UTPL
La Universidad Católica de Loja

Modalidad Abierta y a Distancia

Itinerario II-Derecho Privado: Derecho Informático

Guía didáctica

UTPL

Índice
Primer bimestre
Segundo bimestre
Solucionario
Referencias bibliográficas

Facultad de Ciencias Sociales, Educación y Humanidades
(Resolución Rectoral de Transición de la titulación de Derecho número RCT_RR_15_2021_V1)

Departamento de Ciencias Jurídicas

Itinerario II-Derecho Privado: Derecho Informático

Guía didáctica

Carrera	*PAO Nivel*
▪ *Derecho*	VI

Autor:

Ordóñez Pineda Luis Oswaldo

DERE_3051

Índice
Primer bimestre
Segundo bimestre
Solucionario
Referencias bibliográficas

Universidad Técnica Particular de Loja

Itinerario II-Derecho Privado: Derecho Informático
Guía didáctica
Ordóñez Pineda Luis Oswaldo

Diagramación y diseño digital:

Ediloja Cía. Ltda.
Telefax: 593-7-2611418.
San Cayetano Alto s/n.
www.ediloja.com.ec
edilojacialtda@ediloja.com.ec
Loja-Ecuador

ISBN digital - 978-9942-39-045-5

1 de marzo, 2021

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 específicas de la carrera

- Relaciona fenómenos globales con la realidad jurídica nacional.

1.4. Problemática que aborda la asignatura

El estudio de la relación entre el Derecho y la Informática constituye uno de los pilares fundamentales para los estudiantes de Derecho. En la sociedad moderna, el Derecho Informático plantea un enfoque transversal en el ejercicio de los derechos producto del avance vertiginoso de las tecnologías de la información y comunicación (TICs).

En este marco, esta asignatura propone un estudio de las diversas problemáticas y conflictos que las TICs plantean en la sociedad de la información. Precisamente, la incorporación de los procesos tecnológicos en las actividades jurídicas; posibilidades y amenazas en el comercio electrónico; las garantías que requiere la implementación de la firma electrónica; la protección de datos personales en la sociedad de la información; y, las conductas reconocidas como delitos informáticos, son algunas de las instituciones que plantean problemáticas relacionadas con: la privacidad; intimidad; transparencia, eficiencia y calidad en la administración pública; validez de los documentos electrónicos y, bienes jurídicos protegidos en la sociedad de la información, desde el ámbito penal. En suma, todos los fenómenos jurídicos globales que, a partir del desarrollo tecnológico, afectan a los derechos de las personas.

Por tanto, a través de un estudio interdependiente de las diferentes áreas de las ciencias jurídicas, que denotan la necesidad de abordarse desde el derecho informático, estas problemáticas serán abordadas atendiendo la realidad jurídica nacional.

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, en relación a los componentes de aprendizaje: de contacto con el docente (ACD); práctico-experimental (APE) y, de trabajo autónomo (AA), se plantea la siguiente metodología:

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 a distancia, 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.

Contenidos, recursos y actividades de aprendizaje

Estimado estudiante, para comprender la naturaleza del Derecho Informático, principalmente, haremos un análisis teórico de las instituciones jurídicas asociadas al Derecho y a la Informática. Así,

en primer término, se abordará al “Derecho Informático” como una disciplina de las ciencias jurídicas, en la cual converge el estudio de la Informática Jurídica y del 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 en esta guía didáctica, vinculando, principalmente, el aprendizaje por indagación.

Sin duda, al final de este primer bimestre estará en condiciones de aportar su propio criterio y definiciones vinculadas con la naturaleza del Derecho Informático.

Semana 1

Unidad 1. Derecho e Informática

1.1. Nociones preliminares

Estimado estudiante, para iniciar el estudio de este tema, tome en consideración que debe remitirse al texto básico “Primera Parte”, en donde encontrará una breve aproximación sobre la relación entre el Derecho y la Informática. Le propongo analizar esta parte.

Una vez revisados estos contenidos, se comprende que la sociedad ha experimentado diversos avances sociales, políticos, económicos y tecnológicos. Así, advertimos una nueva etapa denominada "revolución tecnológica", la cual nace como producto de los avances experimentados en la "sociedad de la información". En este aspecto, hay que considerar que ésta hace referencia al "uso masivo de las Tecnologías de la Información y Comunicación (TICs) para difundir el conocimiento y los intercambios en una sociedad" (Téllez, 2004, p.6).

La sociedad basada en el uso de tecnologías se convierte en un paradigma trascendental de nuestra cultura, hasta el punto que, para designar el modelo de nuestras relaciones interpersonales, mediante las TICs, alude, reiteradamente, para señalar a lo que conocemos como "sociedad de la información". Por tanto, se advierte que esta noción engloba "la contratación de bienes y servicios por vía electrónica, el suministro de información por dicho medio, las actividades de intermediación relativas a la provisión de acceso a internet, a la transmisión de datos por redes de telecomunicaciones" (RAE, 2020).

> **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 establecer nuevos marcos teóricos que permitan alojar los problemas y cuestiones surgidos de la interacción entre el Derecho y la Informática (Pérez, 1996, p.18). 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.

Ante el ineludible desarrollo de las TICs, los sistemas jurídicos deben encaminarse a regular las tensiones respecto a la garantía de los derechos fundamentales en la sociedad de información. Especialmente, aquellos relacionados con la dignidad humana, tomando en consideración que aquellos tienen como objeto central responder a la realidad que vivimos. 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, además, la sociedad de la información plantea trascender y adaptarse a nuevas posibilidades, que permitan agilitar las actividades relacionadas con el ejercicio del Derecho.

Esta temática es interesante ¿verdad? Entonces, luego de haber analizado esta parte, usted ya podrá elaborar su propia definición acerca de la relación entre el Derecho y la Informática. Si bien, hasta ahora, hemos determinado la relación jurídica, entre el derecho y las TICs. A continuación, se estudiará a la rama de las ciencias jurídicas encargada de estudiar estas conexiones. Vea a continuación:

1.2. Derecho Informático

Estimado estudiante, para comprender la esencia del "Derecho informático" es fundamental examinar, detenidamente, los contenidos desarrollados en el texto básico, bajo el tema "Concepto y clasificación de la informática jurídica".

Luego de este análisis, habrá determinado la naturaleza jurídica del Derecho Informático. No obstante, a continuación, efectuaremos 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, 2021), 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, 2021).

Notamos que el tratamiento automatizado de la información puede desembocar en un estudio o una regulación específica, desde una disciplina del Derecho. Precisamente, esta disciplina o rama de las ciencias jurídicas se denomina Derecho Informático, por cuanto, responde "a los problemas que la informática aporta como fenómeno multifacético" (García, 2011, p.97).

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).

Además, Pérez Luño (2007) considera que es una materia inequívocamente jurídica, conformada por el sector normativo de los sistemas jurídicos contemporáneos integrados por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir, la informática y la telemática (p. 84).

> **IMPORTANTE:** 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.

Es conveniente señalar que el texto básico define al Derecho informático como "la regulación, la norma jurídica que regula el uso de las nuevas tecnologías". Si bien, esta definición se asemeja al criterio de Pérez Luño. Hay que considerar que esta rama del

Derecho, no solamente, está compuesta por un esquema de regulación de las tecnologías o de la informática sino, además, por un componente instrumental, el cual supone la implementación de las TICs en la actividad jurídica.

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

1.3. Informática Jurídica

Estimado estudiante, en el texto básico encontrará una amplia perspectiva respecto a la conceptualización de la Informática Jurídica. Por lo 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 maquinas 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).

Ahora bien, de la revisión de los conceptos señalados en el texto básico, una definición completa es la que ofrecen los autores Hayna, Lagreza y Muñoz, quienes consideran que la Informática Jurídica consiste en las posibles aplicaciones de la informática en el ejercicio del derecho tanto en sus aspectos legislativos, como judiciales y profesionales (Páez, 2015, p. 31). 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 la informática jurídica se identifica con el uso de la tecnología en la actividad jurídica, es fundamental aclarar que la compilación de la información jurídica por medios electrónicos –con la intervención del jurista y cuando el objeto de análisis es de índole jurídica- centra su objeto en tres asuntos fundamentales, a saber: (Páez, 2015, p. 30).

- Tratamiento de la información.
- Utilización de mecanismos automáticos.
- Información de carácter jurídico.

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, Pérez considera que el carácter instrumental del Derecho Informático, es decir, la informática jurídica es una disciplina bifronte en la que se entrecruzan una metodología tecnológica con su objeto jurídico que, a su vez, condiciona las propias posibilidades o modalidades de tal aplicación (2007, p. 84). En este sentido, esta disciplina dedica su estudio al tratamiento automatizado de: fuentes de conocimiento jurídico (..) fuentes de producción jurídica (..) y los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el derecho.

Lo invito a reforzar sus conocimientos, participando en la siguiente actividad recomendada:

Actividades de aprendizaje recomendadas

Primera actividad: En el entorno virtual de aprendizaje, usted encontrará el documento “Internet y Derecho”. La revisión de este recurso educativo, le permitirá afianzar su conocimiento, respecto a la relación entre en el Derecho y las TICs.

A partir de los modelos de control y libertad en Internet, este análisis nos permitirá concluir que las restricciones, frente al uso de las TICs son cuatro, a saber: la ley, las normas sociales, el mercado y la “arquitectura”. Así también, la Declaración de Independencia del Ciberespacio presenta un interesante paradigma, en cuanto a los problemas que plantea el esquema de regulación en Internet.

En este orden, la pregunta que se intenta responder es si, ¿el Ciberespacio es diferente al mundo real y, por tanto, existiría una imposibilidad para regular las conductas y relaciones en este espacio virtual?

Segunda actividad: La doctrina advierte una necesaria distinción entre el Derecho Informático, el Derecho de la Informática y la Informática Jurídica. Para este fin, le recomiendo consultar el siguiente documento: Derecho de la Informática, capítulo cuarto, en donde se ejemplifica el objeto de estudio de las disciplinas que se anotan.

De la revisión de este documento, identificamos que el Derecho Informático alude al estudio de la relación entre el Derecho y la Informática y, en donde convergen dos disciplinas que nacen de su análisis teórico o normativo (Derecho de la Informática) y de su contexto práctico o instrumental (Informática Jurídica).

Según lo expuesto, el problema que se trata de resolver es si, ¿nuestro objeto de estudio debería hacer referencia al "Derecho Informático o al Derecho y a la Informática"?

Semana 2

1.3.1. Clasificación y fuentes de la Informática Jurídica

Estimado estudiante, los contenidos relativos a la "clasificación de la informática jurídica" se encuentran, debidamente, ampliados en el texto básico, en donde se detallan sus niveles o clasificación. Por ello, previo a revisar este tema, se sugiere analizar esta temática con la finalidad de determinar la naturaleza de las vertientes o fuentes relacionadas con los documentos, la gestión y la toma de decisiones.

