hace referencia a:

   a. La gestión de redes de datos para la transmisión de información.
   b. Procesos relacionados con la adquisición, examen y presentación de pruebas digitales.
   c. El mantenimiento preventivo de sistemas informáticos.

8. Es el principal objetivo de la informática forense:

   a. Desarrollar software especializado para evitar delitos financieros.
   b. Precautelar la evidencia desde una perspectiva técnica.
   c. Realizar mantenimiento preventivo de dispositivos tecnológicos.

9. Las metodologías de investigación forense buscan:

   a. La validez de la evidencia digital, frente al fuero judicial.
   b. Facilitar la implementación de bases de datos.
   c. Garantizar la aplicación de la ofimática.

10. Figura que ha sido incorporada en la normativa penal ecuatoriana dentro de las técnicas especiales de investigación:

    a. Perito judicial en ciberseguridad.
    b. Administrador de bases de datos judiciales.
    c. Agente encubierto informático.

Ir al solucionario

¡Revise la última unidad de la asignatura!

Resultado de aprendizaje 4:

Aplica el Derecho Penal y Procesal Penal para distinguir los tipos penales derivados de los delitos informáticos

En virtud de la complejidad que las tecnologías plantean en las ciencias jurídicas, a partir de las infracciones informáticas, este resultado de aprendizaje permitirá dimensionar la influencia del fenómeno informático, en otra rama del derecho de la informática.

En este caso, el derecho penal informático. Así, se destacarán las conductas típicas y sus elementos, los sujetos de la infracción, los medios probatorios y el proceso penal que se encuentra vinculado a la comisión de delitos digitales o informáticos.

Por consiguiente, desde los presupuestos legales y doctrinarios que se asocian con la criminalidad informática; al final de esta unidad, estará en condiciones de identificar y evaluar los tipos penales vinculados al delito informático, principios del derecho procesal penal y las consideraciones doctrinarias sobre la naturaleza de esta clase de delitos.

Contenidos, recursos y actividades de aprendizaje recomendadas

Semana 12

Unidad 5. Delitos informáticos

5.1 Conceptualización del delito informático

Como introducción a este tema, en la bibliografía básica, usted podrá analizar los antecedentes del fenómeno relacionado con la cibercriminalidad, desde la perspectiva del derecho penal y derecho procesal penal. Al respecto, se resaltan las siguientes ideas.

En Ecuador la ley penal que regula el delito informático es el Código Orgánico Integral Penal. Este orden normativo, en su parte sustantiva (teórica) surge, frente a las reformas de tipos penales obsoletos que no responden a las necesidades actuales de la población; y, en su parte adjetiva (procesal) como un orden procedimental orientado a garantizar los derechos y libertades de los sujetos procesales, particularmente, de las víctimas y de las personas procesadas.

A partir del paradigma del Estado constitucional de derechos y justicia, la Constitución confiere mayor legitimidad al Código Orgánico Integral Penal.

Precisamente, en los antecedentes del COIP se señala que el derecho penal está destinado a determinar límites para no caer en la venganza privada, ni en la impunidad. Por ello, dicha normativa ha tratado de adecuarse "a los nuevos desarrollos conceptuales que se han producido en el mundo y en la región, como mecanismo para asegurar un correcto funcionamiento de la justicia penal" (COIP, 2014). Sobre esta parte, es preciso que, de conformidad a los contenidos de la bibliografía básica, amplíe la revisión de las características que se destacan en relación al derecho penal informático.

De esta manera, como una introducción al siguiente tema, usted habrá identificado que a nivel internacional, una de las preocupaciones y, a la vez, un desafío para el derecho penal informático es "desarrollar un marco legal, políticas y acciones educativas que apunten a convertir la ciberseguridad y la lucha contra el cibercrimen y la violencia digital en un empeño colectivo orientado a garantizar los derechos de las personas" (Secretaría General Iberoamericana, 2023, p. 9). Preste atención a las siguientes precisiones.

A. **Antecedentes**

En la bibliografía básica se realiza un estudio preliminar sobre el fenómeno de la cibercriminalidad. En esta parte se hace referencia a que, en el marco de los denominados delitos informáticos, la cibercriminalidad plantea

nuevos escenarios que afectan, naturalmente, a los derechos y libertades de las personas, desde la perspectiva del derecho penal. Le sugiero resaltar las ideas más importantes sobre esta parte.

Para empezar este tema es necesario señalar que, en la medida en que se intensifica el uso de las tecnologías de la información y comunicación, se incrementa, proporcionalmente, el riesgo de ser sujeto pasivo de conductas ilícitas tipificadas como delitos informáticos. En este marco, aparecen tipos penales como: la suplantación a la identidad, el ciberacoso, la pornografía infantil, entre otros.

¡Interesante, verdad! Ahora preste atención a las siguientes precisiones.

En un estudio expuesto por la Policía Nacional de Ecuador, a propósito de la emergencia sanitaria causada por la Covid 19, se describe que "en el 2017 se registró 8421 casos; subieron a 9571 y 10279 en 2018 y 2019. La tendencia se mantiene. Los más frecuentes son las estafas digitales con modalidades como la suplantación de la identidad y la apropiación fraudulenta a través de medios electrónicos" (Departamento de Seguridad de las TIC, 2020). Al respecto, le sugiero revisar este análisis en los contenidos que se desarrollan en la bibliografía básica.

Así también, en el contexto internacional, la Organización de Estados Americanos (OEA) precisa que las tipologías informáticas que marcan una tendencia emergente tienen relación con la pornografía por venganza, el asedio cibernético y la ingeniería social (Grupo de Trabajo en Delito Cibernético, s.f.).

En este sentido, puede decirse que "los actos delictivos cibernéticos son muy diversos a nivel mundial, desde actos motivados por intereses financieros y actos relacionados con el contenido informático, hasta actos que atentan contra la confidencialidad, la integridad y la accesibilidad de los sistemas informáticos" (UNODC, 2013, p. 3).

Luego de haber contextualizado algunos antecedentes de los delitos informáticos es preciso definir su naturaleza, considerando los elementos que configuran esta clase de infracciones, a partir de los criterios que la doctrina refiere.

Continuemos con el siguiente tema.

B. **Definiciones**

Para concretar una definición preliminar sobre el delito informático, es necesario que realice una revisión de los contenidos que se señalan en la bibliografía básica. Luego de este análisis, se aprecia que la definición general que determina el Código Orgánico Integral Penal acerca de la Infracción penal aplica para los definir a esta clase de ilícitos.

El COIP la define como una conducta típica, antijurídica y culpable que se clasifica en delitos y contravenciones. A partir de esta consideración, conviene destacar la definición de Julio Téllez sobre delitos informáticos, desde un concepto típico y atípico.

