UNIVERSIDAD CONTINENTAL | MODALIDAD VIRTUAL

UNIVERSIDAD CONTINENTAL VIRTUAL

MANUAL AUTOFORMATIVO

ASIGNATURA
DERECHO INFORMATICO

Autor

ING. JOSÉ HECTOR ACOSTA VELARDE

ÍNDICE

INTRODUCCIÓN

El derecho informático, es una asignatura que corresponde al área de estudios de especialidad, es de naturaleza teórica-práctica. Tiene como propósito desarrollar en el estudiante la capacidad de interpretar las diversas normas nacionales e internacionales que regulan el buen uso de la Tecnología de la Información y Comunicación.

La asignatura contiene: Introducción al derecho informático. La protección de datos. Ley orgánica de protección de datos de carácter personal. Protección jurídica del software. Protección jurídica de las bases de datos. El delito informático. La Ley de servicios de la sociedad de la información y comercio electrónico.

Es recomendable que desarrolle una permanente lectura de estudio, de los contenidos desarrollados y de los textos seleccionados que amplían o profundizan el tratamiento de la información…junto a la elaboración de resúmenes y una minuciosa investigación vía Internet, … El desarrollo del manual se complementa con autoevaluaciones, que son una preparación para la prueba final de la asignatura…

Organiza tu tiempo para que obtengas buenos resultados, la clave está en encontrar el equilibrio entre tus actividades personales y las actividades que asumes como estudiante. El estudio a distancia requiere constancia, por ello es necesario encontrar la motivación que te impulse a hacer mejor cada día…

El autor

ORGANIZACIÓN DE LA ASIGNATURA

RESULTADO DE APRENDIZAJE DE LA ASIGNATURA

Al término de la asignatura el estudiante será capaz de analizar e interpretar la normatividad vigente sobre el uso de las Tecnologías de la Información y la Comunicación; para el desarrollo ético de sus actividades profesionales.

UNIDADES DIDÁCTICAS

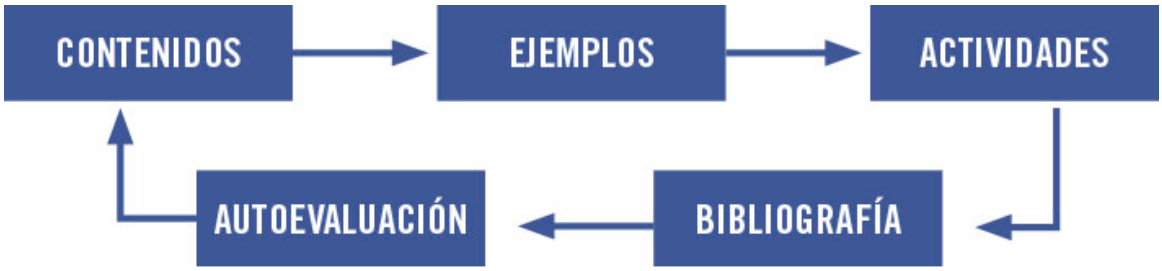
UNIDAD I	**UNIDAD II**	**UNIDAD III**	**UNIDAD IV**
La sociedad de la información y la legislación informática	El gobierno electrónico y la regulación jurídica de la información	Los contratos informáticos y riesgos informáticos	Riesgos del spam y aspectos laborales de la informática
Resultado de aprendizaje Al finalizar la unidad, el estudiante será capaz de exponer e interpretar la estructura de las normas peruanas donde se evidencia las fuentes del derecho, la informática jurídica que serán aplicadas dentro del derecho informático, demostrando dominio del tema, claridad y fluidez.	**Resultado de aprendizaje** Al finalizar la unidad, el estudiante será capaz de analizar y describir la implementación del Gobierno electrónico a través del ONGEI, la Ley de protección de datos personales, demostrando dominio teórico adecuado.	**Resultado de aprendizaje** Al finalizar la unidad, el estudiante será capaz de describir y discutir temas relacionados a los contratos informáticos, considerando los riesgos, delitos informáticos y la regulación del uso del comercio electrónico.	**Resultado de aprendizaje** Al finalizar la unidad, el estudiante será capaz implementar tecnologías considerando las normas del SPAM, firmas y documentos electrónicos otros para el uso adecuado de la informática en la práctica de su profesión.

TIEMPO MÍNIMO DE ESTUDIO

UNIDAD I:	UNIDAD II:	UNIDAD III:	UNIDAD IV:
Semana 1 y 2	Semana 3 y 4	Semana 5 y 6	Semana 7 y 8
16 horas	16 horas	16 horas	16 horas

UNIDAD I: La sociedad de la información y la legislación informática

DIAGRAMA DE ORGANIZACIÓN DE LA UNIDAD I



ORGANIZACIÓN DE LOS APRENDIZAJES

Resultado de aprendizaje de la Unidad I:

Expondrá e interpretará la estructura de las normas peruanas demostrando dominio del tema.

CONOCIMIENTOS	HABILIDADES	ACTITUDES
Tema N° 1: Conceptos Generales sobre la sociedad, tecnología y derecho 1. Sociedad de la Información 2. Tecnología y derecho **Tema N° 2:** Fuentes del Derecho. La legislación peruana 1. Fuentes del Derecho 2. La legislación Peruana **Lectura seleccionada 1:** Alcances de la sociedad de la información y la sociedad del conocimiento Jhon Jairo Herrera Sánchez **Tema N° 3:** El Derecho Informático. La Informática Jurídica 1. Derecho Informático 2. Informática Jurídica **Tema N° 4:** La libertad informática en la legislación peruana. 1. Libertad Informática 2. Legislación Peruana. **Autoevaluación de la Unidad I**	1. Interpreta y analiza los resultados de la Cumbre Mundial de la Sociedad de la Información. 2. Examina la estructura de las normas jurídicas peruanas. 3. Compara el Derecho Informático y la Informática Jurídica 4. Analiza las normas jurídicas del Perú sobre la libertad informática **Actividad N°1** Los estudiantes Participan en el Foro de discusión sobre la Sociedad de la Información Compara el Derecho Informático y la Informática Jurídica **Control de lectura N° 1** Evaluación del tema N° 1 y 3 más los contenidos de la lectura 1	1. Asume una actitud reflexiva sobre la importancia de la normatividad en el desarrollo de las Tecnologías de la Información

TEMA N° 1: Sociedad, Tecnología y Derecho

La sociedad de la información es un tema vital en el desarrollo y evolución del uso de las Tecnologías de la información y las telecomunicaciones (TIC) debido al comienzo de la sociedad de la información y por ende los grandes cambios que han surgido en los últimos años en relación a las telecomunicaciones y al intercambio de información a nivel global. Desde la perspectiva del derecho, esto abre una nueva visión de lo que representa la información su acceso y su uso, así como su regulación a nivel mundial y en cada país. Por este motivo, el conocimiento de la sociedad de la información y su vinculación con el derecho es vital para un desenvolvimiento profesional competente.

1. **Sociedad de la Información:**
   Se caracteriza principalmente por la capacidad de ciudadanos, instituciones privadas e instituciones públicas, estas obtienen y comparten toda información de forma instantánea desde cualquier lugar.

   Este nuevo modelo de sociedad trata de crear, modificar y distribuir la información, siendo parte en la actividad de económica y social de un país, esta soportada en el buen uso de las Tecnologías de la Información (TICs) que son aplicadas para el desarrollo de una nación.

   Según lo estipulado en la resolución 56/183 de la Asamblea General de la ONU, la Cumbre Mundial en relación a la Sociedad de la Información (CMSI) tuvo 2 etapas.

   - Ginebra, del 10-12 de diciembre del 2003.
   - Túnez, del 16-18 de noviembre del 2005.

   La Cumbre Mundial de Sociedad de Información CMSI fue un foro organizaciones internacionales, gobiernos; el sector privado y la sociedad civil analizaron el nuevo ambiente de información y comunicación; así mismo como afrontar retos de la desigualad en el acceso a la información y la comunicación conocida como “brecha digital”.

   En la CMSI se han desarrollado varios documentos finales, de igual forma se ha creado el Foro de la Gobernanza de Internet (Internet Governance Forum, 2013).

   1.1. **Primera fase Cumbre de Ginebra**
   Fue desarrollado en el año 2003, dentro de Declaración de Principios, los representantes del mundo declararon “…Nosotros, los representantes de los pueblos del mundo, reunidos en Ginebra del 10 al 12 de diciembre de 2003 con motivo de la primera fase de la Cumbre Mundial sobre la Sociedad de la Información, declaramos nuestro deseo y compromiso comunes de construir una Sociedad de la Información centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respe-

tando plenamente y defendiendo la Declaración Universal de Derechos Humanos..." (WSIS-03, 2004, p. 23).

1.2. Segunda fase Cumbre de Túnez

Del 16-18 de noviembre del 2005, construir una Sociedad de la Información centrada en la persona, abierta a todos y orientada al desarrollo. Se reiteró el apoyo a la Declaración de Principios de Ginebra. También sirvió para crear una oportunidad sin precedentes de mayo conciencia con respecto de las visibles ventajas de las TIC (Tecnologías de la Información y la Comunicación), esforzándose en el promover el acceso universal a estas, garantizando a todos los países del mundo el acceso equitativo y asequible. (WSIS-05, 2006).

Según William J. Martin y Frank Webster, se puede distinguir cinco elementos que nos ayudarán a comprender mejor que es la sociedad de la información.