En este orden, previo a identificar la clasificación de la Informática Jurídica, realicemos un breve resumen de lo que hasta ahora hemos puntualizado.

RECAPITULEMOS:

Derecho e Informática

Pues bien, luego de haber puntualizado estos conceptos, a continuación, abordaremos el último tema de esta Unidad, el cual refiere a 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 fuente se encuentra relacionada con la creación de documentos que contienen información jurídica referente a legislación, jurisprudencia o casación y a la doctrina del derecho (Páez, 2015, p. 1). 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 "estudia el tratamiento automatizado de las fuentes de conocimiento jurídico, a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal (Pérez, 1996, p.84).

En este sentido, dentro de la Informática Jurídica evidenciamos que la informatización documentaria consiste en un sistema, mediante el cual se puede hacer una búsqueda rápida, clara y pertinente de lo que se está buscando en la información ya guardada.

> **RECUERDE:** Para encontrar las ventajas de esta fuente de la informática jurídica: primero, se debe conocer cómo está estructurada la información; segundo, aprender a buscar y ordenar la búsqueda de los datos; y tercero, saber personalizar la información recuperada.

La informática jurídica documental se convierte en una herramienta para almacenar grandes cantidades de información. 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); en el caso

de los juristas este paradigma exige aprender las diferentes formas de consultar, recuperar y aprovechar la información jurídica en entornos tecnológicos.

Para ilustrar mejor, en el texto básico se describen los elementos estructurales de la organización, la búsqueda y la recuperación de la información jurídica. En este orden, a partir de los mecanismos de automatización de los datos que contienen información jurídica, identificamos que la Informática jurídica documental se convierte en una herramienta de uso de los juristas, la cual tiene por objeto procesar, sistematizar información, a través, de bases de datos. Por lo que, su desarrollo depende de los avances de la informática o computación, respecto al procesamiento lógico de la información.

B. Informática jurídica de gestión

Esta vertiente conceptualiza la sistematización de la información jurídica, la cual desarrolla o gestiona el jurista en forma diaria. Por tanto, hace referencia a la actividad que desarrolla el jurista en sus actividades cotidianas, elaborando escritos, providencias, sentencias, entre otros. Es decir, comprende todos los ámbitos, tanto jurídicos como administrativos, que involucran la gestión diaria, dentro de una oficina jurídica, instancia o dependencia judicial.

> **IMPORTANTE:** La Informática jurídica de gestión se presenta en el mundo jurídico en forma de programas de software de gestión jurídica.

A partir de los programas de gestión jurídica, el sistema de información se desarrolla tomando en cuenta la tarea, gestión o actividad que le corresponde a cada persona. Por tanto, es necesario:

- Contar con organigrama funcional.
- Establecer niveles de organización de la información.
- Identificar el sistema de información.

En este aspecto, el texto básico destaca que para el desarrollo de los sistemas informáticos de gestión se requieren cinco etapas principales, las cuales están relacionadas con el diseño, la programación, las pruebas, la implantación y la actualización y mantenimiento.

Bajo estas consideraciones, se concluye que la Informática jurídica de gestión comprende el procesamiento de la información relacionada con la gestión diaria de las actividades jurídicas, por lo que, también, recibe el nombre de "ofimática" o "burocrática". En todo caso, tiene la característica de organizar la información de hoy para el futuro. Por tanto, tiene que ser procesada diariamente y ser actualizada (Páez, 2015, p. 16).

C. Informática jurídica decisional

Esta fuente de la Informática jurídica representa la aplicación de sistemas lógicos o programas, a través del uso de la inteligencia artificial o sistema jurídicos expertos, los cuales son utilizados para la toma de decisiones de los juristas. Este proceso que se aplica, desde la informática decisional, "debe 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).

> **IMPORTANTE:** Inteligencia Artificial alude al conjunto de actividades informáticas realizadas por el hombre, considerándose estos aspectos técnicos como producto de su inteligencia.

Es importante reflexionar que la inteligencia artificial y el poder sobre las tecnologías son del hombre. 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).

En este plano, tomando en cuenta que en esta vertiente de la Informática Jurídica intervienen programas o software que se convierten en herramientas del jurista para la toma de decisiones a través de "sistemas expertos"; 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).

Bajo estas consideraciones, se concluye que el objeto de la informática decisional se enmarca en la integración de procedimientos computacionales dirigidos a sustituir o reproducir las actividades del jurista. Así, los sistemas expertos desarrollan e incorporan en forma práctica y operativa programas destinados a resolver casos jurídicos complicados tales como: liquidaciones de impuestos y simulaciones para determinar indemnizaciones. En este sentido, destacamos que "la contribución de la informática jurídica al campo de la toma de decisiones es trascendental, pero conviene recordar que la racionalidad de la toma de decisiones consiste en hacer mínima la incertidumbre que ellas puedan generar" (García, 2011, p. 101).

Finalmente, advertimos que, en la clasificación de la informática jurídica, además pueden distinguirse otras dos fuentes o vertientes. En esta parte, se hace referencia a la Informática Jurídica Registral, la cual consiste en el registro de datos jurídicos; y, adicionalmente, a la informática Jurídica Metadocumental o Metadecisional, que se conforma por bases de conocimiento jurídico.

Lo invito a reforzar sus conocimientos, desarrollando lo siguiente:

Actividades de aprendizaje recomendadas

Primera actividad: 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.

Segunda actividad:

Considerando la existencia de la Informática jurídica metadocumental o metadecisional, mediante el análisis del documento sugerido en la primera actividad, puede identificarse, además, la inclusión de herramientas informáticas que son aplicables a otros escenarios, como la educación. En este marco, de conformidad a la subdivisión de esta clase de Informática Jurídica, le propongo resolver el siguiente problema:

CASO PRÁCTICO

A propósito de la emergencia sanitaria originada por el COVID-19, en Ecuador se evidenciaron serias dificultades para canalizar los procesos de enseñanza-aprendizaje en el sistema educativo. En este contexto, la CIDH, mediante la Resolución 4/2020 sobre derechos humanos de las personas con COVID-19, advirtió que, para el pleno ejercicio del derecho a la educación de las personas, “bien por

sufrir la enfermedad directamente o en el núcleo de sus familias, los Estados deben prever dentro de los diferentes niveles de sus sistemas educativos, la implementación de medidas que mitiguen la posible interrupción de los estudios y se enfoquen en la reducción del abandono de los mismos".

De esta manera, conociendo el desarrollo que ha tenido la informática jurídica:

¿Cómo solucionaría este problema, a través de la Informática jurídica metadocumental o metadecisional?

¿Cómo aplicaría, en el caso que se propone, los elementos que son indispensables para el funcionamiento de los sistemas de enseñanza asistidos por computadora?

Lo invito a reforzar sus conocimientos, participando en la siguiente autoevaluación:

Autoevaluación 1

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.

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

1. Informática jurídica significa:

   a. Recuperación de datos y preservación de evidencia.
   b. Procesamiento de información jurídica por medios electrónicos.
   c. Detección de seguridad y auditoria de privacidad informática.

2. Refiere al objeto de estudio de la informática jurídica:

   a. Uso de la tecnología en la actividad jurídica.
   b. Peritaje informático forense y evidencias digitales.
   c. Localización de delincuentes informáticos.

3. Derecho de la Informática significa:

   a. Normativa destinada a regular el uso de las tecnologías de la información y comunicación.
   b. Derecho a tener acceso a las tecnologías de la información y comunicación.
   c. Derecho a la información y comunicación.

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. Inteligencia artificial.
   b. Software de gestión jurídica.
   c. Sistemas expertos.

6. La naturaleza del Derecho de la Informática se vincula como:

   a. Objeto de estudio del derecho informático.
   b. Instrumento de aplicación en el derecho informático.
   c. Derecho a acceder a las TICs.

7. La Informática Jurídica, entre otras disciplinas, incluye una relación con la:

   a. Criminalística.
   b. Informática Forense.
   c. Lógica y la lingüística.

8. La informática jurídica documental enfrenta problemas como:

   a. La regulación normativa.
   b. Representación y el procesamiento de los significados de los textos.
   c. La regulación jurisprudencial.

9. La propiedad intelectual se relaciona con la informática jurídica por:

   a. Los niveles de indización.
   b. Los elementos estructurales de la documentación.
   c. El régimen de protección de los derechos de autor y propiedad industrial.

10. Un ejemplo de sistemas expertos es:

   a. www.derechoecuador.com.
   b. Sistemas tributarios en liquidaciones de impuestos.
   c. Sistemas dentro de la estructura de un Ministerio.

Finalmente, una vez que ha decidido resolver los enunciados propuestos, le propongo comparar sus respuestas con el solucionario que se encuentra en la parte final de esta guía didáctica.

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

Ir al solucionario

Resultado de aprendizaje 2

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

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, doctrinaria 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.

Semana 3

Unidad 2. Derecho y Tics

2.1. Comercio electrónico

Estimado estudiante, 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. Así, en esta primera parte, desde el Derecho de la Informática, se enfocará en el estudio del comercio electrónico y los documentos electrónicos.

Como introducción a este tema, en el texto básico "Segunda Parte" encontrará los antecedentes respecto al desarrollo del denominado "comercio electrónico", en donde la conceptualización más importante es la que realiza la "National Institute of Standards and Technology", considerando al comercio electrónico como "la integración de servicios de Comunicaciones, Administración de Datos y Seguridad para permitir que aplicaciones de negocios intercambien información automáticamente" (Páez, 2015, p. 39).

Ahora observe algunas características sobre el 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	Rapidez en transacciones de productos y servicios.
	Compra de bienes y servicios mediante el uso de la tecnología.
	Satisface necesidades electrónicamente.
	Se desenvuelve en un medio que ha desarrollado sistemas de seguridad para garantizar transferencia de datos.
	Las transacciones se llevan a cabo automáticamente a través de entidades bancarias.
	Abarca entre otras temáticas: mensajes de datos, documentos electrónicos, contratación electrónica, firma electrónica, gobierno electrónico, protección de datos, etc.

Fuente: Páez, J. (2015).
Elaboración: Ordóñez, L. (2021).

¿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 ordenamiento legal en Ecuador.

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). Tomando en cuenta este antecedente, precisamente, el profesor Davara Rodríguez en Páez (2015) advierte que el comercio electrónico constituye aquella actividad que "se lleva a cabo utilizando la herramienta electrónica de forma que tenga o pueda tener alguna influencia en la consecución del fin comercial o en el resultado de la actividad que se está desarrollando" (p. 41).