El término delito informático, se asocia a otros como: "delito digital", "delito electrónico", "infracción informática", "computercrime", entre otras.

Así también, resaltamos que, el concepto de delito informático "ha de comprender todo comportamiento delictivo en el que la computadora es el instrumento o el objetivo del hecho" (Mühlen, 1973, como se citó en Mazuelos, 2007, p. 41).

En todo caso, considerando "la facilidad para buscar y acceder a la información contenida en los sistemas informáticos, unida a las posibilidades casi ilimitadas para su intercambio y difusión, sin tener en cuenta las distancias geográficas" (Consejo de Europa, 2001, p. 2), dicho concepto incluye "aquellas formas de criminalidad que se encuentran directa o

indirectamente en relación con el procesamiento electrónico de datos y se cometen con la presencia de un equipo de procesamiento electrónico de datos" (Dannecker, 1996, como se citó en Mazuelos, 2007, p. 41).

De esta manera, la diversidad de definiciones relativas a la cibercriminalidad surge de la naturaleza heterogénea de las conductas que constituyen la comisión de delitos informáticos, las cuales se configuran como infracciones derivadas del uso indebido de las tecnologías de la información y la comunicación, propias de la sociedad de la información.

5.2 Criminal Compliance

Como hemos destacado, desde la perspectiva del derecho penal informático, el Estado constitucional de derechos en Ecuador promueve un marco de protección y garantías que emanan de la Constitución e instrumentos internacionales de derechos humanos. Una de esas garantías está relacionada con la adopción de mecanismos proactivos de protección, frente al tratamiento de la información, conforme a unos principios como el de licitud, consentimiento, calidad y responsabilidad.

Además, obliga a evitar intromisiones ilegítimas en la vida privada de las personas. Al respecto, apuntamos que "el uso de información (datos) de carácter personal, junto al de las tecnologías de la información y comunicación como las que se desarrollan en Internet, puede dar lugar a la comisión de diversos delitos sin que en ocasiones se llegue a ser consciente de ello" (AEPD, 2018, p. 2).

De esta manera, tomando en cuenta que la teoría del *criminal compliance* propone programas y/o mecanismos de prevención y garantía de los derechos que puedan lesionarse en el ámbito penal, esto supone atender tanto el deber de las personas jurídicas en el derecho penal, como las condiciones que plantea el Estado constitucional de derechos para advertir posibles conductas delictivas relacionadas con la intimidad informática, por cuanto "estamos ante

un derecho complementario del que tradicionalmente trata de garantizar la tutela de la intimidad en su sentido más amplio, simplemente vinculado al desarrollo concreto de la informática" (Hernández, 2009, p. 238).

De este modo, dicha teoría configura "una herramienta organizativa que cumple tres funciones principales: la prevención de delitos (función preventiva), su detección (función de detección), y su eficaz sanción y/o denuncia a las autoridades correspondientes para que si lo estiman oportuno inicien una investigación penal (función represiva)" (Aránguez, 2020, p. 48).

En la bibliografía básica de la asignatura se hace referencia a cómo en el COIP se introduce la teoría del criminal compliance. Le sugiero revisar estas precisiones.

A partir de dichas precisiones, usted podrá identificar que, en la actualidad, el principio de *accountability* (responsabilidad proactiva) adquiere especial importancia en la teoría de la *criminal compliance*, en cuanto a la responsabilidad penal de las personas jurídicas derivada de ilícitos vinculados, particularmente, con la protección penal de la información de carácter personal.

Actividades de aprendizaje recomendadas

Es momento de aplicar su conocimiento a través de las actividades que se han planteado a continuación:

1. Complementariamente y de conformidad a los contenidos de la bibliografía básica, le propongo identificar los principios del sistema adversarial y del sistema acusatorio, los cuales aplican en el derecho penal en el marco de la judicialización de los delitos informáticos. En este orden, a través de una interesante publicación de la Corte Nacional de Justicia se analiza el papel de los jueces dentro del actual sistema procesal penal. Por ello, se sugiere consultar el : Rol del juez y el proceso penal oral, acusatorio y garantista, específicamente la

segunda y tercera parte relativa al proceso penal y la constitucionalización del proceso penal.

2. Así también, la siguiente publicación relacionada con la protección de datos y prevención de delitos de la Agencia Española de Protección de Datos identifica, particularmente, algunos aspectos relacionados con la cibercriminalidad y la prevención de delitos en el ciberespacio. En todo caso, constituyen referencias sobre estado del arte en el derecho comparado.

   A partir de la lectura de los temas recomendados, por una parte, habrá advertido los principios del sistema penal ecuatoriano que caracterizan su ejecución, tanto en la parte sustantiva como adjetiva. Se desprenden, en relación al tema de delitos informáticos, los principios de legalidad (tipicidad), oralidad, contradicción, publicidad, inmediación, privacidad y confidencialidad. Por otra parte, desde la perspectiva comparada, se pone de manifiesto la trascendencia de usar los datos personales propios y de terceros, de manera oportuna y apropiada.

Contenidos, recursos y actividades de aprendizaje recomendadas

Semana 13

Unidad 5. Delitos informáticos

5.3 Clasificación de las infracciones informáticas

En principio, las infracciones informáticas “abarcan tanto actividades que atentan contra la integridad, la disponibilidad y la confidencialidad de los sistemas informáticos y las redes de telecomunicaciones como el uso de esas redes o sus servicios para cometer delitos tradicionales” (Consejo de Europa, 2001, p. 3).

También, en este ámbito se sostiene que "la categoría de delito informático ha de ser reconducida a aquellos comportamientos cuya realización sólo sea posible a través del empleo de los elementos de la informática: el procesamiento y almacenamiento de datos" (Mazuelos, 2007, pág. 44).

De esta manera, atendiendo el criterio de Téllez (2008), las infracciones informáticas se sistematizan considerando a las TIC como instrumento o medio y como fin u objetivo. Por tanto, atendiendo las consideraciones que se señalan en la bibliografía básica de la asignatura se sugiere distinguir dichas categorías.

Así, tal como se ha mencionado, el uso masivo de las tecnologías ocasiona que los índices de comisión de delitos informáticos se eleven, exponencialmente, originando una dispersión de acciones ilícitas que, como distingue el Estudio exhaustivo sobre el delito cibernético, de la Oficina de las Naciones Unidas contra la Droga y el Delito, podrían desembocar en tres grandes categorías relacionadas con la ciberdelincuencia: a) actos contra la confidencialidad, integridad y disponibilidad de los datos o sistemas informáticos; b) actos relacionados con la informática para obtener beneficios o perjuicios personales o económicos; y c) actos relacionados con contenidos informáticos (UNODC, 2013).