1.2.1. Elemento tecnológico:

En la actualidad el costo de un ordenador es accesible, este facilita el manejo de la información dentro de las organizaciones y en las sociedades potenciando el desarrollo en ellas.

Como resultado tenemos que la información se ha vuelto mucho más barata de almacenar, procesar y transmitir, John Naisbitt argumenta que "La tecnología informática es a la era de la información lo que la mecanización fue a la revolución industrial". (Naisbitt, 1982, p. 72)

Las redes se han convertido en una supercarretera siendo indispensables para la interconexión de los ordenadores; así mismo se debe de contar con una capacidad de almacenamiento óptima "la conexión de terminales desde y entre oficinas, bancos, hogares, tiendas, fábricas, escuelas y todo el globo en sí" (Webster, 1994, p. 67).

Existiendo una comparación entre la red eléctrica o el ferrocarril y la red de información actual, donde el elemento principal es el Internet.

Alvin Toffler y Willam J. Martin "sostienen que la tecnología de la información representa el establecimiento de una nueva forma de vida que viene a modificar las actividades de la estructura social" (Toffler, 1980, p. 108)

El uso de la tecnología ha posibilitado el procesamiento, almacenamiento, recuperación y la transmisión de información en toda la sociedad, considerando el uso de los ordenadores como parte principal en el desarrollo de las TICs.

Hoy en día el uso de las tecnologías de la información y las comunicaciones, considerando el ámbito social y el económico, son las principales características de la Sociedad de la Información.

Por otro lado, existen autores quienes enfatizan que el uso de las tecnologías de información y comunicaciones, en sí mismas,

"no son capaces de dar una respuesta real, medible o probable; es por eso que el empleo de este argumento es impreciso para definir cuándo una sociedad se ha convertido en una sociedad de la información" (Castells, 1995, p. 412).

Martin, añade que existen "dos problemas importantes que deben considerarse al hablar sobre una sociedad de información: - Cómo se mide la tasa de innovación tecnológica, y Cuándo cesa una sociedad en su carácter de industrial y se transforma en una sociedad de información" (Castells, 1995, p. 412).

Según Webster F. entendemos que en "una era dada, las tecnologías se inventan y luego impactan sobre la sociedad; así pues, la tecnología en estas versiones está privilegiada, sobre todo y sobre todos, y llega a identificar a un mundo, la era del vapor, la era atómica, entre otras" (Webster, 1994, p. 10)

1.2.2. Elemento económico

En el área económica hay una subcategoría en relación a lo económico en el ámbito de la información y su enfoque económico.
Machlup F. invirtió un considerable tiempo de su vida como profesional con el propósito de poder considerar el impacto del tamaño de las industrias de información y su amplitud con respecto a ellas. En su obra, La Producción y Distribución del Conocimiento, se pueden identificar ciertos parámetros para poder medir una sociedad de la información (Machlup, 1958, p. 93).

A continuación se presentan los 5 ámbitos de estadísticos que distinguen a las industrias de la información:

- Educación, escuelas y bibliotecas.
- Medios de comunicación (radio, televisión y publicidad)
- Máquinas de información (equipos de cómputo e instrumentos musicales)
- Servicios de información (leyes, seguros, salud y entretenimiento)
- Otras actividades de información (investigación y desarrollo)
  Cada una tiene un valor económico que contribuye al Producto Interno Bruto (PIB) (Machlup, 1958, p. 93).

Según este estudio, se concluyó que existía un 29% del PBI (Producto Bruto Interno) en los Estados unidos que tenía su origen en industrias de la información a comienzos de los años 70; este fue el comienzo de la economía moderna basada en el conocimiento.

Según Webster, "podríamos tener una sociedad en la cual a través de la medición del Producto Interno Bruto (PIB), la sociedad de la información sea de mayor peso, en relación con los otros sectores de la economía, pero de pocas consecuencias en cuanto a los orígenes y sostenes de la vida política, económica y social; así pues, el tema del valor cualitativo de la información deberá limitarse a la relevancia a ellos" (Webster, 1994, p. 10)

1.2.3. Elemento ocupacional

El elemento ocupacional es visible cuando el existe una predominancia de empleos en el área de la información. Quieres decir que el número de trabajadores de oficina, profesionales, expertos, entre otros, sea mayor a de los trabajadores que no utilizan las tecnologías de la información y esto tenga un efecto económico.

Estudios realizados por Marc Porat mostraron que al menos un 50% de los trabajadores de los Estados Unidos, se encontraba relacionado al área de la información.

Como conclusión de este estudio Porat argumentó que "el trabajo no informacional del informacional, con base en el grado con el que cada individuo se involucra en la generación de información; en otras palabras, en la medida en que los trabajos son informacionales o no, la categorización es asunto de juicio" (Porat, 1980, p. 1062).

1.2.4. Elemento tiempo-espacio

Si bien es cierto la sociedad de la información que tiene como fundamento los pilares económicos y sociales, tiene también un aspecto de tiempo y espacio. Esto se refiere a las redes informáticas que tienen como función la conexión de distintos pueblos, y que tienen efectos temporales y espaciales en las organizaciones.

(Webster, 1994, p. 10) hace una identificación de 4 elementos relacionados con una necesaria transformación hacia una sociedad de la información, cito en extenso:

- La información está ocupando el lugar central como recurso estratégico clave en la economía mundial, de ello se desprende que la organización y recuperación de información es de valor excepcional y atestiguamos que se aplicará en un gran número de actividades.

- Computación y tecnologías de información suministran la infraestructura que permite que la información se procese y distribuya, facilita las operaciones instantáneas de comercio y monitorea los asuntos económicos y sociales a escala global.

- Ha existido un crecimiento excepcionalmente rápido del sector comercial de la información en la economía de servicios como medios de comunicación (satélite, cable, video) y el desarrollo de bases de datos en línea, que suministran información instantánea de precios de bienes, listas, fluctuaciones de monedas, así como resúmenes de revistas técnicas y científicas, entre otras.

- La creciente informatización de la economía facilita la integración de las economías nacionales y regionales, efecto inmediato y efectivo del proceso e intercambio de la información; la economía se ha convertido en algo verdadera-

mente global, sin restricciones de espacio, los límites rigidos por la ubicación geográfica se han derribado.

1.2.5. Elemento cultural

Existe también un enfoque de tipo cultural en toda sociedad de la información, pero es el más difícil de identificar. Cada uno de nosotros podemos ver un aumento considerable en la información que manejamos. Por ejemplo, la televisión ha pasado de 1 canal con un servicio temporal a tener cientos de canales de forma permanente; por supuesto, esto también involucra un aumento de tecnologías relacionadas como satélites, servicios web, cable, antenas parabólicas, etc. Además, podemos ver la incontable información que nos provee el internet con respecto al intercambio de información. Esto demuestra que vivimos en una sociedad que cada día más está sumergida en información de todo tipo y calidad.

El tipo de cultura presente en la actualidad tiene características informativas muy tangibles en comparación a quienes las precedieron. Es decir, se puede observar claramente que los símbolos que representan la información están presentes en muchas de nuestras transacciones. “Esta explosión de datos y símbolos significa lo que muchos escritores conciben como la sociedad de la información; paradójicamente esta gran explosión de información guía a algunos autores a anunciar que con la muerte del siglo, hay más información y menos significado” (Webster, 1994, p. 16).

TEMA N° 2: Fuentes del derecho

El derecho es tan antiguo como el hombre y las fuentes del derecho varían entre los diversos países; sin embargo, se puede identificar una fuente que fluye en el mundo y que es compartida por muchos países independientemente de su idioma y su cultura. Conocer las fuentes del derecho, es pues, relevante para conocer el derecho informático.

1. **Conceptos relacionados**

El concepto de fuentes del derecho es un tema de particular interés en las ciencias jurídicas actuales. Karl Von Savigny fue el encargado de acuñar el término a mediados del siglo XIX. Para Savigny: “El derecho tiene el carácter esencialmente popular, nacional, humano. El derecho es obra, no de la voluntad arbitraria, según pretendía Rousseau, sino de la conciencia del espíritu del pueblo. Afirmó la importancia de la costumbre como fuente del derecho positivo, acentúo la necesidad de estudiar la historia íntima de los pueblos, como medio de penetrar en su espíritu y de comprender así como en él se elabora el derecho, su derecho; por último determinó que el papel del legislador no debe ser crear el derecho, inventarlo, sino más bien, depurarlo y ordenarlo en vista de las corrientes dominantes en el seno mismo de las sociedades o mejor de los pueblos”. (Savigny, 1967, pp. 13-14)

Savigny creía que el derecho poseía un origen que podía ser determinado, esta idea, se hizo popular en las ciencias jurídicas. Es por este motivo que lo

que conoce como “Fuentes del derecho” concretiza la idea que el derecho tiene un único origen que lo encamina tal cual fuera una corriente de agua; sin embargo, en las ciencias jurídicas, no se puede hacer distinción de una teoría general de estas fuentes del derecho.

2. **Fuentes históricas:**

Víctor García Tomás, nos dice “son aquellos elementos que permiten reconstruir el proceso de formación del derecho a través de las distintas épocas”

Existen dos los elementos:

2.1. **Elementos directos:**

Obtienen información de modo inmediato:

- Normas escritas.
- Costumbres jurídicas.
- Jurisprudencia, etc.