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 y certificación electrónica nacional e internacional. 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).

2.2. Documentos electrónicos

Estimado estudiante, el tema "documentos electrónicos" se encuentra desarrollado en el texto básico, en donde se recalca la importancia de que, tanto en el ámbito público como privado, se debe priorizar el uso de medios telemáticos, especialmente, el documento electrónico.

De la revisión de estos contenidos, se identifica que, según la LCE, el documento electrónico se equipara al contenido de un mensaje de datos y, en suma, de conformidad a lo dispuesto por el art. 2 de

dicha Ley, sobre el reconocimiento jurídico de los mensajes de datos, éstos tendrán igual valor jurídico que los documentos escritos. Así, atendiendo este principio de equivalencia funcional, el documento, sea escrito o electrónico, "representa alguna cosa apta para esclarecer un hecho o se deja constancia de una manifestación de voluntad que produce efectos jurídicos" (García, 2011, p. 107).

En cualquier caso, la primera inquietud sobre este tema, más bien, estaría relacionada con la definición de un mensaje de datos, por cuanto, un documento electrónico es, en sí mismo, un mensaje de datos. Como determina el "Glosario de términos" de la LCE, 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. 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:** Conforme a las exposiciones señaladas, un documento electrónico hace referencia a todos los documentos que son emitidos por medios electrónicos, magnéticos, digitales o informáticos.

En este orden de ideas, el documento electrónico vincula, necesariamente, el desarrollo y la estructuración de un sistema de información. Por ello, hay que señalar que, según el "Glosario de términos" de la LCE, 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".

Así, se desprende 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, cumpliendo los requisitos exigidos por las Leyes Tributarias, Mercantiles y más normas y reglamentos vigentes".

Es preciso identificar que el documento electrónico alude a casos en que el lenguaje magnético constituye la acreditación, materialización o documentación de una voluntad, de la misma manera que se lo hace mediante un documento escrito. 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).

> **TOME NOTA:** El documento electrónico se define como toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, recogida en cualquier tipo de soporte con eficacia probatoria o relevancia jurídica; y, al tenor de la LCE, poseen los mismos elementos que un documento escrito de soporte en papel.

Ahora bien, hemos destacado que la validez y reconocimiento del documento electrónico responde al principio de equivalencia funcional. Considerando las exposiciones que se señalan en el texto básico, este principio "permite aplicar a los soportes informáticos un principio de no discriminación respecto de las declaraciones de voluntad, independientemente de la forma en la que hayan sido expresadas" (Páez, 2015, p. 371).

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 cuanto, "los mismos efectos que surte la manifestación de la voluntad instrumentada a través de un documento en papel, deben producirse independientemente del soporte utilizado en su materialización" (Páez, 2015, p. 371).

2. Al constituirse como un medio probatorio, conforme los dispone la LCE, 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 (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002).

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).

En esta parte continuaremos con su aprendizaje mediante su participación en la actividad que se describe a continuación:

Actividades de aprendizaje recomendadas

Primera actividad: Considerando que algunos países, para la elaboración del marco legal sobre comercio electrónico, la Ley Modelo de la UNCITRAL sirvió de referencia, en este documento encontrará el contenido de la Resolución aprobada por la Asamblea General de las Naciones Unidas.

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.

Segunda actividad: En la obra denominada: Derecho de las nuevas tecnologías - Capítulo tercero, sobre el documento electrónico y la firma electrónica - 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.

Semana 4

2.3. Firma electrónica

Estimado estudiante, el desarrollo del comercio electrónico y la producción de bienes y servicios, mediante vías informáticas o telemáticas ha concretado, tanto en el sector público como privado, la necesidad de establecer parámetros de seguridad, por medio del uso de técnicas que surgen de la criptografía. 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 verá disminuida" (García, 2011, p. 127).

A diferencia de las seguridades que en el mundo físico se exige a todo documento, en el ciberespacio o sociedad de la información se plantea la necesidad de incorporar técnicas de encriptación, mediante cualquier método basado en sistemas y/o servicios electrónicos, los cuales resultan en la aplicación de la firma electrónica. Por tanto, 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).

> **IMPORTANTE:** Dentro del tema relativo a la firma electrónica especial importancia tienen los servicios electrónicos. Al respecto, según el "Glosario de términos" de la LCE un "servicio electrónico" es "toda actividad realizada a través de redes electrónicas de información".

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, 2021). 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

Estimado estudiante, las nociones de seguridad y criptografía son tan antiguas como la escritura. Las primeras civilizaciones que usaron la criptografía fueron la egipcia, la Mesopotamia, la India y la China. Al respecto, el texto básico de nuestra asignatura destaca que, por ejemplo, algunos textos judíos fueron encriptados siguiendo el método de sustituir la primera letra del alfabeto por la última y así sucesivamente (Páez, 2015, p. 52).

En sentido general, puede decirse que la criptografía estudia los procesos de cifrado y descifrado de los mensajes, así como el análisis de los criptogramas para descubrir la clave y el texto original. 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).

> **RECUERDE:** La etimología de la palabra criptografía es: Kriptos (oculto) y Graphos (escribir).

Dicho lo anterior, se advierte que existen sistemas de seguridad simétricos y asimétricos. El primero maneja una sola clave; y, el segundo claves diferentes para el proceso de cifrado y descifrado. En todo caso, 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.

> **IMPORTANTE:** La criptografía con clave pública se constituye como un método para el intercambio seguro de mensajes que ha superado a la criptografía simétrica o con clave privada.

Finalmente, es preciso señalar que entre los aspectos técnicos más importantes que presenta la firma electrónica, como una garantía de seguridad y encriptación de las comunicaciones, se derivan cuatro bloques normativos, a saber:

A. Seguridad técnica.
B. Seguridad Jurídica.
C. Seguridad Mercantil o económica.
D. Seguridad a los consumidores.

En relación a estos bloques normativos, identificamos que en el texto básico se destaca la importancia de proteger las comunicaciones privadas; establecer un marco jurídico adecuado; evitar el abuso de las empresas; y garantizar el marco jurídico de las transacciones internacionales.

Ahora bien, 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. Diferencias entre firma electrónica y firma digital

Estimado estudiante, 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, 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).

El avance de los procesos de contratación y transacciones en el comercio electrónico, dentro de la sociedad de la información, mediante la vía telemática, requiere de procesos informáticos que ofrezcan seguridad en relación a la autenticidad y a la identidad de los intervinientes. Como se explica en el texto básico, la firma electrónica "apunta, precisamente, a que las partes en un negocio electrónico puedan autenticar todos y cada uno de los mensajes que hayan intercambiado" (Páez, 2015, p. 77). Por tanto, en términos de negocios o contratos electrónicos surgen dos instituciones relacionadas –firma electrónica y firma digital–, las cuales tienen el mismo objeto, pero distinta naturaleza como veremos a continuación.

A. Firma electrónica

Según el art. 13 de la LCE, 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".

Conforme a esta definición, se advierte que la firma electrónica 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 un género, caracterizado por el soporte: todo método de identificación de autoría basados en medios electrónicos" (Páez, 2015, p. 87).

> **RECUERDE:** Una especie de firma electrónica es la firma digital, entendida como aquella que se crea usando un sistema de criptografía asimétrica.

En este orden de ideas, 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, Titulo 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, la persona que recibe el mensaje lo puede desencriptar con la clave pública del firmante, a fin de verificar que su transformación coincida con el mensaje encriptado, a través de la clave privada del firmante.

> **RECUERDE:** 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 el texto básico, cuando se utiliza una firma digital "se aplican presunciones *iuris tantum* sobre la identidad del firmante y la integridad del documento que firmó" (Páez, 2015, p. 87). 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:

- Integridad de la Información.
- Autenticidad del origen del mensaje.
- No repudio.

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

Corresponde señalar que, en el texto básico se explica que la firma digital se caracteriza por los siguientes elementos:

- Objetivo-soporte.
- Subjetivo.
- Esfera de control del titular.
- Derechos de verificación del receptor.

Bajo estas supuestos, entendemos que en la firma digital: el soporte no es escrito; se identifica a la persona, la cual refiere una aprobación respecto al mensaje; ésta pertenece únicamente al titular; y se requiere la existencia de sistemas de verificación, que aseguren la autoría.

Finalmente, le propongo identificar las diferencias entre la firma electrónica y firma digital. Preste atención al siguiente recurso:

Diferencias entre firma electrónica y firma digital

Lo invito a reforzar sus conocimientos, participando en la actividad que se detalla a continuación:

Actividades de aprendizaje recomendadas

Primera actividad: Sobre la discusión de los sistemas de clave privada (simétrica) versus el sistema dual de pública y privada (asimétrica), el texto básico identifica los métodos que utilizan cada sistema, a partir de un conjunto de garantías que aseguran la protección de la información. Así, se plantean dos casos. Uno relacionado con la criptografía con clave privada y, otro enfocado con la criptografía con claves complementarias.

Luego de analizar estos casos, primero, encontrará algunas limitaciones relacionadas con la protección a la privacidad; y, segundo, con la lentitud para encriptar grandes volúmenes de información.

Segunda actividad: Tomando en cuenta que el texto básico describe que el proceso de firma comprende que: 1) El usuario prepare el mensaje y use la función hash; 2) El remitente encripte el resumen, una su firma a los datos y, envíe electrónicamente la firma y el mensaje original; y 3) El destinatario use la clave pública del remitente, realice un resumen, utilizando la función resumen y, compare que los datos no han sido alterados. Le propongo construir un caso que identifique cada fase de este proceso.

Semana 5

2.4. Certificados electrónicos y entidades de certificación

Estimado estudiante, 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. 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".

> **IMPORTANTE:** El certificado constituye un documento electrónico que contiene un conjunto de información, la cual está vinculada a una clave pública de una persona o entidad determinada.

Para comprender mejor, el sistema de certificados de clave pública supone la participación de los siguientes sujetos:

- Titular del certificado.
- Usuario o persona que confía en el certificado.
- Entidad de certificación.

Respecto a la descripción de los sujetos (titular y usuario) que participan en los certificados electrónicos, el texto básico advierte que, por una parte, el titular es la persona "que tiene legítimamente la clave privada correspondiente a la clave pública que contiene el certificado" (Páez, 2015, p. 97). Por otra que, el usuario es la persona "que obtiene la clave pública del suscriptor a través del certificado y que actúa basándose en él y en la clave pública que contiene" (Páez, 2015, p. 97).

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 se emplea para certificar la identidad del titular de una firma electrónica. Así pues, el texto básico identifica un ciclo vital del certificado, plasmado en "tres aspectos principales: la generación y emisión, la distribución y la vigencia del mismo" (Páez, 2015, p. 98).