Por otra parte, el Convenio de Budapest (2001) agrupa en 4 categorías diferentes el ámbito de los delitos informáticos o los delitos relacionados con el empleo de ordenadores (Consejo de Europa, 2001). Así, por ejemplo:

a. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos
b. Delitos informáticos, propiamente dichos
c. Delitos relacionados con contenidos informáticos
d. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

En lo relativo a estas clasificaciones de los delitos informáticos, las mismas se encuentran debidamente ampliadas en la bibliografía básica de la asignatura. Por ello, le sugiero estudiar estos contenidos con el objeto de determinar su naturaleza.

Ampliando este escenario, se advierte una clasificación interesante, que categoriza a las infracciones informáticas, a partir del procesamiento de datos en internet.

Respecto a esta última clasificación, se sugiere revisar las consideraciones que se señalan en la bibliografía básica, atendiendo el criterio de Jofer en Mazuelos, 2007.

De este estudio se desprende que un factor importante que debe abordarse en el marco de la cibercriminalidad tiene relación con los sujetos de las infracciones informáticas. Por tanto, es necesario realizar su estudio, a partir de la siguiente temática.

5.4 Aspectos criminológicos relacionados con los sujetos de las infracciones informáticas

Tanto la doctrina como la jurisprudencia identifican como elementos generales para la configuración del delito la identificación del sujeto activo y sujeto pasivo. Con esta precisión, el Código Orgánico Integral Penal determina que se consideran como sujetos del proceso penal, entre otros a la persona procesada o sujeto activo y a la víctima o sujeto pasivo.

Respecto a las consideraciones legales sobre la persona procesada o sujeto activo y a la víctima o sujeto pasivo, se sugiere revisar las disposiciones legales contenidas en el Código Orgánico Integral Penal.

Desde esta perspectiva, los contenidos de la bibliografía básica de la asignatura resaltan que la Criminología es “la ciencia que se encarga del estudio del delito como conducta humana y social, de investigar las causas de la delincuencia, de la prevención del delito y del tratamiento del delincuente” (Tavira y López, s/f, como se citó en Di Iorio, Cistoldi & Nuñez, 2017). En todo

caso, junto a la Criminología, aparece la Victimología, la cual es una “disciplina que se encarga del estudio multidisciplinar de las peculiaridades, necesidades, situación procesal y protección de la víctima, que se ha independizado de la criminología” (Real Academia Española, 2024).

En este orden de ideas, en la era de la transformación digital, por una parte, destacamos que “las consecuencias del comportamiento delictivo pueden tener mayor alcance que antes, porque no están restringidas por los límites geográficos o las fronteras nacionales” (Consejo de Europa, 2001, p. 2); y, por otra parte, “el fenómeno informático ha alcanzado sus actuales dimensiones, en gran medida gracias a la aparición de la red Internet”. (Reina, 2002, p. 7).

Con el objeto de vincular este tema con las referencias que la doctrina apunta, se sugiere revisar los contenidos determinados en la bibliografía básica en relación al sujeto activo y, particularmente, pasivo de la infracción (victimología).

De este análisis, se infiere que el sujeto activo se caracteriza por encontrarse “en lugares estratégicos donde se maneja información de carácter sensible; o son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos” (Téllez, 2008, p. 188). En tanto que el sujeto pasivo solicita “campañas de sensibilización pública, en particular las relativas a las nuevas amenazas y las dirigidas a destinatarios específicos, como los menores” (UNODC, 2013, p. 14).

Actividad de aprendizaje recomendada

Lo invito a participar en la siguiente actividad:

A partir de la siguiente infografía relacionada con la: Responsabilidad de los y las menores (y de su padres y madres) por los actos cometidos en Internet, se ejemplifican ciberdelitos que involucran a la niñez y la adolescencia. Particularmente, desde el derecho comparado, este estudio

de la Agencia Española de Protección de Datos identifica aspectos criminológicos relacionados con la responsabilidad de los menores en el ciberespacio.

En este marco, pretendemos analizar de manera global los delitos informáticos, tomando en cuenta las implicaciones tecnológicas que éstos conllevan.

Contenidos, recursos y actividades de aprendizaje recomendadas

Semana 14

Unidad 5. Delitos informáticos

5.5 Tipos penales en la legislación ecuatoriana

A partir de la revisión de este tema, usted podrá determinar los distintos tipos penales sobre delitos informáticos que regula en la actualidad el Código Orgánico Integral Penal del Ecuador. En este marco, recuerde que para considerar que una infracción penal se reconozca como tal, debe invocarse el principio del derecho penal de legalidad que refiere que no hay infracción penal, pena, ni proceso penal sin ley anterior al hecho.

En este sentido, todos aquellos actos ilícitos que se desprenden de la criminalidad informática deben estar contemplados o tipificados en la ley penal, antes de que se cometa el hecho, materia de procesamiento.

Las reformas penales de 2021 y de 2023 ponen de manifiesto, fundamentalmente, tanto nuevas tipologías relacionadas con la violencia digital como técnicas de investigación vinculadas con el análisis forense en el ciberespacio.

Bajo estas consideraciones, en la bibliografía básica de la asignatura, en relación al Código Orgánico Integral Penal, se describen los tipos penales considerados como delitos informáticos. En este aspecto, con el objeto de ahondar en los elementos constitutivos de cada delito, le sugiero analizar el siguiente ejemplo. Preste atención al siguiente cuadro.

Tabla 6

Elementos constitutivos del delito informático.

TIPO PENAL	SUJETO ACTIVO	SUJETO PASIVO	ELEMENTOS CONSTITUTIVOS	BIEN JURÍDICO PROTEGIDO	SANCIÓN
Pornografía con utilización de niños, niñas o adolescente.	Cualquier persona.	niños, niñas o adolescentes niños, niñas o adolescentes con discapacidad o enfermedad grave o incurable.	Fotografías, filmaciones, grabaciones informáticas o en cualquier otro soporte físico o formato que contenga desnudos o semidenudos.	Intimidad, Interés superior del niño.	Pena privativa de 13 a 16 años Pena privativa de 16 a 19 años.

Nota. Ordóñez, L., 2021

Finalmente, si de los considerados del Código Orgánico Integral Penal se menciona que la tipificación de esta clase de infracciones responde a la existencia de tipos penales obsoletos –anteriores al COIP– que no responden a las necesidades de la sociedad; hay que tomar en consideración que el antecedente de esta regulación fue la Ley de Comercio Electrónico Firmas y Mensajes de Datos (2002) que, derogada actualmente, en esta parte específica, se derivó de modelos internacionales que en la materia se habían avanzado.

Un recurso importante en esta parte es la reforma penal de 2021, que introdujo nuevos tipos penales relacionados con la prevención de la violencia digital y el fortalecimiento de la lucha contra los delitos informáticos. Por ello, para identificar este y otros tipos penales, se sugiere revisar el Registro Oficial Nro. 526 de 2021.