2.2. **Elementos indirectos:**

Permiten complementar o ampliar la información que son obtenidas de los elementos directos:

- Crónicas.
- Testimonios.
- Restos arqueológicos.
- Expresiones folklóricas.
- Literatura.
- Informes administrativos.
- Documentos.
- Memorias.
- Cuantas.
- Estadísticas.

2.3. **Fuentes Reales:**

Como anota Claude du Pasquier, existe un “conjunto de fenómenos sociales que contribuyen a formar la sustancia o materia del derecho como movimientos ideológicos, necesidades prácticas, etc. (Pasquier, 1983, P. 266).

2.4. **Fuentes Formales del Derecho:**

Son los diversos modos como éste se manifiesta. Corresponde tal denominación a las normas jurídicas en relación con su origen.

Además, “Es aquel procedimiento, a través del cual se produce válidamente normas jurídicas que adquieren el rango de obligatoriedad propia del derecho y, por lo tanto, la característica de ser impuestas legítimamente a las personas mediante los instrumentos de coacción del Estado”. (Rubio Correa, 1985, p. 87)

Siendo las siguientes:

- La Legislación.

- La Jurisprudencia Fuentes Formales del Derecho.
- La Costumbre.
- La Doctrina.
- La Declaración de Voluntad.

2.5. **La pirámide kelseniana:**

Esta pirámide elaborada por Kelsen, establece jerarquías en cuanto a las normas que debemos usar para poder interpretar y la aplicar los diversos principios jurídicos.

Kelsen menciona que, “En el ordenamiento jurídico estatal, concebido como un sistema de normas gradualmente estructurado, el fundamento de validez de una norma lo constituye otra norma jerárquicamente superior. Es decir, toda norma de grado superior, funda la validez de una norma de grado inferior derivada de ella. A su vez, todo el ordenamiento así estructurado tiene un último fundamento de validez; es la norma fundamental hipotética, supuesto gnoseológico que confiere unidad al orden jurídico.” (Kelsen, 1946, P. 113).

Además, García Maynezindica que, “La tesis de Kelsen sobre las fuentes formales descansa en la doctrina de la estructuración escalonada del ordenamiento jurídico, puesto que el problema de la vigencia de las distintas normas se resuelve, refiriéndolas a las que condicionan su fuerza obligatoria, del mismo modo, que la de éstas es después referida a otras de grado más alto, hasta que el fin se llega a la suprema, de la cual depende la existencia de todas las restantes.” (García Maynez, 1989. p. 17-18.)

Ilustración 1: Piramide kelseniana
Fuente: Kelsen

3. **Legislación Informática.**

Es muy amplia, ha dificultado los trabajos relacionados con su aplicación, las TICs apoyaron para crear sistemas digitalizados, los que facilitan el trabajo de los operadores del derecho creándose diferentes sistemas. Así, se han creado sistemas como el SPIJ que reúne las normas legales peruanas en general (Legislación del Perú).

3.1. El Sistema Peruano de Información Jurídica – SPIJ

Para este caso se tomará la definición de la propia página web del SPIJ:

> "Es una edición a través de medios electrónicos elaborada por el Ministerio de Justicia y Derechos Humanos del Perú, en cumplimiento a su función de sistematizar y difundir la legislación, expresada en la Ley de Organización y Funciones del Sector Justicia y Derechos Humanos (Ley N° 29809, Artículo 7° inciso j), y Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos en el Decreto Supremo N° 011-2012-JUS, Artículo 5° numeral 5.2, inciso j. Contiene la legislación nacional vigente y derogada en textos completos y concordados y actualizados, así como información jurídica complementaria.
>
> En tal sentido, el SPIJ contiene: Constitución Política de 1979 y 1993, 12 Códigos (Civil, Penal, Procesal Civil, etc), Leyes Orgánicas, Compendios de Legislación por Materias, Legislación General y Particular (Poderes del Estado, Organismos Autónomos, Gobiernos Regionales y Locales, etc), Textos Únicos de Procedimientos Administrativos – TUPAS, Jurisprudencia Judicial y Administrativa, Directorio de Asesorías Jurídicas.
>
> Cuenta con potentes herramientas de búsqueda y recuperación de la información que le permite un acceso fácil y fluido a la legislación a través de palabras, frases, número de norma, tipo de norma, por materia, por sectores, fecha de publicación, a nivel de sumillas, por órgano emisor, etc. Asimismo, permite imprimir todos los textos, formatos, anexos y gráficos contenidos en el sistema, así como copiarlos a un procesador de textos de acuerdo a su necesidad" (PSIJ, 2016).

3.2. Gaceta Jurídica

Es la publicación de Derecho de mayor reconocimiento en el medio gracias a la calidad de información que mensualmente proporciona a través de sus diversas publicaciones, productos y servicios que integran su paquete de suscripción.

Desde hace más de diecisiete años los abogados y jueces del país que se suscriben a Gaceta Jurídica han obtenido beneficios significativos en el ejercicio de su profesión. Mensualmente cuentan con las herramientas que le ayudan a simplificar su trabajo accediendo no solo al universo de los textos normativos publicados (sistematizados y actualizados), sino también a los artículos de análisis y comentarios, así como a la jurisprudencia, casuística y absolución de consultas; permitiéndoles entender a cabalidad los contenidos y alcances no solo de los dispositivos legales sino también de los temas jurídicos de mayor actualidad y relevancia.

La calidad y el rigor de la información que Gaceta Jurídica proporciona se deben al equipo de calificados profesionales que elabora esta publicación. En este sentido cuenta con una organización debidamente estructurada con el objeto de garantizar que la información producida cubra las verdaderas necesidades de los abogados, jueces y demás operadores jurídicos. (Gaceta Jurídica, 2016).

3.3. **Actualidad Penal**

Es una publicación especializada en materia penal, procesal penal, penitenciaria, criminológica y temas afines, desarrollada por los más destacados especialistas nacionales e internacionales en estos campos. Los Jueces, Fiscales y Abogados encontrarán en esta revista un alto valor dogmático y práctico como características predominantes en sus contenidos. (Actualidad Penal, 2016).

TEMA N° 3: EL DERECHO INFORMÁTICO

El Dr. Wilhelm Steinmüller de la Universidad de Regensburg en Alemania fue el primero en utilizar el término "Derecho Informático" en 1970. Este termino no es el único puesto que también se le ha llamado, Iuscibernética, Derecho de las nuevas tecnologías, derecho telemático, Derecho de la sociedad de la información, Derecho tecnológico, entre otros. El Derecho informático como rama complementaria del derecho, es de importancia para aquellos que requieren ser parte de la sociedad de la información y sus beneficios y responsabilidades.

1. **Conceptos**

Flores Gómez F. menciona que el Derecho proviene del vocablo latino Directum, que significa en su primer origen, lo que dirige o es bien dirigido, no apartarse del buen camino, seguir el sendero señalado por la ley (Flores, 2004, p. 2)

La revista electrónica Master Magazín, contiene el artículo escrito por Ana Cecilia Lancillota quien expresa que la "informática es la ciencia que tiene como objetivo estudiar el tratamiento automático de la información a través de la computadora." (Lancillota, 2007, p. 23)

Téllez Valdes J. lo define como "…una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica y como objeto de estudio (Derecho de la información)" (Téllez, 1991, p. 73).

En la Revista electrónica Alfa-Redi, se encuentra un artículo escrito por Rodríguez Hernández V. quien cita la definición expresada por el Dr. Fix Fierro H., "La Informática Jurídica debe entenderse como el conjunto de estudios e instrumentos derivados de la aplicación de la informática al derecho o as precisamente, a los procesos de creación, aplicación y conocimiento del derecho". (Rodríguez Hernández, 2007)

De todo esto se concluye que el derecho informático es en su conjunto un grupo de normas que regulan el accionar, los diversos procedimientos y procesos, productos y su aplicación jurídica relacionados a la informática y las áreas relacionadas. Es, además, el conglomerado de todas las normas, leyes y principios que pueden aplicarse a las actividades y hechos derivados de la ciencia informática.

2. **Características:**

- Es de carácter moderno, comparado con las ramas habituales del Derecho, Se originan en su origen en el uso de los computadores en la sociedad.
- Está influenciado por las TICs, como base en los ordenadores y su entorno.
- Está relacionado con la globalización, En cada caso en particular, el administrador de justicia debe considerar todo lo relacionado a una situación en particular y al mismo tiempo que involucra a otras fuentes del mundo.
- Debe tener leyes exclusivas, esto se debe a que la naturaleza de las TICs es muy cambiante.
- Es autónomo, porque cuenta con instituciones especializadas encargas de proveer alternativas de solución de tipo legal a problemas que se generan por el cambiante avance tecnológico y científico.

3. **Informática Jurídica**
   - Es la ciencia que se dedica al estudio del manejo de los recursos informáticos (hardware y software) a fin de mejorar los procesos análisis, investigación y gestión en el ámbito jurídico.
   - Es también, el "tratamiento automatizado de las fuentes de conocimiento jurídico (sistemas de documentación legislativa, jurisprudencial y doctrinal), de las fuentes de producción jurídica y su organización (funcionamiento de organismos legislativos y judiciales) y de las decisiones judiciales (informática jurídica decisional)" (Pérez Luño, 2003. P. 55).