Con el objeto de ampliar el estudio de este tema, se sugiere revisar las disposiciones legales del Capítulo 2, Titulo 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, 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:** La tercera parte de confianza que desempeña la función de emisión de certificados se conoce como autoridad o entidad de certificación, prestador de servicios de certificación o, simplemente, certificador.

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].

[1] Según el texto básico, el CONATEL o Consejo Nacional de Telecomunicaciones y la Superintendencia de Telecomunicaciones son organismos de autorización y control de las entidades de certificación, respectivamente. No obstante, en virtud de los cambios estructurales y orgánicos, precisamos actualizar esta referencia, por la institución que queda anotada en esta parte.

IMPORTANTE: 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. Para identificar estas entidades, le sugiero consultar el enlace: https://www.arcotel.gob.ec/?s=entidades+de+certificaci%C3%B3n

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, Titulo 2, de la LCE en relación a las entidades de certificación. Dentro de esta revisión, habrá determinado 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.

Lo invito a reforzar sus conocimientos, participando en la siguiente autoevaluación:

Autoevaluación 2

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:

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

1. El orden jurídico para el comercio electrónico en Latinoamérica surgió de:

   a. Ley modelo de comercio electrónico de la UNICITRAL.
   b. Las Directivas de la Unión Europea.
   c. La Secure Electronic Transaction.

2. El comercio electrónico en Europa se regula a través de:

   a. La Constitución.
   b. Directivas.
   c. Instrumentos internacionales.

3. Un área de estudio del comercio electrónico es:

   a. El gobierno electrónico.
   b. La Informática jurídica documental.
   c. La Informática jurídica decisional.

4. En Ecuador, el orden jurídico del comercio electrónico se regula por:

   a. Código de Comercio.
   b. Código Monetario.
   c. Ley de Comercio Electrónico, Firmas y Mensajes de datos.

5. La primera ley que reguló los aspectos jurídicos del documento electrónico nació en:

   a. Alemania.
   b. Estados Unidos.
   c. México.

6. El documento electrónico hace referencia a:

   a. Documentos magnéticos, digitales o informáticos.
   b. Telefonía y voz por IP.
   c. Aplicaciones sobre Wireless.

7. El documento no electrónico hace referencia a:

   a. Correo electrónico.
   b. Registros electrónicos.
   c. Documentos micrograbados.

8. La firma digital es:

   a. Una expresión de voluntad en un medio o soporte en papel.
   b. El reemplazo de la firma ológrafa por medios electrónicos.
   c. Un avance criptográfico de la pericia digital forense.

9. La firma digital se constituye por:

   a. La firma analógica o convencional.
   b. La firma ológrafa.
   c. Matemáticas aplicadas, a través, de algoritmos de criptografía.

10. Una especie de la firma electrónica es:

a. La firma convencional.
b. La firma digital.
c. La criptografía.

Una vez que ha decidido resolver los enunciados propuestos, le propongo comparar sus respuestas con el solucionario que se encuentra en la parte final de esta guía didáctica. ¡Continuemos con la revisión de la siguiente Unidad!.

Ir al solucionario

Semana 6

Unidad 3. Contratación electrónica y régimen jurídico de protección de datos personales

3.1. Contratos electrónicos

3.1.1. Nociones preliminares

Estimado estudiante, este tema se encuentra desarrollado en el texto básico “Segunda Parte”. A partir de estos contenidos, usted podrá encontrar una aproximación al concepto de los contratos electrónicos e identificar los elementos jurídicos e informáticos de los principales contratos electrónicos. De esta manera, se sugiere revisar las siguientes apreciaciones.

Como queda anotado, las tecnologías de la información y comunicación permite beneficiar, entre otras actividades, el comercio electrónico, mediante la contratación de bienes y servicios de la sociedad de la información. Así, “aparece un elemento importante. El contrato, que es un negocio jurídico entre vivos, en el cual sus participantes hacen una declaración conjunta de voluntades con la finalidad de reglar sus relaciones jurídicas presentes y futuras” (Páez, 2015, p. 107).

En primer término, 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".

Finalmente, conforme a los contenidos señalados en el texto básico, se pueden distinguir dos conceptos. Uno relacionado con los contratos informáticos y otro con los contratos electrónicos. El primero, constituye "todo aquel que tenga como objeto u bien o un servicio informático" y el segundo, "todo aquel contrato (tradicional o no) que se haya realizado por ese medio (electrónico", lo cual no sólo se limita a Internet, sino a tecnologías anteriores como el Fax o posteriores, aun en desarrollo" (Páez, 2015, p. 108).

Para ilustrar mejor, el texto básico identifica tres teorías que conceptualizan a los contratos informáticos de diferente manera. Al caso, usted podrá examinar en el texto básico la referencia de las teorías antes mencionadas con el objeto de precisar la naturaleza jurídica de este tipo de contratos. En este orden de ideas y a la luz de la teoría que pretende definir al contrato informático desde su objeto, puede decirse que éste es todo aquel que tenga como objeto un bien o un servicio informático.

> **IMPORTANTE:** En sentido estricto, el contrato electrónico se denomina "contrato a distancia", por cuanto se realiza por vía electrónica o telemática.

Nótese entonces que, el contrato electrónico, también se lo conoce con el nombre de "contrato por medio de las nuevas tecnologías" o "contrato telemático", etc.

Ahora bien, respecto a la validez de este tipo de contratos, 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".

En este marco, un aspecto fundamental que hay que destacar 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".

> **IMPORTANTE:** Con el fin de profundizar en las reglas aplicables a la jurisdicción para la resolución de conflictos, ante la falta de cumplimiento, se sugiere analizar con detenimiento el Art. 47 de la LCE.

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

3.1.2. Clasificación

Conforme a las explicaciones que se señalan en el texto básico, se distingue las siguientes clases de contratos informáticos:

1. De hardware.
2. De software.
3. De instalación de llave en mano.
4. De servicios auxiliares.
5. Por su objeto.
6. Por el negocio jurídico.
7. Complejos.

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. "Por ejemplo, clausulas especiales que no recoge la normativa, por lo que amerita actualizar la legislación" (Páez, 2015, p. 109). En todo caso, la doctrina conviene en vincular dichos principios,

a la luz de los contratos tradicionales. A continuación, se señala los siguientes:

- Consentimiento.
- Causa lícita.
- Objeto lícito.

> **IMPORTANTE:** En el texto básico se realiza un interesante análisis de cada uno de estos elementos. Le sugiero revisarlos a fin de contextualizar su naturaleza.

En este caso, debe señalarse que la LCE sobre los contratos electrónicos refiere que "el perfeccionamiento de los contratos electrónicos se tendrá como lugar de perfeccionamiento el que acordaren las partes. La recepción, confirmación de recepción, o apertura del mensaje de datos, no implica aceptación del contrato electrónico, salvo acuerdo de las partes".

Ahora bien, por tratarse de una nueva forma de contratación, esta manifestación de los contratos tradicionales presenta una serie de características particulares, las cuales se describen a continuación. Preste atención a la siguiente tabla.

Tabla 2.
Características de la contratación informática.

	CONTRATACIÓN INFORMÁTICA
CARACTERÍSTICAS	Las operaciones se realizan por vía electrónica o digital.
	Prescinde del lugar donde se encuentran las partes.
	No quedan registrados en papel.
	La importación del bien no pasa por las aduanas.
	Se reducen, drásticamente, los intermediarios.
	Se materializan, rápidamente, las transacciones.

Fuente: Páez, J. (2015).
Elaboración: Ordóñez, L. (2021).

Luego de haber revisado esta parte. A continuación, le propongo revisar la siguiente tabla, en donde se identifican algunas nuevas clases de contratos informáticos. Preste atención.

Tabla 3.
Nuevas clases de contratos informáticos.

	CONTRATOS INFORMÁTICOS
CLASE Y/O NOMBRE	Shrinkwrap y Webwrap.
	Electronic Data Interchange.
	De Servicios por Internet.

Fuente: Páez, J. (2015).
Elaboración: Ordóñez, L. (2021).

De las nuevas clases que se anotan, encontramos, por ejemplo, el contrato de licencia de uso de software, en el cual los usuarios de software pueden utilizar el programa de ordenador respetando los derechos de autor protegidos por la licencia. (Páez, 2015, p. 117). Como se puede identificar, la naturaleza propia de los contratos informáticos responde siempre al objeto que materialice el negocio jurídico, siempre y cuando, en esta relación exista la intervención de las TICs.

Continúe con el aprendizaje mediante la participación en la siguiente actividad:

Actividades de aprendizaje recomendadas

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 redactarse un contrato informático.

Semana 7

3.2. Marco de protección y garantía del derecho fundamental a la autodeterminación informativa

Para aclarar el contenido del derecho a la autodeterminación informativa o de protección de datos personales, es necesario que acuda al texto básico y revise, detenidamente, tanto el marco legal de protección como las consideraciones que hace la doctrina, respecto a esta libertad informática.

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 habeas 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, lo invito a continuar con la revisión de este interesante tema.

3.2.1. Conceptualización y definiciones

Luego de las precisiones señaladas, puntualizamos que Dávara en Páez (2015) hace referencia al término "protección de datos", en cuanto a la protección jurídica de la persona, frente a la tecnología que automatiza sus datos. Así, lo que se pretende es proteger al individuo ante la manipulación no autorizada de la información personal.

Este tema es muy interesante, ¿verdad? Ahora, como usted recuerda, 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 adquiere especial importancia, a través del reconocimiento de derechos como la libertad informática, autodeterminación informativa o, simplemente, de protección de datos personales.

Ahora bien, en el texto básico se realiza un estudio interesante acerca de la protección de este derecho, dentro del ámbito constitucional en Ecuador. Por tanto, para comprender mejor este apartado debe revisar los contenidos que se sugieren en el texto base de la asignatura.

Por otra parte, 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

> **RECUERDE:** 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 tomar en consideración que dicha Ley determina que "son accesibles al público y susceptibles de tratamiento los datos personales referentes al contacto de profesionales y los datos de comerciantes, representantes y socios y accionistas de personas jurídicas y servidores públicos, siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo y se trate de nombres y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, y, número de teléfono profesional. En el caso de los servidores públicos, además serán de acceso público y susceptibles de tratamiento de datos, el histórico y vigente de la declaración patrimonial y de su remuneración" –art. 2–.

> **IMPORTANTE:** Con el objeto de profundizar el estudio de este derecho fundamental, le sugiero revisar el siguiente artículo: https://revistas.uasb.edu.ec/index.php/foro/article/view/502, en donde se estudia la evolución de la protección de datos, en el contexto de la Comunidad Andina.