En este marco, son ejemplos de delitos informáticos en la actual legislación penal:

- El hostigamiento (art. 154.2)
- El ciberacoso sexual (art. 166)
- El contacto con finalidad sexual con menores de dieciocho años por medios electrónicos (art. 173)
- La oferta de servicios sexuales con menores de dieciocho años por medios electrónicos (art. 174)
- La violación a la intimidad (art. 178)
- La suplantación a la identidad (art. 212), entre otros.

¡Este tema es muy interesante! Hasta ahora, hemos avanzado en el estudio de los delitos informáticos dentro del contexto ecuatoriano. Así, haciendo un paréntesis se enfocará en los instrumentos internacionales más importantes que sobre delitos informáticos se han creado.

5.6 Importancia del Convenio de Budapest

Uno de los objetivos fundamentales del derecho internacional es la lucha contra la ciberdelincuencia, cuyo origen se vincula al impacto del uso de las nuevas tecnologías de la información y comunicación, en virtud de su capacidad para trascender las fronteras geográficas en el marco de la transformación digital. En este contexto, se ha propiciado la creación de organismos de cooperación internacional, con el propósito de establecer un marco jurídico común y mecanismos de asistencia y reciprocidad legal que permitan la efectiva sanción de las conductas constitutivas de criminalidad informática.

Para comprender mejor este tema, en los contenidos de la bibliografía básica se hace especial referencia a los principales convenios y tratados internacionales que se han creado en materia de regulación de delitos informáticos. Se sugiere revisar esta parte, con el objeto de ampliar el estudio de este tema.

Luego de esta revisión, merece especial referencia el Convenio sobre cibercriminalidad de Budapest, el cual constituye el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia

La Carta Iberoamericana de principios y derechos en entornos digitales destaca que "las dificultades que afrontan los Estados a prevenir y combatir el uso de las TIC con fines delictivos requieren de mayores esfuerzos para fortalecer la cooperación internacional, las actividades de asistencia técnica y desarrollo de capacidades para prevenir y sancionar dicho uso".

Precisamente, el Convenio de Budapest se presenta como el principal instrumento internacional que apunta a reconocer "conductas tipificadas (es decir, a establecer cuáles de ellas serán ilícitas) así como a establecer las medidas procesales idóneas para su esclarecimiento, y a la coordinación y cooperación entre las policías y administraciones de los países que se adhieran al mismo" (Lamperti, 2017, p. 96).

Es conveniente señalar que, en el caso de Ecuador, el Convenio de Budapest fue ratificado en todo su contenido vía Decreto Ejecutivo Nro. 332 el 12 de julio de 2024. Al respecto, destacamos que dicha ratificación tuvo como antecedente el Dictamen 1-24-TI/24 de la Corte Constitucional de Ecuador, en el que se resolvió que dicho convenio requería de aprobación legislativa, en tanto implicaría una adecuación normativa del COIP.

Para profundizar esta parte, se sugiere revisar el Dictamen 1-24-TI/24 de la Corte Constitucional, relativo a la adopción del Convenio de Cibercriminalidad de Budapest.

Bajo estas consideraciones, se advierte que adquiere especial importancia el Convenio de Budapest, por cuanto las medidas internacionales podrían desempeñar "un papel fundamental en la prevención del delito cibernético y en la lucha contra él. Son necesarias en todas las esferas, incluida la tipificación como delito, la competencia procesal, la jurisdicción, la cooperación internacional y la responsabilidad" (UNODC, 2013, p. 4).

Finalmente, desde la perspectiva de este Convenio, otro elemento para la configuración del delito es el elemento material que configura el carácter probatorio dentro de un proceso penal. Para ello, preste atención a los siguientes apartados que desarrollará en la siguiente semana.

Actividades de aprendizaje recomendadas

Lo invito a desarrollar las actividades que se describen a continuación:

1. En la siguiente actividad se sugiere la revisión de una importante campaña de prevención relacionada con los delitos informáticos.

   Se trata especialmente de abordar los casos de ciberacoso que pueden perpetrarse como resultado del uso ilícito de las TICs. Por ello lo invito a revisar el programa "Tú decides en Internet", el cual forma parte de los mecanismos de prevención de delitos informáticos en España.

2. Así también, se sugiere revisar el programa "Dile No al Grooming", orientado a proteger a la niñez y la adolescencia en el mundo digital. Naturalmente, desde la perspectiva del derecho argentino, intentamos identificar distintas acciones que puedan ayudar a combatir el tipo penal previsto en el art. 173 del Código Orgánico Integral Penal ecuatoriano.

¡Continúe con este estudio!

Semana 15

Unidad 5. Delitos informáticos

5.7 Prueba electrónica en el derecho penal informático

En principio, la prueba electrónica puede entenderse como "todo ese tipo de material que existe en forma electrónica o digital.

Puede estar almacenado o ser transitorio. Puede existir en forma de archivos informáticos, transmisiones, registros, metadatos o datos de la red" (UNODC, 2013, p. 10).

Esta noción, no solamente reitera la importancia de que la administración de justicia debe estar lo suficientemente capacitada y preparada para admitir elementos probatorios que se desprenden de las infracciones informáticas, sino que, además, resultaría imprescindible contar con la ayuda de expertos (investigadores forenses) en la materia, quienes, al momento de recabar, resguardar y examinar las evidencias, aseguren su valor probatorio ante la administración de justicia.

Para comprender mejor este tema, la bibliografía básica de la asignatura realiza una revisión en detalle sobre la configuración legal de los medios de prueba, atendiendo lo que dispone el Código Orgánico Integral Penal. Para los fines correspondientes, revisar detenidamente este tema.

Luego de esta revisión, puede entenderse que "la capacitación judicial en derecho cibernético, recopilación de pruebas y conocimientos informáticos básicos y avanzados constituye una prioridad especial" (UNODC, 2013, p. 11), es decir, "se hace indispensable para la valoración de las pruebas o elementos de convicción la intervención de personas que tengan especiales conocimientos en materias especiales en este caso de la materia informática" (Acurio del Pino, 2009, p. 16).

Por tanto, como hemos señalado en temas anteriores, el proceso de identificación, recolección, preservación y formalización de la prueba implica la aplicación de una serie de procedimientos técnicos y legales, entre los cuales destaca la cadena de custodia. Dichos procedimientos tienen como finalidad garantizar la integridad, autenticidad y legalidad de la prueba, asegurando su idoneidad para que sea valorada y motivadamente considerada por el juez al momento de resolver.

En este marco, es preciso mencionar que la bibliografía básica identifica dos funciones orientadoras de la evidencia electrónica. La primera, una función orientadora; y, la segunda, una función probatoria. Al efecto, se sugiere examinar estas conceptualizaciones.