4. **Origen y Evolución**

   Con respecto a su origen y evolución se hará referencia al estudio del Dr. Peñaranda Quintero H. (Peñaranda Quintero H, 2013),
   - En el año de 1938 se creó la primera máquina para cálculos orientada al ámbito jurídico; la cual se encontraba en la Cámara de Representantes en el estado de Ohio en los Estados Unidos. Esta máquina utilizaba tarjetas perforadas para su funcionamiento y se utilizó para dar seguimiento a las iniciativas de ley.
   - En los años cincuenta, se desarrollaron una serie de investigaciones con el propósito de poder recuperar documentos de índole jurídica de forma automática. Así también se empieza a usar ordenadores para otros usos aparte de los cálculos matemáticos, tales como lingüísticos. Luego de esto se desarrolló una iniciativa para contar con acceso a la información legal de forma automática por medio de la iniciativa de John Horty en la Universidad de Pittsburg, Pennsylvania.
   - En 1.959, los ordenamientos jurídicos de Pennsylvania fueron puestos en cintas magnéticas por la Universidad de Pennsylvania dando origen a la recopilación informática legal, la cual fue mostrada el siguiente año ante la Asociación Americana de Abogados en Washington, D.C. Posteriormente, La Corporación de Sistemas Aspen se encargó del rediseño del sistema legal automático y luego lo comercializó. Asi se dio inicio a los ordenamientos legales
   - Para 1966, 12 fueron los estados tenían dicho sistema y en 1968, 50 estados lo aceptaron. Es pues en la década de los 60 donde se da inicio a los sistemas automatizados legales.
   - El sistema Lite (hoy Flite) y el sistema Aspen, surgen surgen en este tiempo.

- En 1.964 luego del éxito de los demás sistemas, la Corporación Americana de Recuperación de Datos comercializó por primera vez los sistemas que procesaban datos legislativos.
- Posteriormente, en 1967, la denominada Corporación de Investigación Automatizada perteneciente a la Barra de Ohio, creo también sistemas con un enfoque en los abogados litigantes, el cual se llamó OBAR.
- El sistema LEXIS llegó a sustituir al sistema OBAR en 1973.

5. Clasificación de la informática jurídica

5.1. Informática Jurídica Documental:

El área documental es por sí la más antigua de las áreas de la informática jurídica; tiene como origen las investigaciones llevadas a cabo en la Universidad de Pittsburg por John Horty.

María Fernanda Guerrero M., en su publicación "La inteligencia artificial aplicada al derecho" en la Revista uno y cero de Milán, la define como "la aplicación de técnicas informáticas a la documentación jurídica en aspectos sobre análisis, archivo y recuperación de información contenida en la legislación, jurisprudencia, doctrina o cualquier otro documento con contenido jurídico relevante". (Guerrero Molina, 1999. P. 64)

Consiste en el empleo de los sistemas de información y documentación jurídica. Se integran por la legislación, la doctrina y la jurisprudencia, siendo fundamento principal de los bancos de datos jurídicos. Todo esto con la finalidad de ser de apoyo a la toma de decisiones. La relevancia de la informática jurídica en el ámbito documental se fundamenta sobre el principio de que el ordenador facilite información adecuada al jurista para ayudarle a adoptar una determinada decisión. Supone el tratamiento y recuperación de información jurídica por medio de los ordenadores, y en los tres tradicionales campos de legislación, jurisprudencia y bibliografía.

Entre los sistemas pioneros de consulta de bases de datos jurídicas fueron los sistemas Batch, estos permitieron una búsqueda en archivos de texto que contenían palabras ordenadas de forma alfabética, estas consultas daban como respuesta la ubicación de los archivos o ficheros específicos donde se encontraba la información, lo cual permitía realizar búsquedas al combinar palabras con el fin de hacer la búsqueda más específica, separando la información general de la especifica.

Luego de los sistemas Batch se utilizaron los sistemas en línea para trabajar con Internet, con espacios multimedia, interactivos, y software especializado como los sistemas expertos y de inteligencia artificial.

Entre los métodos de búsqueda existen:

- **Texto completo:** Se utiliza el mismo criterio de búsqueda a todo el texto.

- **Palabras clave:** Se aplica un criterio de búsqueda a un grupo de palabras claves el texto a analizar.

- **Resumen:** Se aplica un criterio de búsqueda a un resumen del texto.

5.2. **Informática Jurídica para la gestión y el control:**

Se utilizan programas informáticos para gestiones y actividades jurídicas tales como mandatos judiciales, certificaciones y contratos.

5.3. **Subclasificación**

5.3.1. Informática Registral:

Para la administración pública, es conveniente acelerar los procesos de registro y para esto se utiliza un tratamiento electrónico de la información; en este caso se realizan los procesos de almacenamiento de información y también su actualización correspondiente.

5.3.2. Informática Parlamentaria:

Dentro del entorno parlamentario, se hace uso de la informática para poder guardar registro de los debates, bibliografía, información de proyectos, entre otros con la finalidad de informar sobre los actos del gobierno y como registro de sus actividades.

5.3.3. Informática para la Gestión en los Estudios Jurídicos:

Se hace uso de la informática para el manejo del estudio jurídico y de este modo, agilizar sus procesos. Se logra el manejo de agendas, cobranza y facturación, gestión de recursos humanos, entre otros manejos propios de estos estudios.

5.3.4. Informática Notarial:

Dentro de las notarías se utiliza la informática para generar documentos e interactuar con ellos desde la perspectiva notarial y registral.

5.3.5. Informática Jurídica Decisoria o Metadocumental:

Ayuda, por medio de sistemas inteligentes, en la toma de decisiones, proveyendo soluciones a problemas jurídicos específicos. Esta inteligencia artificial, hace uso de sistemas expertos que logran estructurar conocimientos especializadospara obtener conclusiones basados en la información que se les ha suministrado considerando el esquema pregunta y respuesta.

El esquema de un sistema experto es:

- Una base de conocimientos (base de datos).
- Las reglas de razonamiento para el ente.
- La interfaz que permite la comunicación.

La informática jurídica para la toma de decisiones aun es nueva, pero es capaz de proveer los medios necesarios para la toma de decisiones.

TEMA N° 4: La Libertad Informática

Con respecto a lo visto a la sociedad de la información, se deben establecer los límites de libertad en relación a la información que se comparte. Por lo tanto, una forma de establecer estos límites es a través del derecho y las regulaciones que la ley exige. Sin embargo, todo empieza con el acceso a esta información, lo cual se considera como uno de los objetivos de la sociedad de la información.

1. **Antecedentes**

La libertad informática es entendida como el derecho al acceso a los servicios informáticos; quiere decir, que contempla la información familiar y personal que posee un individuo.

La Constitución Política del Perú indica en su Artículo 2° que, "Toda persona tiene derecho:

.....

6. "A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar."

La libertad informática garantiza a los ciudadanos el derecho fundamental a:

- **Información:** Que los usuarios puedan conocer sobre la finalidad y titularidad de la información concerniente a ellos que se encuentra en los bancos de datos.
- **Control**: Se les brinda a los usuarios la facultad de acceder a la información que les concierne.
- **Tutela**: les permite a los usuarios controlar la información en las tarjetas de un programa de computadora que contiene los datos personales inscritos.

2. **Legislación peruana.**

A continuación se citan normas que se aplican en el Perú sobre TICs y que se encuentran en la página web del (ONGEI, 2016)

2.1. **Constitución Política del Perú**

La constitución de nuestro país hace referencia a este derecho en los siguientes artículos:

- Inciso 3 del artículo 200
- Incisos 5 del artículo 2
- Incisos 6 del artículo 2
- Ley referida a la aplicación de la Acción Constitucional de Hábeas Data en la LEY Nº 26301, modificada en la ley Nº 26470

2.2. **Manifestación de Voluntad por Medios Electrónicos**

- Ley que permite el uso de medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica. LEY Nº 27291

2.3. **Firmas y Certificados Digitales**

- Ley de Firmas y Certificados Digitales LEY Nº 27269
- Ley que modifica la Ley de Firmas y Certificados Digitales, en relación con Certificados emitidos por Entidades Extranjeras LEY Nº 27310
- Comisión multisectorial encargada de elaborar el Reglamento de la Ley de Firmas y Certificados Digitales, RESOLUCION SUPREMA 098-2000-JUS
- Disposiciones complementarias al Reglamento de la Ley de Firmas y Certificados Digitales RESOLUCION COMISION DE REGLAMENTOS TECNICOS Y COMERCIALES Nº 0103-2003-CRT-INDECOPI
- Reglamento de la Ley de Firmas y Certificados Digitales DECRETO SUPREMO N° 004-2007-PCM
- Reglamento de la Ley de Firmas y Certificados Digitales, DECRETO SUPREMO Nº 052-2008-PCM

2.4. **Delitos Informáticos**

- Ley que incorpora los delitos informáticos al Código Penal LEY Nº 27309
- Delito de Violación a la Intimidad, CODIGO PENAL, Artículo 154
- Uso Indebido de Archivos Computarizados CODIGO PENAL, Artículo 157
- Hurto Agravado por Transferencia Electrónica de Fondos CODIGO PENAL, Artículo 185
- Delitos contra los Derechos de Autor Difusión, distribución y circulación de la obra sin la autorización del autor, CODIGO PENAL, Artículo 217
- Plagio y comercialización de obra, CODIGO PENAL, Artículo 218

2.5. **Microformas - normas generales:**

- Dictan normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuan-to la producida por procedimientos informáticos en computadoras. DECRETO LEGISLATIVO Nº 681
- Reglamento del Decreto Legislativo Nº 681, sobre el uso de tecnologías de avanzada en materia de archivos de las empresas DECRETO SUPREMO Nº 009-92-JUS
- Modifican el D. Leg. N° 681, mediante el cual se regula el uso de tecnologías avanza-das en materia de archivo de documentos e información LEY Nº 26612
- Decreto Legislativo Nº 827, Amplían los alcances del D. Leg. Nº 681 a las entidades públicas a fin de modernizar el sistema de archivos oficiales.