De la revisión de este documento, usted pudo evidenciar que existen notables diferencias entre los países que han recibido reconocimiento internacional, en relación con otros que, aun, 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.

3.2.2. Relación conceptual con el habeas data

Estimado estudiante, 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 habeas data. Así, doctrinariamente, el habeas 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 habeas data, se ejerce mediante la tutela de los denominados “derechos ARCO”, es decir: acceso, rectificación, cancelación u oposición.

> IMPORTANTE: A partir de la garantía del habeas data, el siguiente artículo (http://3.14.189.95/index.php/rnv/article/view/219) estudia la importancia de este mecanismo constitucional, frente a las implicaciones que suponen las tecnologías de la información y comunicación.

Como pudo identificar, el hábeas data no significa, únicamente, una garantía procesal constitucional de acceso a la información de carácter personal sino, 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 habeas 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 el texto básico, por cuanto, en los contenidos pertinentes, se realiza un análisis de varias normas que se relacionan con la protección de datos.

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

Actividades de aprendizaje recomendadas

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.

Luego de este análisis, resuelva las siguientes interrogantes:

1. ¿Qué entiende por Sharenting?

2. La familia, ¿tiene algún deber relacionado con la protección de los datos de los menores?

Lo invito a reforzar sus conocimientos, participando en la siguiente autoevaluación:

Autoevaluación 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:

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

1. Las teorías que conceptualizan los contratos informáticos son:

   a. En relación al objeto y relaciones que emanan del mismo acto.
   b. La firma electrónica y firma digital.
   c. La encriptación y desencriptación.

2. Otra denominación para hacer referencia al contrato electrónico es:

   a. Firma Electrónica.
   b. Firma Digital.
   c. Contratos a distancia.

3. El objeto de los contratos informáticos corresponde a:

   a. Transacciones de bienes y servicios en forma electrónica.
   b. Asignar claves simétricas.
   c. Asignar claves asimétricas.

4. Uno de los problemas de los contratos informáticos es el:

   a. Llamado “web of trust”.
   b. Riesgo de contratar personas ficticias.
   c. Registro de claves públicas.

5. Una de las normas internacionales que regulan los contratos electrónicos es:

   a. El Convenio de Roma.
   b. La Security Data.
   c. El ANF.

6. Una forma de resolver problemas derivados de los contratos informáticos es acudir a:

   a. La Superintendencia de Telecomunicaciones.
   b. La Corte Penal Internacional.
   c. El arbitraje internacional.

7. Un tipo de contrato informático es el:

   a. Contrato telemático.
   b. Contrato de instalación de llave en mano.
   c. Contrato a distancia.

8. Los contratos informáticos complejos abarcan el contrato de:

   a. Servicios auxiliares.
   b. Software.
   c. Joint venture.

9. La protección de datos personales hace referencia a la protección jurídica de la persona frente a:

   a. La automatización de sus datos personales.
   b. La causa licita.
   c. El objeto lícito.

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

Actividades finales del bimestre

Semana 8

Estimado estudiante, dentro de esta semana académica se propone hacer una nueva revisión de los contenidos abordados en esta guía didáctica, de conformidad a la planificación señalado 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: foros, chats, cuestionarios en línea y actividades del componente práctico-experimental, le permitirán vincular los contenidos que se explican en el texto básico.

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

Segundo bimestre

Resultado de aprendizaje 3

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

Contenidos, recursos y actividades de aprendizaje

Estimado estudiante, para comprender la naturaleza de la Informática Forense o de la Técnica Digital 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.

Semana 9

Unidad 4. Técnica digital forense

4.1. Introducción a la Informática Forense

Como punto de partida en este tema, el texto básico "Tercera Parte" realiza una aproximación sobre la conceptualización de la técnica digital o informática forense. Le propongo analizar esta parte. Ahora, preste atención a las siguientes anotaciones.

Sobre la técnica digital forense, Luis Ángel Gómez en Páez (2015) destaca que esta ciencia abarca "la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal".

En consecuencia, la técnica digital forense se considera como "un método científico porque supone la adquisición de nuevos conocimientos, mediante el estudio de la evidencia observable y

medible, aplicando un razonamiento lógico, elaborando modelos e hipótesis y corrigiendo o mejorando estas últimas según se obtenga de la "evidencia" (Páez, 2015, p. 147).

Por tanto, la informática forense constituye un método científico aplicado, a través, de técnicas especializadas, tales como: la identificación, observación y el análisis de las evidencias o vestigios, que se desprenden de una infracción, conducta ilegitima o actividad judicial que requiera la aplicación de técnicas, con intervención de la tecnología.

En este orden de ideas, según el criterio del autor López Rey en Páez (2015), mientras el derecho penal determina lo que se considera delito y la criminología estudia la causación del delito; la criminalística tiene como finalidad el descubrimiento del delito.

Así, en primer término y en relación con el derecho penal, se entiende que la informática forense se desprende de la criminalística, toda vez que se constituye como una ciencia forense destinada a recabar elementos de convicción que presuman la comisión de un delito informático, a fin de constituirlos como prueba, mediante los procedimientos y diligencias que la ley penal señala.

Ahora bien, respecto al origen del término "informática forense" y otras definiciones sobre su naturaleza se sugiere revisar los contenidos previstos en el texto básico. Así, estoy seguro que identificará que la principal característica de este método científico es que "los resultados deben ser objetivos e imparciales, lo que implica un alto grado de profesionalidad y responsabilidad ética en el análisis técnico digital forense" (Páez, 2015, p. 147).

Por otra parte, entre los objetivos de la Informática Forense se destacan:

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

Así también, hay que tomar en consideración que, en el texto básico se hace referencia al uso o aplicaciones relacionados a la informática forense en distintos ámbitos. Preste atención al siguiente recurso:

Usos – aplicaciones de la informática forense

Luego de revisar estas anotaciones, 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.

A continuación, en relación a las reglas de aplicación se sugiere revisar los contenidos previstos en el texto básico. Así como, ampliar la revisión de las disposiciones legales contenidas, tanto en el Código Orgánico Integral Penal como en el Código Orgánico General de Procesos.

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

Actividades de aprendizaje recomendadas

Habiendo destacado el vínculo entre la técnica digital forense con el desarrollo tecnológico, 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

4.2. Modelos y metodologías

Estimado estudiante, la investigación procesal moderna se caracteriza por su amplia esfera de vinculación con el uso de las tecnologías de la información y comunicación. Este avance, sin duda, ha contribuido al mejoramiento de los procesos de investigación, mediante la aplicación de diversos métodos.

En este punto, la técnica digital forense se apoya de una serie de modelos o técnicas y, desde luego, en una metodología estándar, con el objeto de estandarizar los procedimientos vinculados a la investigación.

Para profundizar el estudio de este apartado, tome en consideración que, en el texto básico se hace referencia a los principales modelos de técnica digital forense, así como una descripción de algunos de ellos. Por tanto, podrá reconocer que "el aspecto más importante para un análisis digital forense es seguir la metodología estándar de investigación, y definir bien el problema forense al que ha sido sometido" (Páez, 2015, p. 153).

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	Del Departamento de Justicia de los Estados Unidos.
	Forense del Instituto Nacional de Estándares de Tecnología.
	De análisis Forense de la Red Europea de Institutos Forenses.
	De análisis Forense del EC-COUNCIL.

Fuente: Páez, J. (2015).
Elaboración: Ordóñez, L. (2021).

Corresponde agregar que existen 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. Sobre estos modelos de control y seguridad, el texto básico 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.

Le invito a desarrollar lo siguiente:

Actividades de aprendizaje recomendadas

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.

Semana 11

4.3. Actuaciones y técnicas especiales de investigación

Como introducción a este tema, es preciso anotar que en nuestro país con gran decisión se ha impulsado la vinculación de las TICs en los procesos de administración de justicia, tanto en su parte administrativa como en la determinación de los principios jurídicos, que garanticen la legalidad de la prueba, a partir de la aplicación de medios tecnológicos.

Aunque en un inicio estas actuaciones y técnicas especiales de investigación dentro de los procesos judiciales provocan cambios con las formas tradicionales para el aseguramiento de la prueba; resaltamos su importancia, por cuanto, la integridad que sus procedimientos pueden atribuir a la validez de la prueba, es incuantificable.

Con respecto a este tema, el texto básico realiza una descripción de los principios que el Código Orgánico Integral Penal establece para el anuncio y práctica de la prueba. En este orden, se sugiere revisar en qué consiste cada uno de estos principios.

Ahora bien, lo que se busca, a través, de 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. Preste atención al siguiente recurso:

Actuaciones y técnicas especiales de investigación

Luego de este análisis, se concluye que para que un elemento de convicción, vestigio o evidencia, en general, pueda llegar a constituir prueba legal, dentro de un proceso se requiere el cumplimiento de guías, procedimientos y buenas prácticas con la finalidad de dotar a éstos, elementos de suficientes criterios legales que garanticen su pertinencia al momento de valorarse.

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

4.4. Procedimiento de investigación

La obtención de información de un equipo informático se la puede realizar de diferentes maneras en relación con la metodología operativa o procedimiento para la validación de la misma. Sobre este tema, revise las siguientes recomendaciones.

A. Retirar el dispositivo de almacenamiento del dispositivo que está conectado a una máquina y conectarla al dispositivo forense.

B. Capturar la imagen del disco utilizando el equipo que analizó la fuente y guardar el resultado en un medio externo o extraíble en una máquina de análisis forense.

C. Para escribir en un medio externo se tendrá que montar el dispositivo en lectura y escritura con el comando nativo de montaje.

> **IMPORTANTE:** Los principales sistemas operativos que ofrecen soluciones de aplicaciones nativas para la copia forense de los datos son Linux y Windows.

Estos sistemas operativos se encuentran, ampliamente, desarrollados en el texto básico identificándose algunas herramientas o distribuciones para cada uno de estos. En la siguiente tabla, se resume esta parte.

Tabla 6.
Herramientas / Distribuciones del sistema operativo.

HERRAMIENTAS / DISTRIBUCIONES DE SISTEMA OPERATIVOS	
LINUX	**WINDOWS**
Hélice 3 Enterprise	AccessData FTK (Forensic Toolkit) Imager freeware
DEFT (Digital Evidencia y ForensicToolkit) de Linux	DIM-AM (Gerente de Investigación Digital - Módulo de Adquisición)
CAINE (ComputerAided Medio Ambiente de Investigación)	Herramienta Encase
INTELIGENTE Linux	Drive Snapshot
Forlex	SafeBack
Proyecto IRItaly (Proyecto de Respuesta a Incidentes Italia)	Monte Imagen Pro
El Kit de pingüino Sleuth	
Backtrack 4	

Fuente: Páez, J. (2015).
Elaboración: Ordóñez, L. (2021).