Por otro lado, como también hemos advertido, en la investigación forense, dirigida a la determinación de la materialidad y responsabilidad de los delitos (nexo causal), la obtención de indicios o elementos de convicción, que posteriormente se configurarán como pruebas, debe observar las disposiciones legales y técnicas aplicables. Estas normas tienen como finalidad asegurar su validez y admisibilidad, evitando así que puedan ser objeto de impugnación o exclusión en el proceso judicial.

Atendiendo el COIP, la impugnación o exclusión de medios probatorios podría estar enfocado con el denominado "fraude procesal". Por esta razón, se sugiere revisar el artículo 272 del COIP.

Ahora bien, recordemos que, en el caso ecuatoriano, la LCE, reconocida, históricamente, como la primera ley que regulaba las infracciones informáticas, identifica en su Art. 55, por ejemplo, a los mensajes de datos y documentos electrónicos como medios de prueba, los cuales serán valorados, atendiendo los principios de la ley y, en todo caso, considerando de esta información la "seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectúe con el empleo de otros métodos que aconsejen la técnica y la tecnología" (LCE, 2002).

En este escenario, relacionado con los medios de prueba penal digital, particularmente, debe advertirse que, el COIP (2014) determina que la prueba "tiene por finalidad llevar a la o al juzgador al convencimiento de los hechos y circunstancias materia de la infracción y la responsabilidad de la persona procesada" (Art. 453).

De este modo, dicha normativa reconoce que uno de los principios procesales de la prueba es el de libertad probatoria, por el cual "todos los hechos y circunstancias pertinentes al caso, se podrán probar por cualquier medio que no sea contrario a la Constitución, los instrumentos internacionales de derechos humanos, los instrumentos internacionales ratificados por el Estado y demás normas jurídicas" (COIP, 2014, Art. 454.4). Por tanto, cuando se identifica que los hechos se podrán probar por cualquier medio, se infiere el reconocimiento de medios electrónicos o digitales como prueba, vinculado o no a una infracción informática.

De todo lo mencionado, se desprende que una clasificación general de los medios de prueba penal digital considera a la prueba de tipo: documental, testimonial y peritaje.

Conforme a los contenidos de la bibliografía básica, se realiza un amplio análisis relacionado con las tipologías de los medios de prueba penal digital. Le sugiero realizar una lectura preliminar sobre el tema a fin de desarrollar la siguiente actividad.

Luego de realizar este análisis, usted está en condiciones de identificar y exponer los tipos de pruebas que se desprenden de la clasificación anotada. Para este fin, tenga presente las explicaciones que se refieren al respecto en los contenidos de la bibliografía básica. Así, habrá evidenciado que, uno de los tipos de prueba más relevantes son los que se desprenden del peritaje digital forense en materia de delitos, propiedad intelectual, sistemas, servicios, dispositivos, intimidad y privacidad.

Finalmente, revise lo relacionado al proceso penal de las infracciones informáticas, atendiendo las disposiciones del Código Orgánico Integral Penal. Para ello, se sugiere revisar el siguiente tema.

5.8 Referencia al procedimiento penal

La implementación del Código Orgánico Integral Penal ha introducido nuevos procedimientos orientados a la optimización y celeridad en la prestación del servicio de administración de justicia, en estricta observancia de los principios del debido proceso y de la tutela judicial efectiva.

En primer término, el COIP señala que el ejercicio de la acción penal puede ser público y privado.

Según dispone el Código Orgánico Integral Penal, el ejercicio público de la acción corresponde a la Fiscalía, sin necesidad de denuncia previa.

Al recaer la titularidad de la acción penal pública en la Fiscalía, ésta instancia ejercerá la acción penal cuando tenga los elementos de convicción suficientes, sobre la existencia de la infracción y de la responsabilidad de la persona procesada. Así, el ejercicio de la acción penal pública conlleva aplicar el procedimiento ordinario, previsto en el Código Orgánico Integral Penal, mediante tres etapas:

1. Instrucción Fiscal.
2. Evaluación y preparatoria del juicio.
3. Etapa del juicio.

Adicionalmente, se señalan algunos procedimientos especiales que se derivan del ejercicio de esta acción. Al respecto, le invito a revisar estos cuatro procedimientos a fin de ampliar el tema.

Ahora bien, de conformidad a los contenidos desarrollados hasta esta parte, se sugiere analizar y resolver el siguiente caso:

CASO PRÁCTICO

Juan Pérez acude a su despacho jurídico a comentarle que la hija Juan (María Pérez) ha sido víctima de un delito de "Grooming".

Juan asegura que no sabe en qué consiste este tipo penal, pero que, a través, de los distintos medios de comunicación ha llegado a enterarse que se trata de abuso de menores mediante medios tecnológicos.

De esta manera, conociendo usted los tipos penales que se ventilan, mediante una acción pública:

1. ¿Qué tipo penal, establecido en el Código Orgánico Integral Penal, encaja en la conducta que refiere Juan Pérez?
2. ¿Quién es la autoridad competente ante la cual se debe denunciar este hecho?
3. ¿Qué técnica digital forense (modelo y metodologías) aplicaría dentro de la investigación de este delito?

Por otra parte, como se había señalado, el ejercicio de la acción penal, también puede ser privada. En este contexto, según se desprende del Código Orgánico Integral Penal, los tipos penales que corresponden a esta categoría se encuentran: la calumnia, la usurpación, el estupro, las lesiones que generen incapacidad o enfermedad de hasta treinta días, y los delitos contra animales que forman parte del ámbito para el manejo de la fauna urbana.

Según dispone el Código Orgánico Integral Penal, el ejercicio privado de la acción penal corresponde únicamente a la víctima, mediante querella.

De este modo, el tipo penal que puede constituirse como un delito informático por la vía de acción privada es la calumnia, toda vez, que según el Código Orgánico Integral Penal "la persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra, será sancionada con pena privativa de libertad de seis meses a dos años".

El ejercicio de la acción penal privada se sujetará al procedimiento establecido en la "Sección Cuarta" del Código Orgánico Integral Penal. Le sugiero revisar detalladamente cada disposición legal que se anota.

En este marco, de conformidad a los contenidos desarrollados hasta esta parte, se sugiere analizar y resolver el siguiente caso:

CASO PRÁCTICO

Mario Moreno acude a su despacho jurídico a comentarle que ha sido insultado, por medio de redes sociales por su mejor amigo Roberto Gómez. De lo que le ha referido, se evidencia que Roberto Gómez lo ha calificado como un vulgar "ladrón" y "estafador", por el simple hecho de haberle solicitado la devolución de un dinero.

De esta manera, conociendo los tipos penales que se ventilan, mediante una acción privada:

1. ¿Qué tipo penal, establecido en el Código Orgánico Integral Penal, encaja en la conducta que refiere Juan Pérez?
2. ¿Quién es la autoridad competente ante la cual se debe denunciar este hecho?
3. ¿Qué técnica digital forense (modelo y metodologías) aplicaría dentro de la investigación de este delito?