2.6. **Correo Electrónico - Normas Generales**

- Ley del Procedimiento Administrativo General, Ley 27444
- Facultades, normas y organización del INDECOPI - DECRETO LEGISLATIVO Nº 807 Inciso d) del artículo 24

- Ley General de Sociedades LEY N° 26887, Artículo 245 Inciso 3 del artículo 294
- Ley que regula el uso del Correo Electrónico Comercial No Solicitado (SPAM) - LEY N° 28493
- Reglamento de la Ley Nº 28493 que regula el envío del correo electrónico comercial no solicitado (SPAM), DECRETO SUPREMO Nº 031-2005-MTC
- Reglamento General de la Ley de Telecomunicaciones DECRETO SUPREMO Nº 06-94-TCC Artículo 102
- Texto Único Ordenado de la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública, DECRETO SUPREMO Nº 043-2003-PCM.
- Directiva sobre "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública" RESOLUCIÓN JEFATURAL N° 088-2003-INEI.
- Reglamento de la Ley de Transparencia y Acceso a la Información Pública, DECRETO SUPREMO 072-2003-PCM.
- Directiva que establece disposiciones que regulan documentos internos del ministerio vía correo electrónico. RESOLUCIÓN DE SECRETARÍA GENERAL Nº 020-2004-VIVIENDA-SG.
- Ley del Silencio Administrativo, LEY 29060.
- Servicio de Notificaciones Electrónicas en el Poder Judicial, RESOLUCION ADMINISTRA-TIVA 214-2008-CE-PJ.
- Lineamientos y mecanismos para implementar la interconexión de equipos de procesamiento electrónico de información entre las entidades del Estado, ESOLUCION MI-NISTERIAL 381.
- Comisión Multisectorial Temporal encargada de elaborar el “Plan Nacional para el Desarrollo de la Banda Ancha en el Perú” RESOLUCION SUPREMA Nº 063-2010-PCM.
- Comité Coordinador de la Infraestructura de Datos Espaciales del Perú - IDEP. RESOLU-CION MINISTERIAL Nº 126-2003-PCM

2.7. **Software**

- Ley que norma el uso, adquisición y adecuación del software en la administración pública, LEY N° 28612
- Reglamento de la Ley N° 28612, Ley que norma el uso, adquisición y adecuación del software en la Administración Pública, DECRETO SUPREMO N° 024-2006-PCM
- "Guía Técnica sobre Evaluación de Software para la Administración Pública", RESOLUCION MINISTERIAL Nº 139-2004-PCM
- Guía para la Administración Eficiente del Software Legal en la Administración Pública, RESOLUCION MINISTERIAL Nº 073-2004-PCM
- Medidas para garantizar la legalidad de la adquisición de software en entidades y de-pendencias del sector público, Decreto Supremo Nº 013-2003-PCM y sus modificatorias
- Decreto Supremo 076-2010-PCM, Decreto Supremo que modifica el Decreto Supremo Nº 013-2003-PCM estableciendo disposiciones referidas a las adquisiciones de computadoras personales que convoquen las entidades públicas

2.8. **Internet**

- Lineamientos de Políticas Generales para promover la masificación del acceso a Inter-net en el Perú, DECRETO SUPREMO Nº 066-2001-PCM
- Proyecto Piloto en Telecomunicaciones "Cabinas de Acceso Público a Internet - Banco de la Nación" RESOLUCION MINISTERIAL Nº 347-2001-MTC-15.03
- Crean el Proyecto Huascarán DECRETO SUPREMO Nº 067-2001-ED

- Reglamento del Fondo Nacional para el Uso de Nuevas Tecnologías en la Educación - FONDUNET DECRETO SUPREMO Nº 070-2001-ED

2.9. **Páginas Web (Portal)**

- Directiva sobre publicación en la Página Web del Ministerio de con-vocatorias y resulta-dos de procesos de concurso, licitación y ad-judicación directa pública que se realicen en el sector RESOLUCION MINISTERIAL Nº 220-2001-MTC-15.14
- Portal de Transparencia Económica como plataforma informativa del Ministerio de Economía y Finanzas para los ciudadanos a través de Internet - DECRETO DE URGEN-CIA Nº 077-2001
- Precisan información que publicará OSINERG en su página Web y en el Diario Oficial El Peruano RESOLUCION DE CONSEJO DIREC-TIVO Nº 1170-2001-OS-CD
- Disponen difusión periódica de la relación de proveedores aptos para el pago por ser-vicios y bienes recibidos a través de la pági-na Web de ESSALUD RESOLUCION DE PRESIDENCIA EJECUTIVA Nº 446-PE-ESSALUD-2001
- Reglamento del Sistema de Denuncias por Web RESOLUCION DE LA FISCALIA DE LA NACION N° 1205-2001-MP-FN
- Página Web del Poder Judicial – RESOLUCION ADMINISTRATIVA DE PRESIDENCIA Nº 198-2001-P-CS
- Directiva "Normas y Procedimientos Técnicos sobre Contenidos de las Páginas Web en las Entidades de la Administración Pública" - RESOLUCION JEFATURAL N° 234-2001-INEI
- Directiva "Lineamientos para la implementación del Portal de Transparencia Estándar en las entidades de la Administración Pú-blica" RESOLUCION MINISTERIAL Nº 200-2010-PCM.
- Evaluación de Portales Institucionales de la Administración Pública - 2010" RESOLUCION MINISTERIAL Nº 362-2010-PCM
- Ventanilla Única del Estado a través del Portal de Servicios al Ciu-dadano y Empresas y se crea el Sistema Integrado de Servicios Públicos Virtuales, DECRETO SUPREMO N° 019-2007-PCM

2.10. **Portal del Estado Peruano**

- Portal del Estado Peruano como sistema interactivo de información a los ciudadanos a través de Internet - DECRETO SUPREMO N° 060-2001-PCM
- Portal de Servicios al Ciudadano y Empresas – PSCE - DECRETO SUPREMO N° 032-2006-PCM
- Centro de Administración del Portal del Estado Peruano – CAPEP RESOLUCIÓN JEFATU-RAL N° 229-2001-INEI
- Directiva "Normas y Procedimientos Técnicos sobre Contenidos de las Páginas Web en las Entidades de la Administración Pública RE-SOLUCIÓN JEFATURAL N° 234-2001-INEI

- Directiva "Normas y Procedimientos Técnicos para garantizar la Seguridad de la In-formación publicadas por las entidades de la Administración Pública" RESOLUCION JEFATURAL N° 347-2001-INEI
- Directiva N° 006-2002-INEI/DTNP sobre "Normas y Procedimientos Técnicos para la Actualización de Contenidos del Portal del Estado Peruano" RESOLUCION JEFATU-RAL N° 160-2002-INEI
- Implementación del Portal de Transparencia Estándar en las Entidades de la Administración Pública, - DECRETO SUPREMO Nº 063-2010-PCM
- Administración del "Portal del Estado Peruano" - DECRETO SUPREMO Nº 059-2004-PCM
- Ventanilla Única del Estado a través del Portal de Servicios al Ciudadano y Empresas y se crea el Sistema Integrado de Servicios Públicos Virtuales DECRETO SUPREMO N° 019-2007-PCM

2.11. Nombres de Dominio

- Encargan al INDECOPI la administración del nombre de dominio correspondiente al Perú en Internet - RESOLUCION SUPREMA Nº 292-2001-RE
- Directiva "Normas Técnicas para la asignación de nombres de Dominio de las entidades de la Administración Pública" - RESOLUCIÓN JEFATURAL N° 207-2002-INEI
- Constituyen Comisión Multisectorial de Políticas del Sistema de Nombres de Dominio, - RESOLUCION MINISTERIAL Nº 285-2005-PCM

2.12. Sociedad de la Información

- Convenio a suscribirse con el PNUD para ejecutar Proyecto "Desarrollo de la Sociedad de la Información", RESOLUCION SUPREMA Nº 004-2003-MTC
- Comisión Multisectorial para el Desarrollo de la Sociedad de la Información - CODESI RESOLUCION MINISTERIAL Nº 181-2003-PCM
- Adenda al Convenio con el PNUD para administración del Proyecto PER/03/005 "Desarrollo de la Sociedad de la Información en el País". RESOLUCION SUPREMA Nº 014-2003-MTC
- Publicación en la Web de PCM y CODESI, informes relacionados al desarrollo de la sociedad de la información en el Perú RESOLUCION MINISTERIAL Nº 235-2004-PCM
- Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Pe-ruana, DECRETO SUPREMO N° 031-2006-PCM
- Reglamento Interno de la Comisión Multisectorial Permanente para el Seguimiento y Evaluación del "Plan de Desarrollo de la Sociedad de la Información – La Agenda Digital Peruana" (CODESI)