Finalmente, se recomienda revisar en el texto básico la naturaleza de cada una de estas herramientas, con el objeto de contextualizar su aplicación en la investigación, a través, de las técnicas digitales forenses.

Lo invito a reforzar sus conocimientos, participando en la actividad que se describe a continuación:

Actividades de aprendizaje recomendadas

Como pudo evidenciar, los sistemas operativos que ofrecen soluciones para la copia forense de los datos son Linux y Windows. Así, con referencia al siguiente estudio: Metodologías para el análisis forense, se sugiere identificar las metodologías de análisis forense que estructuran un proceso general, desde un sistema Linux.

Realice la autoevaluación para comprobar sus conocimientos.

Autoevaluación 4

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, le propongo resolver las siguientes interrogantes:

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

1. La palabra forense viene del latín:

   a. Forensis.
   b. Kriptos.
   c. Graphos.

2. La técnica digital forense se encuentra vinculada científicamente a:

   a. La criminalística.
   b. El derecho Romano.
   c. La historia del Derecho.

3. La criminalística tiene por objeto:

   a. Aplicar los principios penales para la valoración de la prueba.
   b. Desarrollar la cadena de custodia.
   c. El descubrimiento del delito.

4. En la actualidad, la criminalística está relacionada con:

   a. La teoría del caso.
   b. La ciencia forense.
   c. El derecho penal sustantivo.

5. El almacenamiento forense constituye:

   a. El primer paso que un forense digital debe ejecutar.
   b. Encontrar la información vulnerada.
   c. La garantía y el máximo cuidado para preservar la evidencia.

6. El forense digital lleva a cabo el análisis de la evidencia dentro del proceso de:

   a. Almacenamiento.
   b. Protección.
   c. Documentación.

7. La Forensia en redes, se llama también:

   a. Computer forensics.
   b. Network forensics.
   c. Digital forensics.

8. Define a la captura, almacenamiento y análisis de los eventos de una red:

   a. Computación Forense.
   b. Forensia en Redes.
   c. Forensia digital.

9. La evidencia incriminatoria para procesar una variedad de crímenes se ejecuta, a través de:

   a. El mantenimiento de la Ley.
   b. La investigación de seguros.
   c. La prosecución criminal.

10. La recolección de información sobre casos de apropiación de información confidencial se produce en:

   a. Temas Corporativos
   b. Prosecución criminal
   c. Investigación de seguros

Finalmente, una vez que ha decidido resolver los enunciados propuestos, le propongo comparar sus respuestas con el solucionario que se encuentra en la parte final de esta guía didáctica.

¡Revise la última unidad de la asignatura!

Ir al solucionario

Resultado de aprendizaje 4

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

Contenidos, recursos y actividades de aprendizaje

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 y procesal penal. Así, se destacará en el Derecho Penal, 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.

Semana 12

Unidad 5. Delitos informáticos

5.1. Nociones sobre Derecho Penal y Derecho Procesal Penal

Como introducción a este tema, en el texto básico "Cuarta Parte" usted podrá analizar los antecedentes del derecho penal y derecho procesal penal, a través, de un estudio pormenorizado del sistema penal adversarial acusatorio. Desde esta perspectiva, se resaltarán algunas las ideas principales.

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, el cual se orienta a garantizar la existencia de un sistema adversarial que cuente con fiscales que promuevan el ejercicio de la acción penal, dentro de los principios y fundamentos del sistema acusatorio.

> **TOME NOTA:** En el caso de Ecuador el sistema penal es mixto, es decir, adversarial (teórico legal) – acusatorio (oral procesal).

Bajo estas consideraciones, el sistema adversarial trae consigo un lenguaje de protección y derechos humanos; en tanto que el sistema acusatorio busca mayor eficacia, rapidez y garantías procesales a través del debido proceso. Sobre esta parte, es preciso que, de

conformidad a los contenidos del texto básico, amplíe la revisión de las características que se destacan en relación al sistema adversarial y acusatorio.

De esta manera, como una introducción al tema de delitos informáticos, haciendo una breve referencia al modelo del sistema penal en Ecuador, el modelo mixto que se propone busca eficacia, mejores resultados, pero sobre todo garantizar el debido proceso y los derechos fundamentales de los sujetos procesales.

5.2. Conceptualización del delito digital

5.2.1. Antecedentes

En el texto básico se realiza un estudio preliminar sobre el exordio o antecedentes de los delitos informáticos. En esta parte se hace referencia a las principales causas que motivan la comisión de esta clase de delitos. Le sugiero resaltar las ideas más importantes sobre este parte.

Para empezar este tema es necesario señalar que, a medida que se utilizan las tecnologías de la información y comunicación el riesgo de ser víctima de un delito informático se acelera. En este marco, aparecen tipos penales como: el fraude financiero, sabotaje informático, pornografía infantil, entre otros.

¡Interesante, verdad! Ahora preste atención a los siguientes temas.

Según, Páez (2015) la dependencia tecnológica se concentra en el fenómeno de la tecnología informática, es decir la información y la comunicación, lo cual viene acompañado de riesgos en su uso cotidiano. Esta afirmación tiene su razón de ser, ya que en un inicio los ciberdelincuentes infectaban los equipos informáticos de sus víctimas al transportar mano a mano los virus desarrollados; más tarde, utilizaron las redes de datos al aprovechar el acceso a internet.

Precisamente, recordemos que un antecedente sobre el origen de los delitos informáticos se desarrolla en un estudio documentado por ARPANET en 1980. Al respecto, le sugiero revisar este análisis en los contenidos que se desarrollan en el texto básico.

Ahora bien, a partir del uso de las tecnologías de la información y comunicación se desprenden acciones que, necesariamente, deben ser reguladas y judicializadas por los Estados que, en principio, requieren reformar y modernizar los procesos judiciales, en virtud de regular el escenario informático.

Por otra parte, sobre los factores del origen y causas informáticas que motivaron el surgimiento de los delitos informáticos en Latinoamérica, es importante que usted se refiera al texto básico con el objeto de examinar esta parte, a partir de un estudio realizado por CISCO.

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

Continuemos con el siguiente tema.

5.2.2. Definiciones

Para concretar una definición preliminar sobre el delito informático, es necesario que realice una revisión de los contenidos que se señalan en el texto básico. 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. Este cuerpo normativo 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.

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

Así también, resaltamos que, por ejemplo, el orden jurídico de España realiza una definición de delito informático, desde el ámbito constitucional, considerándolo como una acción que delimita el concepto de delito y que se ha ejecutado por medios informáticos o telemáticos contra los derechos y libertades del individuo.

De esta manera, la variedad de definiciones, de algún modo, vienen de la mano de la distinta naturaleza de la que proviene la comisión de los delitos informáticos, dado que se conciben como una infracción que proviene del uso de las distintas TICs que se experimentan en la sociedad de la información.

Lo invito a participar en la siguiente actividad:

Actividades de aprendizaje recomendadas

Complementariamente y de conformidad a los contenidos del texto básico, 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. 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 siguiente texto: Rol del juez y el proceso penal oral, acusatorio y garantista, específicamente

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

A partir de la lectura de los temas recomendados, habrá podido notar los principios del sistema penal ecuatoriano que han caracterizado 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.

Semana 13

5.2.3. Clasificación

Según Oliver Hance en Páez (2015), existen tres categorías de comportamientos que pueden afectar, negativamente, a los usuarios de los delitos informáticos.

Como se había 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 menciona Oliver Hance, desembocan en tres categorías: acceso no autorizado, actos dañinos o circulación del material dañino e interceptación no autorizada.

Por otra parte, otros autores abordan la clasificación de los delitos informáticos sobre la base de dos criterios: como instrumento o medio y como fin u objetivo.

En lo relativo a la clasificación de los delitos informáticos, desde la perspectiva de instrumento y fin, se encuentra debidamente ampliada en el texto básico. Le sugiero estudiar estos contenidos con el objeto de determinar su naturaleza.

Ampliando este segundo escenario, se advierte una tercera clasificación que a diferencia de la anterior concibe al delito informático, desde una tercera categoría; a saber: los que utilizan la tecnología electrónica como método.

> **IMPORTANTE:** Los que utilizan la tecnología electrónica como método refieren a conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

De este estudio se desprende que un factor importante dentro del fenómeno informático es la identificación de conductas que se utilizan y conductas que atacan. Por tanto, es necesario realizar su estudio, a partir de la siguiente temática.

5.2.4. Sujetos del delito

Además de la doctrina, la jurisprudencia ecuatoriana identifica que para la configuración del delito en general se debe cumplir con varios elementos entre ellos: sujeto activo y sujeto pasivo.

Con esta precisión que, no solamente, se encuentra matizada por la jurisprudencia sino, también, en la ley penal; 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.

Ahora bien, de conformidad a los contenidos del texto básico, se resalta que el sujeto activo se caracteriza por tener habilidades en el manejo de sistemas informáticos. Por esta razón, se los conoce como delitos de “cuello blanco”; en tanto que, el sujeto pasivo puede llegar a constituirse una persona natural o jurídica.

Con el objeto de vincular este tema con las referencias que la doctrina apunta, se sugiere revisar los contenidos determinados en el texto básico en relación al sujeto activo y pasivo de la infracción. De este análisis, se infiere que el sujeto activo se vincula a la “delincuencia informática”; mientras que, el sujeto pasivo se vincula a la “protección penal”, a través de las distintas disposiciones legales que se señalan para el efecto.

Lo invito a participar en la siguiente actividad:

Actividades de aprendizaje recomendadas

A partir del siguiente estudio que se sugiere: Delitos Informáticos: Generalidades, se presenta un análisis de los principales temas relacionados con los delitos informáticos. Desde el derecho comparado, y estableciendo una perspectiva desde nuestro país, se identifican elementos relacionados con el fenómeno de la delincuencia informática

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

Semana 14

5.3. 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.

> **RECUERDE:** En materia penal o sustantiva (teórica del delito) se aplican todos los principios que emanan de la Constitución de la República, de los instrumentos internacionales de derechos humanos y los desarrollados en el Código Orgánico Integral Penal.

Bajo estas consideraciones, en el texto básico, 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 7.
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.

Fuente: Páez, J. (2015).
Elaboración: 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 respondían 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.

En este marco, son ejemplos de delitos informáticos en la actual legislación penal: 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); y, la suplantación a la identidad (art. 212).

¡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.

5.4. Orden jurídico internacional

Uno de los objetivos del derecho internacional es combatir el cibercrimen originado, debido al impacto del uso de las nuevas tecnologías de la información y comunicación, por cuanto, éstas trascienden fronteras geográficas en la sociedad de la información. Este antecedente ha desencadenado en la creación de agencias de cooperación internacional con la finalidad de establecer un marco legal común y mecanismos jurídicos de reciprocidad para la sanción de la criminalidad informática.