Adicionalmente, conviene destacar que una infracción informática, también, puede desprenderse de algunas contravenciones tipificadas por el COIP. Particularmente, el artículo 396.1, relativo a las contravenciones de cuarta clase, establece que, "será sancionada con pena privativa de libertad de quince a treinta días: La persona que, por cualquier medio, inclusive a través de cualquiera de las tecnologías de la información y comunicación, profiera expresiones en descrédito o deshonra en contra de otra, ya sea mediante lenguaje violento, agresivo, vulgar u hostil".

Así también, como parte de las reformas penales de 2021, el COIP introdujo las contravenciones relativas al ciberacoso académico; y, de violencia contra la mujer o miembros del núcleo familiar. Por ello, atendiendo dicha normativa, se sugiere identificar su naturaleza y el procedimiento previsto para esta clase de contravenciones.

Actividades de aprendizaje recomendadas

Lo invito a participar desarrollando las siguientes actividades:

1. Mediante el siguiente enlace relacionado con denuncias en línea de la Fiscalía General del Estado de Ecuador, podrá algunas infracciones informáticas que afectan a la mujer o miembros de la familia y, principalmente, a la niñez y la adolescencia. De esta manera, determinará cómo se puede iniciar un proceso penal, mediante denuncia ante la Fiscalía.
2. Particularmente, hoy en día, llama la atención el uso de tecnologías disruptivas en el marco del derecho penal informático. Por ello, un tema relevante es la prueba electrónica. Por ello, a través, del siguiente estudio relacionado con "El rastro digital del delito" se advierten cuestiones fundamentales derivadas de la investigación forense y, en todo caso, de la prueba, el rol del perito y la actuación forense.
3. Finalmente, le sugiero realizar la siguiente actividad, con el objeto de medir su nivel de conocimiento. A continuación, le propongo resolver las siguientes interrogantes:

Autoevaluación 5

A partir de los enunciados que se proponen, escoja la respuesta correcta:

1. ¿Qué regula el Código Orgánico Integral Penal en Ecuador respecto a los delitos informáticos?

    a. La actualización de tipos penales obsoletos y del orden procedimental que garantiza los derechos de las víctimas y procesados.
    b. La creación de nuevos derechos digitales para todos los ciudadanos ecuatorianos.
    c. La regulación exclusiva del uso de tecnologías en instituciones privadas.

2. El derecho penal informático, según el COIP, está destinado a:

    a. Garantizar exclusivamente la protección de bienes materiales.
    b. Establecer nuevos desarrollos conceptuales.
    c. Regular las sanciones administrativas en casos de infracciones civiles.

3. ¿Cuál es uno de los desafíos del derecho penal informático?

    a. Crear redes sociales exclusivas para monitorear el comportamiento de los ciudadanos.
    b. Regular únicamente las transacciones económicas realizadas en línea.
    c. Desarrollar un marco legal, políticas y acciones educativas para convertir la ciberseguridad y la lucha contra el cibercrimen en un empeño colectivo.

4. Las tipologías informáticas de tendencia emergente según la OEA están relacionadas con:

    a. El desarrollo de software para la protección de datos personales.

b. La pornografía por venganza, el asedio cibernético y la ingeniería social.
c. La regulación del comercio electrónico internacional.

5. Definición de infracción atendiendo el COIP:

a. Acción regulada exclusivamente por normas administrativas.
b. Comportamiento moralmente reprochable sin consecuencias legales.
c. Conducta típica, antijurídica y culpable, clasificada en delitos y contravenciones.

6. ¿Con qué términos se asocia el concepto de "delito informático"?

a. Computer crime.
b. Ciberseguridad.
c. Comercio electrónico.

7. Se distinguen como las funciones principales del criminal compliance:

a. Prevención, detección y sanción.
b. Protección de datos personales, control financiero y auditoría interna.
c. Mediación de conflictos y control administrativo.

8. Principio relacionado con el criminal compliance:

a. Oralidad.
b. Accountability.
c. Neoconstitucionalismo.

9. Atendiendo a Téllez, el delito informático se define desde un punto de vista:

a. Inquisitivo.
b. Típico y atípico.
c. Inductivo.

10. La prosecución de un delito informático de calumnia se realiza mediante una:

a. Acción pública.
b. Acción privada.
c. Acción reservada.

Ir al solucionario

De esta manera, ha llegado a la parte final de esta unidad y, consecuentemente, de la asignatura. Espero que los temas aquí expuestos hayan sido de su agrado.

Resultados de aprendizaje 3 y 4:

- Comprende la técnica digital forense en los procedimientos de investigación penal de los delitos informáticos
- Aplica el Derecho Penal y Procesal Penal para distinguir los tipos penales derivados de los delitos informáticos

Contenidos, recursos y actividades de aprendizaje recomendadas

Semana 16

Actividades finales del bimestre

Dentro de esta semana académica se propone hacer una nueva revisión de los contenidos abordados en esta guía didáctica, de conformidad a la planificación señalada en el plan docente de la asignatura.

Cada uno de los recursos doctrinarios, autoevaluaciones de cada unidad y actividades recomendadas, le permitirán ampliar y comprender de mejor manera las instituciones jurídicas que quedan expuestas.

Así también, en cada una de las actividades: video colaboraciones, cuestionarios en línea y actividades del componente práctico- experimental, le permitirán vincular los contenidos que se explican en la bibliografía básica. En todo caso, el siguiente vídeo de retroalimentación de contenidos le permitirá recapitular los contenidos más esenciales del segundo bimestre.

Resumen del segundo bimestre

Estoy seguro que la suma de todas estas actividades, le permitirán desarrollar, adecuadamente, su evaluación en línea.

Desde luego, espero que todas las orientaciones hasta aquí anotadas hayan servido de manera satisfactoria dentro de su proceso de aprendizaje a lo largo de este período académico. ¡Le deseo todos los éxitos en el desarrollo de sus evaluaciones!

¡Hasta pronto!