2.13. Simplificación Administrativa

- Ley que modifica el párrafo 38.3 del artículo 38º de la Ley Nº 27444, Ley Del Procedimiento Administrativo General, y establece la publicación de diversos dispositivos le-gales en el Portal del Estado Peruano y en Portales Institucionales, LEY 29091
- Reglamento de la Ley Nº 29091 - Ley que modifica el párrafo 38.3 del artículo 38º de la Ley Nº 27444, Ley del Procedimiento Admi-

nistrativo General, y establece la publicación de diversos dispositivos legales en el Portal del Estado Peruano y en Portales Institucionales, DECRETO SUPREMO 004-2008-PCM

- Decreto Legislativo que Modifica la Ley del Procedimiento Administrativo General - Ley 27444 y la Ley del Silencio Administrativo - Ley 29060, DECRETO LEGISLATIVO 1029
- Plan Nacional de Simplificación Administrativa, RESOLUCIÓN MINISTERIAL Nº 228-2010-PCM,
- Establecen el uso del Sistema de Programación y Gestión por Metas y Resultados de-nominado Sistema de Metas SIGOB/Perú, DECRETO SUPREMO Nº 038-2010-PCM
- Centro de Atención Telefónica "Aló MAC" como servicio integrado de atención dirigido a la ciudadanía, DECRETO SUPREMO Nº 027-2010-PCM

2.14. **Gobierno Electrónico**

- Estrategia Nacional de Gobierno, RESOLUCION MINISTERIAL Nº 274-2006-PCM
- Uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2004 Tecnología de la Información. "Procesos del Ciclo de Vida del Software, 1ª Edición" en entidades del Sistema Nacional de Informática, RESOLUCION MINISTERIAL Nº 179-2004-PCM
- Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática, RESOLUCION MINISTERIAL Nº 247-2006-PCM
- Formulación y evaluación del Plan Operativo Informático de las entidades de la Administración Pública y su Guía de Elaboración, RESOLUCION MINISTERIAL Nº 19-2011-PCM
- Lineamientos que establecen el contenido mínimo de los Planes Estratégicos de Gobierno Electrónico, - RESOLUCIÓN MINISTERIAL Nº 61-2011-PCM

LECTURA SELECCIONADA N° 1

Trejo Delarbre, R. (2001). Vivir en la Sociedad de la Información Orden global y dimensiones locales en el universo digital. Revista iberoamericana de ciencia, tecnología, sociedad e innovación. P. 1 Disponible en: http://www.oei.es/revistactsi/numero1/trejo.htm

ACTIVIDAD N° 1

Instrucciones

- Ingrese al foro y participe con comentarios críticos y analíticos del tema Sociedad de la Información
- Lea y analice el tema N° 1 y 3 del manual
- Responda en el foro a las preguntas acerca de Sociedad de la Información y Derecho Informático

  ¿Cuál es el objetivo de la Cumbre de Ginebra?

¿Cuál es la diferencia entre informática jurídica documental e informática jurídica de gestión?

¿Cómo se puede fomentar el uso de las TICs en el Perú? Brinde 5 ejemplos

¿Qué posibles problemas podría traer el avance de la sociedad de la información para el país? Mencione 5 posibles problemas.

GLOSARIO DE LA UNIDAD I

1. Cumbre Mundial sobre la Sociedad de la Información (CMSI):

Se desarrolló en dos fases. La primera fase tuvo lugar en Ginebra acogida por el Gobierno de Suiza, del 10 al 12 de diciembre de 2003 y la segunda en Túnez acogida por el Gobierno de Túnez, del 16 al 18 de noviembre de 2005. (WSIS, 2016)

2. Jurisprudencia:

Es el conjunto de sentencias o resoluciones judiciales emitidas por órganos judiciales y que pueden repercutir en sentencias posteriores. Legislación. (Hess Araya, 2009)

3. Doctrina Jurídica:

Es un concepto que sustentan los juristas y que influye en el desarrollo del ordenamiento jurídico, aunque cuando no originan derecho de forma directa. (Hess Araya, 2009.En línea)

4. Iuscibernetica :

Es la interrelacion entre el Derecho y la Informatica, para algunos autores es la ciencia que estudia el control que tiene el hombre sobre la maquina en el campo del Derecho., son los fenomenos de interrelacion juridico social y las tecnicas de formalizacion del Derecho aplicadas al conocimiento del funcionamiento de las computadoras. (Hess Araya, 2009)

5. Pirámide kelseniana:

Es un sistema del derecho que ordena sus prioridades en forma de pirámide, de esta forma se busca especificar cuál es el orden jerárquico de las leyes que rigen a la sociedad. (definiciónyque, 2016)

6. SPIJ:

El Sistema Peruano de Información Jurídica**,** contiene: Constitución Política de 1979 y 1993, 12 Códigos (Civil, Penal, Procesal Civil, etc), Leyes Orgánicas, Compendios de Legislación por Materias, Legislación General y Particular (Poderes del Estado, Organismos Autónomos, Gobiernos Regionales y Locales, etc), Textos Únicos de Procedimientos Administrativos – TUPAS, Jurisprudencia Judicial y Administrativa, Directorio de Asesorías Jurídicas. (SPIJ, 2016)

7. Certificados Digitales

Es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet. Se trata de un requisito indispensable para que las instituciones puedan ofrecer servicios seguros a través de Internet. (IVNOSYS, 2016)

8. INDECOPI

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI, 2016)

BIBLIOGRAFÍA DE LA UNIDAD I

1. Toffler, A. (1980). The third wave. New York : William Morrow
2. Castells, M. (1995). La ciudad informacional: tecnologías de la información, reestructuración económica y el proceso urbano regional. Madrid : Alianza, 412 p.).
3. Webster, F. Theories…, op. cit., p. 10. (Prólogo de A. Posada. Savigny Ob.Cit. Editorial La España Moderna. Madrid. Pp. 13-14)
4. Laclaun, M. (1984) "La Constitución de la Noción "Fuentes del Derecho" en el Pensamiento Occidental". Anuario de Filosofía Jurídica y Social de la Asociación Argentina de Derecho Comparado. Abeledo-Perrot. Buenos Aires.
5. Pasquier, C. (1983) Introducción al Derecho. Lima, Justo Valenzuela
6. Rubio Correa, M. (1946). Ob. Cit. Kelsen, Hans. Editorial Losada. Buenos Aires. P. 113.
7. García Maynez, E. (1949). "Diálogo sobre las Fuentes Formales del Derecho". Revista de la Escuela Nacional de Jurisprudencia. Tomo XI. N°41. Enero-Marzo. México D.F. Pp. 17-18.)
8. SPIJ. (2016). Disponilble en: http://spij.minjus.gob.pe/spij.html
9. Téllez Valdes, J. (2008). Derecho Informático. México: Instituto de Investigaciones Jurídicas, p.13
10. Peñaranda Quintero H. (2013). La informática jurídica: mecanismo de gestión de la información jurídica. Disponible en: http://www.cibersociedad.net/congreso/comms/c13penaranda2.htm
11. Internet Governance Forum. (2013).Sociedad de la información. Disponible en: http://www.intgovforum.org/cms/
12. Gaceta Jurídica. (2016). Disponible en: http://www.gacetajuridica.com.pe/gaceta-producto/gacetajuridica.php
13. Actualidad Penal. (2016). Disponible en: http://actualidadpenal.com.pe/quienes-somos.html
14. Lancillota, Ana cecilia. (2007). Definición y significado de informática Revista digital Master Magazín. http://www.mastermagazine.info/termino/5368.php
15. Rodríguez Hernández, Víctor. (2007). La informática jurídica y su papel en el Derecho Mexicano Alfa-Redi Revista de Derecho Informático electrónica. Disponible en: http://docente.ucol.mx/daniel_or/public_html/Marcot.doc.
16. Trejo Delarbre, R. (2001). Vivir en la Sociedad de la Información Orden global y dimensiones locales en el universo digital. Revista iberoamericana de ciencia, tecnología, sociedad e innovación. P. 1 Disponible en: http://www.oei.es/revistactsi/numero1/trejo.htm
17. WSIS, (2016). Disponible en: http://www.itu.int/net/wsis/index-es.html
18. Hess Araya, C. (2009). Diccionario básico de derecho informático. Disponible en: http://derechoinformaticouna.blogspot.pe/2009/diccionario-basico-del-derecho.html
19. Definicionyque. (2016). Definiciones. Disponible en: http://definicionyque.es/piramide-de-kelsen/
20. SPIJ. (2016). Disponilble en: http://spij.minjus.gob.pe/spij.html
21. IVNOSYS (2016). Proyectos. Disponible en: http://www.ivnosys.com/es/proyectos/
22. INDECOPI (2016). Disponible en: https://www.indecopi.gob.pe/inicio

AUTOEVALUACIÓN Nº 1

1. ¿Qué es la Sociedad de la Información?
   a) La Internet y su función de herramienta social y comercial.
   b) La Cumbre Mundial sobre la Sociedad de la Información.
   c) La revolución digital en las tecnologías de la información y las comunicaciones (TIC) que ha creado una plataforma para el libre flujo de información en el planeta.
   d) La revolución documentaria en las tecnologías de la información y las comunicaciones (TIC) que ha creado una plataforma para el libre flujo de información en el planeta.