Para comprender mejor este tema, en los contenidos del texto básico 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.

> **TOME NOTA:** El Convenio sobre Cibercriminalidad de Budapest es el único que se encarga de la seguridad de la información y trata los delitos contra la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos. (Páez, 2015, p. 290).

Considere ahora la clasificación sobre delitos informáticos que en el contexto internacional realiza las Naciones Unidas. Sobre esta categorización, se definen una serie de tipos penales que la mayoría de legislaciones, a nivel internacional, han decidido incorporar en los ordenamientos jurídicos internos.

Respecto a esta clasificación o categorización de los delitos informáticos realizada por las Naciones Unidas, el texto básico realiza una descripción de estos tipos penales. En este aspecto, se sugiere identificar, tanto las denominaciones como los elementos que componen a cada tipo penal. Así, luego del análisis que se puede realizar del tema en referencia, se advierte que, entre los tipos penales descritos por las Naciones Unidas, el sistema penal ecuatoriano recoge el fraude efectuado por manipulación informática, las falsificaciones informáticas, entre otros.

Por otra parte, el Manual de las Naciones Unidas para la prevención y control de los delitos informáticos considera que cuando el problema se eleva a escala internacional se magnifican los problemas por el carácter transnacional del delito y la falta de cooperación internacional. Al caso, se precisa que la ONU refiere algunas causas sobre los problemas que involucran la cooperación internacional en el área de los delitos informáticos. Le sugiero revisar el texto básico a fin de precisar este estudio.

Finalmente retomando el estudio de la normativa ecuatoriana en relación a los criterios doctrinarios, otro elemento para la configuración del delito, que se identifica desde la jurisprudencia es el elemento material que configura a largo plazo el carácter probatorio dentro de los procesos penales.

Lo invito a desarrollar la actividad que se describe a continuación:

Actividades de aprendizaje recomendadas

Preste atención a la siguiente actividad que sugiere el estudio de nuevas tipologías penales relacionadas con los delitos informáticos. Se trata especialmente de abordar los casos de ciberacoso y abuso

sexual que pueden perpetrarse como resultado del uso ilícito de las TICs. Así, mediante la siguiente actividad que se propone, identificaremos el programa “En tic confío”, el cual forma parte de los mecanismos de prevención de delitos informáticos en Colombia. Para este fin, ingrese al siguiente enlace: http://www.enticconfio.gov.co/

¡Continúe con este estudio!

Semana 15

5.5. Medios de prueba penal digital

Hablar de medios probatorios, que se posibilitan mediante recursos informáticos o tecnológicos, se hace referencia a los presupuestos por los cuales se configura el delito informático. Naturalmente, dichos medios nacen, en virtud del proceso de investigación de las conductas punibles que se asocian con estos delitos.

A priori, es necesario realizar una evaluación respecto de cómo la sociedad de la información influye en la presentación y sustentación de las TICs como prueba en el proceso penal, y en qué medida el sistema penal ecuatoriano provee a los operadores de justicia elementos tecnológicos, como medios de prueba penal digital.

Para comprender mejor este tema, el texto básico 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 prueba en materia penal es de especial importancia, en virtud de configurar la teoría del caso o hipótesis que afirma la vinculación del nexo causal entre la materialidad de la infracción con la responsabilidad de una persona.

Por tanto, el proceso de identificación, recolección, protección y legalización de la prueba conlleva una serie de procedimientos, como la cadena de custodia, los cuales tienen por objeto el aseguramiento de la prueba, para que ésta pueda sostener un valor legal, frente a la valoración y motivación que realice el juez al momento de resolver. En este marco, es preciso mencionar que el texto básico identifica algunas disposiciones que, según la Constitución de la República del Ecuador, se orientan a garantizar los medios de prueba. Al efecto, se sugiere examinar estos principios.

Por otro lado, en el proceso de investigación para la determinación de la materialidad y responsabilidad de los delitos, la obtención de indicios o elementos de convicción, los cuales, en suma, se constituirán como elementos probatorios, debe seguir las normas legales y técnicas que garanticen su presentación, en virtud de no ser objeto de impugnación o penalización.

> **IMPORTANTE:** El texto básico señala tres casos por los que los medios de prueba se pueden penalizar. Le sugiero estudiarlos y relacionarlos con el contexto de los delitos informáticos.

Ahora bien, con relación a las actuaciones técnicas y especiales de investigación vinculadas con los delitos informáticos, se puede señalar que – a partir de las reglas del consentimiento, diligencias y registros- estas diligencias están encaminadas a establecer el procedimiento técnico, especial y legal adecuado para el aseguramiento de la prueba en los delitos informáticos.

De este escenario, en referencia a los medios de prueba penal digital, se desprenden las siguientes actuaciones en los delitos informáticos:

- Actuaciones técnicas: Reconocimiento de objetos, reconstrucción del hecho, comunicaciones personales, registros relacionados a un hecho constitutivo de infracción, entre otras.
- Actuaciones especiales: Retención de correspondencia, interceptación de comunicaciones y reconocimiento de grabaciones.

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.

> I**MPORTANTE:** En el texto básico se realiza un amplio análisis de esta clasificación. 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 del texto básico. 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 según las disposiciones del Código Orgánico Integral Penal.

5.6. Procedimiento penal

Con la implementación del Código Orgánico Integral Penal se desprenden nuevos procedimientos, los cuales tienen la finalidad de agilitar el servicio de administración de justicia, de conformidad a los principios del debido proceso y tutela judicial efectiva.

En primer término, se señala que el ejercicio de la acción penal puede ser pública y privada.

> **TOME NOTA:** 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.

Este 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.

> **IMPORTANTE:** Adicionalmente, se señalan algunos procedimientos especiales que se derivan del ejercicio de esta acción. Al respecto, 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.

> **TOME NOTA:** 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".

> **IMPORTANTE:** 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?

Lo invito a participar desarrollando la siguiente actividad:

Actividades de aprendizaje recomendadas

Mediante la siguiente publicación que se sugiere, y con el objeto de fundamentar el análisis de los casos propuestos en esta última parte, la Corte Nacional de Justicia analiza, integralmente, el tema de “Delitos Informáticos en el COIP”. Para este fin, debe consultar el siguiente enlace: https://tinyurl.com/y3fpzwc9, específicamente, la primera y segunda parte relativo a los delitos informáticos y los principios de la etapa de juicio y la finalidad de la prueba, en el ordenamiento jurídico-penal ecuatoriano.

Realice la autoevaluación para comprobar sus conocimientos.

Autoevaluación 5

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.

Finalmente, le sugiero realizar la siguiente actividad, con el objeto de medir su nivel de conocimiento. A continuación, le propongo resolver las siguientes interrogantes:

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

1. El sistema penal en Ecuador, se caracteriza por ser:

    a. Inquisitivo.
    b. Adversarial – acusatorio.
    c. Garantista.

2. En el proceso penal, se reconoce la aplicación de los tratados internacionales en:

    a. Derechos humanos.
    b. Delitos informáticos.
    c. Criminalidad informática.

3. El derecho de la persona a no declarar contra sí misma, se relaciona con el principio de:

    a. Intimidad.
    b. Igualdad.
    c. Autoincriminación.

4. El modelo adversarial fue extraído del procedimiento penal:

   a. Anglosajón.
   b. Mexicano.
   c. Chileno.

5. En el sistema adversarial, como sujeto procesal, está separado de las partes:

   a. El juez.
   b. El fiscal.
   c. El Jurado.

6. El sistema acusatorio funciona haciendo una separación entre las funciones de:

   a. Inmediación, contradicción y objetividad.
   b. Investigación, acusación y sentencia.
   c. Publicidad, concentración e intimidad.

7. El sistema acusatorio se rige por los principios que busca garantizar:

   a. La seguridad y los derechos del imputado y ciudadanía en general.
   b. La imparcialidad.
   c. El impulso procesal.

8. El sistema adversarial trajo consigo un lenguaje:

   a. Oral.
   b. De derechos humanos y de protección.
   c. Inquisitivo.

9. La metodología que emplea el sistema adversarial es:

   a. Inquisitivo.
   b. Empírico.
   c. Inductivo.

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

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

Finalmente, una vez que ha decidido resolver los enunciados propuestos, le propongo comparar sus respuestas con el solucionario que se encuentra en la parte final de esta guía didáctica.

Ir al solucionario

Resultado 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

Semana 16

Estimado estudiante, dentro de esta semana académica se propone hacer una nueva revisión de los contenidos abordados en esta guía didáctica, de conformidad a la planificación señalado 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: foros, chats, cuestionarios en línea y actividades del componente práctico-experimental, le permitirán vincular los contenidos que se explican en el texto básico.

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

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. Solucionario

Autoevaluación 1		
Pregunta	**Respuesta**	**Retroalimentación**
1	b	Confróntese página 1 del texto básico. La Informática Jurídica no es otra cosa que el procesamiento de información jurídica, por medios electrónicos, no sólo en lo informático, sino en las telecomunicaciones.
2	a	Confróntese página 1 del texto básico. Nos referimos a la Informática Jurídica cuando el Jurista utiliza las nuevas tecnologías como herramienta para procesar, automatizar, organizar, y, sistematizar información de contenido jurídico.
3	a	Confróntese página 15 de la guía didáctica. 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 página 3 del texto básico. 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.

Autoevaluación 1		
Pregunta	**Respuesta**	**Retroalimentación**
5	a	Confróntese página 2 del texto básico. La Informática Jurídica Decisional es aquella que con la aplicación de sistemas lógicos o programas utiliza inteligencia artificial.
6	a	Confróntese página 15 de la guía didáctica. 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 página 5 del texto básico. La Informática Jurídica, es un campo de aplicación que surge de una gran variedad de disciplinas: La Computación, la Informática, la Lingüística, la Lógica, el Derecho, la Programación y, el Cálculo y otras que han superado el nivel de la experimentación.
8	b	Confróntese página 1 del texto básico. La Informática Jurídica Documental se ha convertido en una herramienta imprescindible del Jurista, pero enfrenta un principal problema que es el de la representación y el procesamiento de los significados presentes en los textos, por eso se da a la SEMÁNTICA y a la SINTAXIS del Lenguaje Jurídico, independiente de la dificultad que plantea la sistematización de los procesos jurídicos.
9	c	Confróntese página 17 del texto básico. La propiedad intelectual está relacionada con la informática jurídica por el régimen de protección, que puede ser en el de derechos de autor cuando implica regulación de bases de datos y software; y en el campo del régimen de propiedad industrial cuando los componentes y partes de las nuevas tecnologías de la información y comunicación están reguladas, como el caso de marcas, signos distintivos, patente, etc.