4. Autoevaluaciones

Autoevaluación 1

Pregunta	Respuesta	Retroalimentación
1	b	Confróntese la bibliografía básica. La Informática Jurídica no es otra cosa que el procesamiento o tratamiento de la información jurídica, por medios electrónicos, no sólo en lo informático, sino también en las telecomunicaciones.
2	a	Confróntese la bibliografía básica. Nos referimos a la cibernética, por cuanto, aborda problemas relacionados con la información.
3	a	Confróntese la bibliografía básica. El Derecho de la Informática surge como una derivación del Derecho Informático y como un modo de regular y legislar, tanto los contenidos como la información que se producen, a través, del uso de la web o cualquier medio electrónico, es decir se encarga de establecer normas para el uso o manejo adecuado de las tecnologías.
4	a	Confróntese la bibliografía básica. La Informática Jurídica Documental se encarga de procesar o crear documentos jurídicos o bases de datos que contengan compilación de las Leyes, Casación, Jurisprudencia, y la Doctrina del derecho.
5	c	Confróntese la bibliografía básica. La Informática Jurídica Decisional es aquella que con la aplicación de sistemas lógicos o expertos utiliza inteligencia artificial.
6	b	Confróntese la bibliografía básica. Según Téllez (2004) el Derecho Informático es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática).
7	c	Confróntese la bibliografía básica. Atendiendo a Ríos Estavillo (1997), en la Informática Jurídica documental, la información debe ser debidamente estructurada, mediante la aplicación de la Lógica o la Argumentación.
8	c	Confróntese la bibliografía básica. En la Informática Jurídica Decisional, en opinión de Asís (2022), el uso de IA en el ámbito de las decisiones judiciales puede ser una cuestión polémica.

Pregunta	Respuesta	Retroalimentación
9	b	Confróntese la bibliografía básica. Siguiendo a la Ley Orgánica de Transparencia y Acceso a la Información Pública, se distinguen cuatro clases o categorías de transparencia, a saber: activa, pasiva, colaborativa; y, focalizada.
10	a	Confróntese la bibliografía básica. En consonancia con la Declaración de Principios Interamericanos en materia de Neurociencias, Neurotecnologías y Derechos Humanos, elaborada por el Comité Jurídico Interamericano de la OEA, es fundamental vincular los avances de la neurotecnología con el marco de protección existente, incluyendo la dignidad, la no discriminación, la identidad, el derecho a la privacidad e intimidad, la salud física y mental, la prohibición de la tortura y los tratos crueles, inhumanos y degradantes, y el acceso a remedios judiciales, entre otros.

Ir a la autoevaluación

Autoevaluación 2

Pregunta	Respuesta	Retroalimentación
1	a	Confróntese la bibliografía básica. La Ley Modelo de la CNUDMI sobre Comercio Electrónico, también conocida como UNCITRAL, fue adoptada con el objetivo de proporcionar un marco normativo uniforme que facilite el comercio electrónico a nivel internacional.
2	b	Confróntese la bibliografía básica. El derecho informático aborda a la informática como su objeto de estudio (derecho de la informática). Por ello, considerando que el uso de TICs está estrechamente vinculado con el comercio electrónico, esta área se convierte en un objeto de estudio relacionado con el derecho de la informática.
3	a	Confróntese la bibliografía básica. Siguiendo la Carta Iberoamericana de principios y derechos en entornos digitales, el comercio electrónico debe ofrecer un adecuado "grado de protección de las personas consumidoras y usuarias en los entornos digitales".
4	c	Confróntese la bibliografía básica. En el caso del Ecuador es la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, aprobada en el año 2002, que es la que permite el uso de servicios electrónicos, lo cual incluye lo relacionado con el comercio electrónico.
5	c	Confróntese la bibliografía básica. Atendiendo a Ríos Estavillo (1997), en el contrato de leasing: las relaciones jurídicas se establecen entre el fabricante de material informático, la entidad financiera de leasing y el usuario. Entre el fabricante y la entidad financiera de leasing hay una compraventa, la entidad de leasing no utiliza el material y lo alquila al usuario juntamente con un compromiso de venta.
6	a	Confróntese la bibliografía básica. La RAE (2024) entiende que un documento electrónico es "todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual".
7	b	Confróntese la bibliografía básica. Un principio básico que debe atenderse es el de equivalencia funcional, por el cual un documento electrónico tiene el mismo valor jurídico que un documento tradicional.
8	b	Confróntese la bibliografía básica. Atendiendo a Téllez (2008), la firma digital es "el nombre que se da a cierto tipo de firma electrónica basada en el uso de criptografía, entre las cuales la más comúnmente usada es la llamada criptografía asimétrica o de llave pública".

Pregunta	Respuesta	Retroalimentación
9	c	Confróntese la bibliografía básica. En el marco del proceso de certificación electrónica, se advierte que “la criptografía necesita de una tercera parte de confianza, una entidad de certificación” (García, 2011, p. 161).
10	a	Confróntese la bibliografía básica. Entre los principios de los contratos informáticos se distinguen, por ejemplo, la inalterabilidad del derecho preexistente, la buena fe, la autonomía de la voluntad, la equivalencia funcional; y, la neutralidad tecnológica.

Ir a la autoevaluación

Autoevaluación 3

Pregunta	Respuesta	Retroalimentación
1	B	Confróntese la bibliografía básica. Puccinelli (2004) nos recuerda que, frente a la aparición del poder informático, estamos ante un derecho con contenidos diferenciales, que se constituye por "la suma de principios, derechos y garantías establecidos en favor de las personas que pudieran verse perjudicadas por el tratamiento de los datos de carácter personal a ella referidos" (p. 2).
2	C	Confróntese la bibliografía básica. La protección de datos personales es un derecho que se encuentra muy vinculado con la protección de la intimidad y la privacidad de las personas. Así lo ha destacado, incluso, la jurisprudencia de la Corte Constitucional.
3	A	Confróntese la bibliografía básica. Tanto la doctrina como la normativa de protección de datos personales de Ecuador distinguen que un dato personal es todo dato que identifica o hace identificable, directa o indirectamente, a una persona natural.
4	A	Confróntese la bibliografía básica. La normativa de protección de datos personales de Ecuador aclara que el objeto y finalidad es garantizar el ejercicio del derecho fundamental a la protección de datos personales, lo cual incluye su acceso y decisión.
5	C	Confróntese la bibliografía básica. Atendiendo la normativa de protección de datos personales de Ecuador, el principio de legalidad obliga a respetar las disposiciones contenidas en la Constitución y, en todo caso, la jurisprudencia e instrumentos internacionales.
6	B	Confróntese la bibliografía básica. Atendiendo la normativa de protección de datos personales de Ecuador, el principio de independencia del control es aplicable a la autoridad de protección de datos personales.
7	B	Confróntese la bibliografía básica. En el caso de Ecuador, el surgimiento del derecho a la protección de datos se enmarca en los principios consagrados dentro de la teoría del neoconstitucionalismo andino, fundamentalmente, en la constitucionalización de nuevos derechos y libertades.
8	C	Confróntese la bibliografía básica. Atendiendo a los derechos de libertad consagrados en la Constitución de Ecuador de 2008, la protección de datos personales se reconoce, por primera vez, como un derecho autónomo.