2. La revolución digital es :
   a) El rápido desarrollo de las TICs ha cambiado fundamentalmente la manera en que la gente piensa, actúa, comunica, trabaja y gana su sustento.
   b) La llamada revolución digital no ha forjado nuevas modalidades de crear conocimientos, educar a la población y transmitir información.
   c) La llamada revolución documentaria ha forjado nuevas modalidades de crear conocimientos, educar a la población y transmitir información.
   d) a y b son correctas.

3. Cuál de los enunciados son correctos
   i. Ha reestructurado la forma en que los países hacen negocios y rigen su economía, se gobiernan y comprometen políticamente. ( )
   ii. No ha proporcionado la entrega rápida de ayuda humanitaria y asistencia sanitaria, y una nueva visión de protección del medio ambiente. Y hasta ha creado nuevas formas de entretenimiento y ocio. ( )
   iii. Puesto que el acceso a la información y los conocimientos es un requisito previo para conseguir los Objetivos de Desarrollo del Milenio, no tiene la capacidad de mejorar el nivel de vida de millones de personas en todo el mundo. ( )

   a) VFF b) FFV c)VFV d)VVV

4. ¿Qué es la brecha digital?
   a) La brecha no se produce tanto a través de las fronteras internacionales como dentro de las comunidades, ya que la gente queda a uno u otro lado de las barreras económicas y de conocimientos.
   b) En la CMSI de Ginebra los líderes mundiales declararon: " No estamos plenamente comprometidos a convertir la brecha digital en una oportunidad digital para todos, especialmente aquellos que corren peligro de quedar rezagados y aún más marginados".
   c) La brecha digital separa los que están conectados a la revolución digital de las TIC de los que no tienen acceso a los beneficios de las nuevas tecnologías.
   d) La brecha digital unifica los que están conectados a la revolución digital de las TIC de los que no tienen acceso a los beneficios de las nuevas tecnologías.

5. Cuál es la jerarquización de las normas jurídicas según la pirámide de KELSEN

a) Resolución Directoral., Ley, Decretos Legislativos, Decretos Supremos, Normas Regionales, Resolución Legislativa, Resolución Suprema, Resolución Ministerial, Resolución Viceministerial, Resolución Jefatural, Constitución,
b) Constitución, Ley, Decretos Legislativos, Decretos Supremos, Normas Regionales, Resolución Legislativa, Resolución Suprema, Resolución Ministerial, Resolución Viceministerial, Resolución Jefatural, Resolución Directoral.
c) Resolución Directoral., Resolución Viceministerial, Decretos Legislativos, Decretos Supremos, Normas Regionales, Resolución Legislativa, Resolución Suprema, Resolución Ministerial, Ley, Resolución Jefatural, Constitución
d) Resolución Directoral., Constitución, Resolución Viceministerial, Decretos Legislativos, Decretos Supremos, Normas Regionales, Resolución Legislativa, Resolución Suprema, Resolución Ministerial, Ley, Resolución Jefatural.

6. Legislación Aplicada a la Informática : El Decreto Legislativo Nº 681
   a) Dicta normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto la producida por procedimientos informáticos en computadoras.
   b) Sobre los efectos legales de los documentos digitales obtenidos producto del microfilmado. (Publicado en el Diario Oficial "El Peruano" el 14 de octubre de 1991)
   c) Declara de necesidad pública el desarrollo de telecomunicaciones y aprueban normas que regulan la Promoción de Inversión Privada
   d) Declara de necesidad privada del desarrollo de telecomunicaciones y aprueban normas que regulan la Promoción de Inversión Privada

7. Microformas:
   En el Perú el uso de las tecnologías de avanzada en materia de archivo de documentos e información está regulada por un conjunto de normas legales orientadas a:
   a) No se aprovecha los adelantos de la tecnología en beneficio de actividades empresariales, alentando las inversiones y mejorando sus rendimientos.
   b) Otorgar reconocimiento de valor legal a los archivos conservados mediante microformas que permitan ahorro de espacio y costos a las organizaciones, colaborando a su eficiencia y productividad.
   c) No se aprovecha los adelantos de la tecnología en beneficio de actividades empresariales, alentando la reparación civil y mejorando sus rendimientos.
   d) Se aprovecha los adelantos de la ciencia y el derecho en beneficio de actividades empresariales, alentando las inversiones y mejorando sus rendimientos paulatinamente.

8. La gestión de la documentación y la información en las organizaciones

a) Adecuado soporte para la gestión y toma de decisiones, facilita el ingreso al contexto de la internacionalización de los intercambios comerciales.
b) No Incrementa la productividad y la competitividad
c) Es independiente de la tecnología de la información y las comunicaciones
d) Es dependiente de la tecnología de la información y las comunicaciones

9. De las siguientes afirmaciones acerca de Libertad Informática: Señale cuáles son verdaderas (V) o falsas (F):
   i. La creación de nuevas tecnologías de la informática, de las telecomunicaciones y de la telemática crean nuevos espacios que requieren ser regulados por el derecho. ( )
   ii. El PeCERT es el organismo encargado de coordinar emergencias en redes teleinformáticas. ( )
   iii. Existe una ley peruana de protección de datos personales. ( )
   iv. La Agenda Digital Peruana establece lineamientos que posibiliten el acceso a las personas a las ventajas que se derivan del desarrollo de las comunicaciones. ( )

   a) VFVF b) VVVV C) FFFF D)VVFF

10.¿Cuáles son los tipos de datos personales?

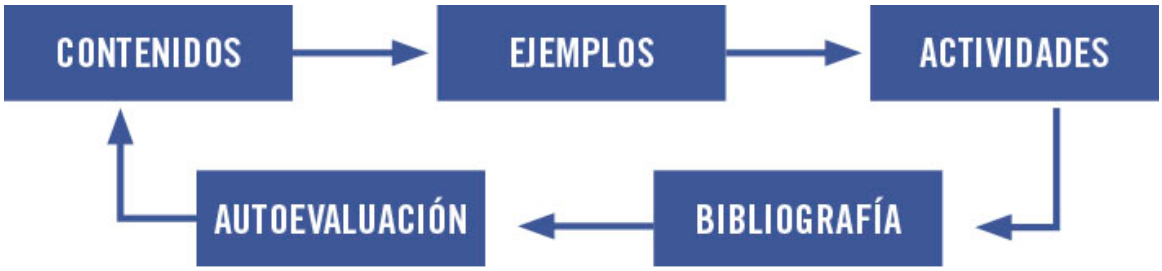
a) Datos lineales y sensibles.
b) Datos públicos y privados.
c) Datos cognitivos y fundamentales.
d) Datos pasivos y activos.

ANEXO Nº 1
Respuestas de la Autoevaluación de la Unidad I

Número	Respuesta
1	C
2	A
3	A
4	C
5	B
6	A
7	B
8	A
9	B
10	B

UNIDAD II: El gobierno electrónico y la regulación jurídica de la información

DIAGRAMA DE ORGANIZACIÓN DE LA UNIDAD II



ORGANIZACIÓN DE LOS APRENDIZAJES

Resultado de aprendizaje de la Unidad II:

Al finalizar la unidad, el estudiante será capaz de elaborar una monografía del avance de la implementación del Gobierno electrónico a través del ONGEI, la Ley de protección de datos personales, demostrando dominio teórico adecuado.

CONOCIMIENTOS	HABILIDADES	ACTITUDES
• **Tema N° 1:** Conceptos de Gobierno electrónico y Ciberjusticia. 1. Gobierno electrónico 2. Gobierno electrónico en el Perú 3. Ciberjusticia • **Tema N° 2:** Protección Jurídica de los datos personales	1. Analizar el Gobierno Electrónico en el Perú 2. Indagar la jurisprudencia administrativa y judicial del Perú en materia de protección de datos. 3. Reconocer la información jurídica del flujo internacional de datos	• Asume una actitud reflexiva sobre la implementación del Gobierno Electrónico en el Perú, la ley de protección de datos personales y la propiedad intelec-

1. Protección Jurídica de los datos personales • **Tema N° 3:** Flujo de datos transfronterizos, regulación jurídica de internet. 1. Flujo de datos transfronterizos Informática Jurídica 2. Regulación jurídica de internet • **Tema N° 4:** El derecho a la propiedad intelectual y las TICs **1.** El derecho a la propiedad intelectual y las TICs. **Lecturas seleccionadas:** • Estrategia Nacional de Gobierno Electrónico - Visión y Objetivo General • El Precio de los Datos Personales: La Regulación de la Ley No. 29733 • Insider Trading o tráfico con información privilegiada • Dominios y cómo registrarlos **Autoevaluación de la Unidad II**	4. Analizar las normas que regulan el derecho a la propiedad intelectual. 5. Valorar las nuevas TIC's con relación a la jurisprudencia reinante. **Actividades Propuestas** • Los estudiantes Participan en el Foro de discusión sobre El gobierno electrónico • Los estudiantes Participan en el Foro de discusión sobre protección de datos personales. • Los estudiantes Participan en el Foro de discusión sobre el Flujo de datos transfronterizos, regulación jurídica de internet. • Los estudiantes Participan en el Foro del derecho a la propiedad intelectual y las TICs **Control de lectura y/o tarea académica** Los alumnos deberán concluir las asignaciones de cada uno de los temas de esta unidad.	tual.

TEMA N° 1: Conceptos de Gobierno electrónico y Ciberjusticia

El gobierno electrónico en los últimos años ha permitido a los gobiernos de muchos países orientar esfuerzos en aras de lograr una mejor comunicación con los ciudadanos y brindar mejores servicios que permiten un desarrollo sostenible y progresivo en los aspectos económicos, sociales y culturales a través de impulsar la cooperación.