Autoevaluación 1		
Pregunta	**Respuesta**	**Retroalimentación**
10	b	Confróntese página 21 del texto básico. Los SISTEMAS EXPERTOS están dirigidos o diseñados para resolver casos jurídicos complicados, como por ejemplo en el Sistema Tributario, el determinar liquidaciones por impuestos.

Ir a la autoevaluación

Autoevaluación 2		
Pregunta	**Respuesta**	**Retroalimentación**
1	a	Confróntese página 41 del texto básico. Los aspectos jurídicos del comercio electrónico son importantísimos, algunos países han seguido muy de cerca la Ley modelo de Comercio Electrónico elaborada por la UNCITRAL, que nació vinculada al entorno tecnológico del EDI (Electronic Data Interchange).
2	b	Confróntese página 41 del texto básico. A diferencia del modelo de la UNCITRAL, la Unión Europea tiende a legislar en forma individualizada cada tema, como por ejemplo: firma electrónica, o la protección de datos, a través, de Directivas.
3	a	Confróntese página 42 del texto básico. El Comercio electrónico abarca como estudio las siguientes temáticas: mensajes de datos, documentos electrónicos, contratación electrónica, firma electrónica, gobierno electrónico, protección de datos, etc.
4	c	Confróntese página 43 del texto básico. En el caso del Ecuador por iniciativa privada, se impulsó la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, aprobada en el año 2002, que es la que regula los aspectos relacionados con el comercio electrónico.
5	b	Confróntese página 43 del texto básico. La primera ley que ha regulado los aspectos jurídicos de la firma digital como documento electrónico e instrumento probatorio, fue en los Estados Unidos. Se aprobó en 1997 en Utah.
6	a	Confróntese página 44 del texto básico. Siendo el documento electrónico toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material; nos referimos a todos los documentos que son emitidos por medios electrónicos, magnéticos, digitales o informáticos.

Autoevaluación 2		
Pregunta	**Respuesta**	**Retroalimentación**
7	c	Confróntese página 44 del texto básico. Por exclusión, entendemos que constituye un documento no electrónico aquel que es elaborado por las formas tradicionales, sean éstas manuales, mecanográficas, micrograbadas, microcopiadas o fotográficas.
8	b	Confróntese página 48 del texto básico. La firma digital, es el reemplazo de la firma ológrafa utilizada en medio papel, que manifiesta la misma intención y expresión de voluntad para el medio electrónico.
9	c	Confróntese página 54 del texto básico. Las firmas digitales se basan en matemáticas aplicadas y utilizan algoritmos de criptografía, que son procesos por los cuales se oculta la información a enviar de un emisor a un receptor, evitando de ésta manera la visualización, manipulación o modificación de la misma en el caso de una interceptación.
10	b	Confróntese página 33 de la guía didáctica. Podemos hablar que el universo de firmas a través de métodos de 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.

Ir a la autoevaluación

Autoevaluación 3		
Pregunta	**Respuesta**	**Retroalimentación**
1	a	Confróntese página 107 del texto básico. En la doctrina, existen teorías que conceptualizan a los contratos informáticos de diferente manera. Una de ellas, considera como elemento determinante para su conceptualización el objeto al cual están referidos dichas contrataciones; y, otra toma como elemento caracterizador las diversas relaciones jurídicas que emanan del mismo acto. Estas dos teorías coinciden en establecer que los contratos informáticos son contratos particulares (e individuales) y difieren del resto de los contratos.
2	c	Confróntese página 108 del texto básico. Al Contrato Electrónico también se le conoce como: "Contratos a Distancia", "Contratos Telemáticos", "Contratos por medio de las nuevas tecnologías", etc.
3	a	Confróntese página 110 del texto básico. Considerando que los contratos informáticos constituyen una nueva forma de contratación, su objeto se constituye en las transacciones de bienes y servicios en forma electrónica, o por cualquier medio magnético.
4	b	Confróntese página 110 del texto básico. Uno de los problemas de la contratación informática es el riesgo de contratar con personas ficticias o empresas virtuales.
5	a	Confróntese página 111 del texto básico. Este es el caso del Convenio de Roma de 19 de junio de 1980, aplicable a las obligaciones contractuales en el marco de la Unión Europea: "Los contratos se regirán por la ley elegida por las partes" –art. 3–.
6	c	Confróntese página 112 del texto básico. Una forma de solución de controversias es el Arbitraje Internacional, la cual se considera como una solución adecuada.

Autoevaluación 3		
Pregunta	**Respuesta**	**Retroalimentación**
7	b	Confróntese página 113 del texto básico. El Profesor español Davara Rodríguez, los divide en cuatro clases de contratos informáticos: a) Contrato de Hardware; b) Contratos de Software; c) Contratos de instalación llave en mano; y d) Contratos de servicios auxiliares.
8	c	Confróntese página 113 del texto básico. Otros autores clasifican los contratos informáticos en: a) Por su objeto: Abarcan los de software, hardware, llave en mano, etc; b) Por el negocio jurídico: Abarcan compra venta, arrendamiento, etc., y, c) Complejos: Abarcan tales como Out sourcing, Joint venture, etc.
9	a	Confróntese página 125 del texto básico. La doctrina utiliza la expresión “protección de datos” en lo referente a la protección jurídica de la persona, frente a la tecnología que automatiza sus datos.
10	b	Confróntese página 126 del texto básico. Este derecho fundamental se encuentra reconocido en el Capítulo sexto: Derechos de libertad –art. 66.19–.

Ir a la autoevaluación

Autoevaluación 4		
Pregunta	**Respuesta**	**Retroalimentación**
1	a	Confróntese página 145 del texto básico. La palabra forense viene del latín “forensis”, que significa, “perteneciente o relativo al foro”. “de o ante el foro”.
2	a	Confróntese página 146 del texto básico. La técnica digital forense se denomina también: Informática Forense, la cual es interdisciplinar y está vinculada, científicamente, a la criminalística y a la ciencia forense.
3	c	Confróntese página 146 del texto básico. Mientras el derecho penal determina lo que se considera delito y la criminología se ocupa de estudiar la causación del delito, la criminalística tiene como finalidad el descubrimiento del delito.
4	b	Confróntese página 145 del texto básico. En la actualidad la criminalística está relacionada a la ciencia forense por lo que su denominación es correcta, y el término “forense” es sinónimo de “legal” y referente a “prueba” en los tribunales de justicia.
5	c	Confróntese página 148 del texto básico. En el almacenamiento, el forense digital debe garantizar el máximo cuidado para preservar la integridad del equipo de prueba.
6	a	Confróntese página 148 del texto básico. En este proceso el forense digital lleva a cabo el análisis. Después de hacer una copia de lo que necesita para verificar la coherencia con respecto a los datos originales, por lo que los datos se firman digitalmente tanto el original y la copia, los cuales deben coincidir.
7	b	Confróntese página 150 del texto básico. Forensia en redes también denominada network forensics.

Autoevaluación 4		
Pregunta	**Respuesta**	**Retroalimentación**
8	b	Confróntese página 150 del texto básico. La forensia en redes es la captura, almacenamiento y análisis de los eventos de una red, para descubrir el origen de un ataque o un posible incidente.
9	c	Confróntese página 151 del texto básico. Dentro de los usos de la técnica digital forense, la evidencia incriminatoria puede ser aplicada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
10	a	Confróntese página 152 del texto básico. En lo que respecta a los temas corporativos, la técnica digital forense puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.

Ir a la autoevaluación

Autoevaluación 5		
Pregunta	**Respuesta**	**Retroalimentación**
1	b	Confróntese página 233 del texto básico. En el caso del Ecuador, el sistema es ADVERSARIAL – ACUSATORIO. Se puede resumir que en la parte sustantiva del concepto (Teoría Del Delito) es adversarial, y en la parte adjetiva (proceso penal), es acusatorio, es decir dos sistemas en uno.
2	a	Confróntese página 233 del texto básico. El art. 2 del COIP expone los principios generales del sistema adversarial: "En materia penal se aplican todos los principios que emanan de la Constitución de la República, de los instrumentos internacionales de derechos humanos y los desarrollados en este Código".
3	c	Confróntese página 235 del texto básico. El principio de prohibición de autoincriminación refiere que ninguna persona podrá ser obligada a declarar contra sí misma en asuntos que puedan ocasionar su responsabilidad penal.
4	a	Confróntese página 237 del texto básico. El modelo adversarial fue extraído del procedimiento penal anglosajón. Es un procedimiento de partes (adversary system).
5	a	Confróntese página 237 del texto básico. En este sistema procesal, el juez, como sujeto procesal, está completamente separado de las partes, el proceso penal es una contienda entre iguales que inicia con la acusación, a quien compete la carga de la prueba, y confronta a la defensa, en un proceso o juicio contradictorio, oral y público, y el juez resuelve según su libre convicción.

Autoevaluación 5		
Pregunta	**Respuesta**	**Retroalimentación**
6	b	Confróntese página 238 del texto básico. El sistema acusatorio funciona haciendo una separación entre las funciones de investigación, acusación y sentencia, en este orden, quien investiga es la policía, quien acusa es el fiscal, y quien sentencia es el juez tomando en cuenta la deliberación de un jurado especializado.
7	a	Confróntese página 238 del texto básico. Dentro del sistema acusatorio se rige por distintos principios que buscan garantizar la seguridad y los derechos del individuo imputado y de los ciudadanos en general.
8	b	Confróntese página 240 del texto básico. Encontramos varias características en la adversarialidad, así tenemos que este sistema trajo consigo, por primera vez en la historia de la humanidad, un lenguaje de derechos humanos y de protección.
9	b	Confróntese página 240 del texto básico. Encontramos varias características en la adversarialidad, así tenemos que, en este sistema la metodología que se emplea es el empírico tanto a nivel del derecho como de la ideología.
10	b	Confróntese página 80 de la guía didáctica. 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

Código Orgánico Integral Penal. Recuperado de: lexis.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. Recuperado de lexis.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. (2019). El hábeas data como garantía procesal frente a las tecnologías de la información y comunicación: situación en el contexto ecuatoriano. Revista RES NON VERBA. Nro. 2. Samborondón: Universidad ECOTEC.

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.

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

Pérez, A. (1996). *Manual de Informática y Derecho*. Madrid: Editorial Ariel S.A.

Pérez, A. (2007). *Trayectorias contemporáneas de la Filosofía y la Teorías del Derecho.* Madrid: Editorial Tebar.

Téllez, J. (2004). *Derecho Informático, Instituto de Investigaciones Jurídicas de la UNAM*. México: Ed. Mc Graw Hill.