Pregunta	Respuesta	Retroalimentación
9	A	Confróntese la bibliografía básica. El derecho fundamental a la protección de datos personales, materializado a través de la garantía jurisdiccional del hábeas data, se ejerce mediante la tutela de los denominados “derechos ARCO”, es decir: acceso, rectificación, cancelación u oposición.
10	B	Confróntese la bibliografía básica. Atendiendo el catálogo de derechos previsto en el capítulo sexto de la Constitución de Ecuador, la protección de datos personales se identifica como un derecho de libertad.

Ir a la autoevaluación

Autoevaluación 4

Pregunta	Respuesta	Retroalimentación
1	A	Confróntese la bibliografía básica. Otra forma de hacer referencia a esta disciplina, desde la perspectiva del Código Orgánico Integral Penal, es llamándola "técnica digital forense".
2	B	Confróntese la bibliografía básica. La informática forense, esencialmente, está guiada por la intervención de las ciencias forenses que, mediante un método científico, emplea técnicas especializadas.
3	C	Confróntese la bibliografía básica. Constituye otra de las áreas que tiene especial interés para el derecho de la informática, mediante el estudio del derecho penal informático.
4	C	Confróntese la bibliografía básica. Según la Carta Iberoamericana, se busca promover estrategias y políticas iberoamericanas en relación con la prevención e investigación de los ciberdelitos.
5	B	Confróntese la bibliografía básica. Según la Carta Iberoamericana, mediante las estrategias se deben desarrollar capacidades y la creación y fortalecimiento de las redes de asistencia y cooperación iberoamericana.
6	A	Confróntese la bibliografía básica. Atendiendo a Pollitt et al. (2004), para conceptualización a la informática forense puede hacerse referencia a: computer forensics, media analysis y network forensics.
7	B	Confróntese la bibliografía básica. Atendiendo a Pollitt et al. (2004), el término cyber forensics se utiliza para referirse al proceso de adquisición, conservación, examen, análisis y presentación de pruebas digitales.
8	B	Confróntese la bibliografía básica. El principal objetivo de la informática forense es precautelar la evidencia de una infracción informática, desde una perspectiva estrictamente técnica.
9	A	Confróntese la bibliografía básica. Frente al aseguramiento de la evidencia digital, Bustamante (2020) menciona que las metodologías de investigación forense buscan establecer bases sólidas para el juzgamiento y la validez delante del fuero judicial.
10	C	Confróntese la bibliografía básica. En los últimos años, la normativa penal ecuatoriana ha tenido un desarrollo importante en lo concerniente a las actuaciones y técnicas especiales de investigación. Particularmente, llama la atención la incorporación del denominado agente encubierto informático.

Pregunta	Respuesta	Retroalimentación

Ir a la autoevaluación

Autoevaluación 5

Pregunta	Respuesta	Retroalimentación
1	A	Confróntese la bibliografía básica. En Ecuador la ley penal que regula el delito informático es el Código Orgánico Integral Penal. Este orden normativo, en su parte sustantiva (teórica) surge frente a las reformas de tipos penales obsoletos que no responden a las necesidades actuales de la población; y, en su parte adjetiva (procesal) como un orden procedimental orientado a garantizar los derechos y libertades de los sujetos procesales, particularmente, de las víctimas y de las personas procesadas.
2	B	Confróntese la bibliografía básica. En los antecedentes del COIP se señala que el derecho penal está destinado a determinar límites para no caer en la venganza privada ni en la impunidad. Por ello, dicha normativa ha tratado de adecuarse "a los nuevos desarrollos conceptuales que se han producido en el mundo y en la región, como mecanismo para asegurar un correcto funcionamiento de la justicia penal".
3	C	Confróntese la bibliografía básica. Una de las preocupaciones y, a la vez, un desafío para el derecho penal informático es "desarrollar un marco legal, políticas y acciones educativas que apunten a convertir la ciberseguridad y la lucha contra el cibercrimen y la violencia digital en un empeño colectivo orientado a garantizar los derechos de las personas".
4	B	Confróntese la bibliografía básica. En el contexto internacional, la Organización de Estados Americanos (OEA) precisa que las tipologías informáticas que marcan una tendencia emergente tienen relación con la pornografía por venganza, el asedio cibernético y la ingeniería social.
5	C	Confróntese la bibliografía básica. El COIP la define como una conducta típica, antijurídica y culpable que se clasifica en delitos y contravenciones.
6	A	Confróntese la bibliografía básica. El término delito informático se asocia a otros como: "delito digital", "delito electrónico", "infracción informática", "computer crime", entre otras.
7	A	Confróntese la bibliografía básica. El criminal compliance configura "una herramienta organizativa que cumple tres funciones principales: la prevención de delitos (función preventiva), su detección (función de detección), y su eficaz sanción y/o denuncia a las autoridades correspondientes para que si lo estiman oportuno inicien una investigación penal (función represiva)".

Pregunta	Respuesta	Retroalimentación
8	B	Confróntese la bibliografía básica. En la actualidad, el principio de accountability (responsabilidad proactiva) adquiere especial importancia en la teoría de la criminal compliance.
9	B	Confróntese la bibliografía básica. Julio Téllez define a los delitos informáticos desde un concepto típico y atípico.
10	B	Confróntese la bibliografía básica. El tipo penal que puede constituirse como un delito informático por la vía de acción privada es la calumnia, toda vez que según el Código Orgánico Integral Penal "la persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra, será sancionada con pena privativa de libertad de seis meses a dos años".
		Ir a la autoevaluación

5. Referencias bibliográficas

Asís, R. (2022). Derecho y tecnologías. Madrid: Dykinson

Código Orgánico Integral Penal (2014). Recuperado de: cepweb.com.ec

García, M. (2011). *Derecho de las nuevas tecnologías*. México: Instituto de Investigaciones Jurídicas de la UNAM.

Ley de Comercio Electrónico, Firmas y Mensajes de Datos (2002). Recuperado de cepweb.com.ec

Ordóñez, L. (2017). La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración. Revista de Derecho: Foro. Nro. 27. Quito: Universidad Andina Simón Bolívar.

Ordóñez, L. & Calva S. (2020). Amenazas a la privacidad de los menores de edad a partir del Sharenting. Revista Chilena de Derecho y Tecnología, Nro. 2. doi:10.5354/0719- 2584.2020.55333. https://rchdt.uchile.cl/index.php/RCHDT/article/view/55333

Ordóñez Pineda, L., Correa Quezada, L., & Correa Conde, A. (2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. Estado & Comunes, 2 (15), 77–97.

Ordóñez, L. (2025). Derecho Informático: Doctrina, legislación y jurisprudencia. Cuenca: CEDIA.

Páez, J. J. (2015). *Derecho y Tics*. Quito: Corporación de Estudios y Publicaciones.

Pérez-Luño Robledo, E. (2017). *El procedimiento de habeas data. El derecho procesal ante las nuevas tecnologías.* Madrid: Dykinson.

Téllez, J. (2008). *Derecho informático*. México: McGraw Hill.