1. **Gobierno electrónico:**

1.1. **Conceptos**

- Peter Drucker, define, "electronic government, e-government o simplemente, e-gov como una herramienta novedosa para garantizar la viabilidad del proceso de reforma. Pero la noción de gobierno electrónico implica la revisión de un conjunto de definiciones y de hechos históricos, indispensables para la comprensión del mismo." (Drucker, 1989, Pág. 254)

- "Es una innovación continua de los servicios, la participación de los ciudadanos y la forma de gobernar mediante la transformación de las relaciones externas e internas a través de la tecnología, el In-

ternet y los nuevos medios de comunicación." (Gartner Group, 2016)

- Pablo Castoldi, considera que el gobierno electrónico contempla las actividades que tienen fundamento en las tecnologías de la información modernas; esto considerando las aplicaciones conctadas con Internet que se utilizan para poder mejorar el servicio que las instituciones públicas brindan a los ciudadanos y de este modo pueden brindar una atención más eficiente y transparente.

- Fernando Ocampo habla sobre el gobierno electrónico como "un esquema de gestión pública basado en la utilización de la tecnología de la información y de las comunicaciones, teniendo como objetivos mediatos optimizar la gestión pública y desarrollar un enfoque de gobierno centrado en el ciudadano." (Ocampo, 2003, Pág. 22).

- "Es el uso de las tecnologías de la información y comunicación (TIC's), particularmente la Internet, como una herramienta para alcanzar un mejor gobierno". (OCDE, 2016)

- "Se refiere al uso de tecnologías de información por parte de las agencias gubernamentales que tienen la habilidad de transformar las relaciones entre los ciudadanos, los negocios y otros brazos del gobierno." (BANCO MUNDIAL, 2013)

- Con respecto a la incorporación de innovaciones tecnológicas al aparato estatal, se debe afirmar que esto constituye "un esquema de gestión pública basado en la utilización de tecnología de la información y de las comunicaciones, teniendo como objetivos mediatos optimizar la gestión pública y desarrollar un enfoque de gobierno centrado en el ciudadano." (Ocampo, 2003. Pág. 23.)

El gobierno electrónico, es por tanto, un modelo de gestión que combina la utilización de las TIC para lograr gestión, planificación y administración, como una nueva forma de gobierno en la administración pública, contribuyendo al uso de las tecnología de la información y de las comunicaciones con la finalidad de brindar mejor información y servicios que se ofrecen a las organizaciones y los ciudadanos; del mismo modo, esto se hace con la finalidad de simplificar y mejorar los procesos de las instituciones y también poder ofrecer alternativas que aumente la participación ciudadana y la transparencia. A continuación veremos algunas cuestiones con respecto a la forma del gobierno electrónico que nos brinda la ONGEI.

1.2. Distribución del Gobierno electrónico

El gobierno electrónico está distribuido en los siguientes rubros según lo establecido por la (ONGEI, 2016):

1.2.1. E-administración (administración electrónica)

Es la utilización de las tecnologías de la información que faciliten la prestación de servicios por parte de la administración estatal para las empresas y los ciudadanos.

1.2.2. E- democracia (democracia electrónica)

Por medio de este tipo de gobierno, se logra la participación ciudadana en los procesos electorales y participación política de los ciudadanos al hacer uso de las tecnologías de la información.

1.2.3. E- gobierno (gobierno electrónico en sentido estricto)

El E-gobierno hace uso de las tecnologías de la información y las telecomunicaciones para administrar el país considerando aspectos simples como las publicaciones de documentos en línea, así como la integración de todos los organismos estatales. Este concepto incluye los anteriores.

1.3. Tipologías de Gobierno Electrónico

Así también, existen algunas tipologías para el Gobierno Electrónico formadas respecto a la relación del Gobierno con otros actores, es decir, a sus interacciones.

1.3.1. De Gobierno a Gobierno (G2G)

Se pueden identificar todas las iniciativas y acciones de Gobierno Electrónico destinadas a generar y facilitar las relaciones intragubernamentales e intergubernamentales. En el Perú, el Sistema Integrado de Administración Financiera (SIAF) Es un ejemplo claro de esto.

1.3.2. De Gobierno a empresa (G2B)

Se cuentan con iniciativas de Gobierno Electrónico que tienen por finalidad brindar, por medio de las TIC, servicios públicos y de información específicamente dirigidos a empresas. Para el Perú, por ejemplo, tenemos el portal del Sistema Electrónico de Adquisiciones y Compras del Estado (SEACE).

1.3.3. De Gobierno a ciudadano / usuario (G2C)

Se muestran iniciativas de Gobierno Electrónico destinadas a ofrecer servicios administrativos o de gobierno, información pública y nuevos canales de conexión a los ciudadanos. Por ejemplo en el Perú, el Portal de Servicios al Ciudadano y Empresas (PSCE).

1.3.4. De Gobierno a empleados (G2E)

Existen iniciativas cuyo objetivo es prestar servicios o capacitar con el uso de las TIC a los empleados, agentes o funcionarios de la Administración Pública. Por ejemplo en el Perú, los cursos virtuales impartidos por la Escuela Nacional del Servicio Civil (SERVIR).

1.4. Etapas del Gobierno Electrónico

En el Gobierno Electrónico también se pueden determinar etapas están relacionadas con el nivel de presencia en la web de las entidades del Estado:

1.4.1. Presencia

Se pone en línea información de los distintos organismos del Estado. Por ejemplo: leyes, servicios, etc.

1.4.2. Interacción

Se abre un espacio de comunicación de los ciudadanos y empresas con los organismos públicos. Por ejemplo, los portales web del Estado con servicio de consulta vía chat institucional como los proporcionados por la Defensoría del Pueblo, o RENIEC, entre otros o por uso de redes sociales.

1.4.3. Transacción

Se puede realizar trámites en línea. Por ejemplo, con la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT), el Servicio de Administración Tributaria (SAT), el Banco de la Nación, el RENIEC, etc.

1.4.4. Transformación

Se establece un nuevo patrón de relación con el ciudadano y una nueva forma de operar de los organismos públicos. Por ejemplo, la Plataforma de Interoperabilidad del Estado (PIDE).

1.4.5. Integración

Se realiza la integración de ciudadanos, organizaciones, empresas, y otras instituciones gubernamentales. Esto permite que el gobierno y el pueblo puedan dialogar bidireccionalmente para tomar decisiones de manera correcta.

1.5. Los beneficios de la tecnología y del Gobierno

Los beneficios que brinda el Gobierno Electrónico son diversos, ya que permite fortalecer y mejorar la gestión pública para el estado y para los ciudadanos.

1.5.1. Para el Estado

- Permite mejorar los procesos de gestión internos.
- Mejora la comunicación y coordinación intrainstitucional e interinstitucional.
- Genera espacios de trabajo colaborativo para brindar servicios.
- En el plano de las políticas públicas, replantea el proceso de diseño, al tomar en cuenta, como nuevo como ponente, a las TIC.
- Fortalece la innovación y modernización del Estado.
- Mejora los procesos de formación y de desarrollo de capacidades.

1.5.2. Para los ciudadanos

- Permite obtener mejores servicios del Estado, con reducción de tiempo y de costos.
- Permite fortalecer la transparencia de las entidades públicas.
- Mejora la participación ciudadana al brindar nuevos espacios de diálogo horizontal, fomenta el control ciudadano (accountability) y, por ende, contribuye a la gobernabilidad.
-

1.5.3. Para las empresas

Les permite establecer relaciones comerciales con el Estado con mayor transparencia.

Agiliza los procesos de los trámites tradicionales sustituyéndolos por trámites en línea

2. El gobierno electrónico en el Perú

Según la Ley N° 29904 se crea la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI). Esta organización es la encargada de crear las diversas políticas de gestion del gobierno electrónico en el Perú; también son los encargados de la creación del Plan Nacional de Gobierno Electrónico en un corte de tiempo así como una serie de indicadores que miden el Gobierno Electrónico y su desarrollo. Esta oficina es la encargada también de administrar el Sistema Nacional de Informática y ejecutar la implementación de la Política Nacional de Gobierno Electrónico. A continuación se hará referencia a parte de lo mencionado en el Plan nacional de gobierno electrónico 2013 - 2017 desarrollado por la (ONGEI, 2016) con respecto al gobierno electrónico en el Perú:

2.1. Lineamientos Estratégicos

"Basándose en los criterios de evaluación de estándares para definir el nivel de desarrollo de Gobierno Electrónico de un país, las tendencias de las TIC en los próximos años, las estrategias y planes de las diferentes entidades del Estado Peruano y las consultas realizadas a la población del interior del país referente a los servicios que las entidades del Estado brinda, se han establecido los siguientes lineamientos estratégicos para Gobierno Electrónico en el Perú" (ONGEI, 2016, p. 14):

2.1.1. Transparencia

"Promover el conocimiento de la gestión del Estado a través de nuevos canales que permitan la participación del ciudadano en las funciones públicas con información confiable, oportuna y accesible. La transparencia generará mayor visibilidad de los asuntos del estado." (ONGEI, 2016, p. 14).

2.1.2. e-Inclusión

"Incluir a todos los ciudadanos sin distinción de origen, credo, idioma, sexo, edad u otra variable de exclusión a la Sociedad de la Información y del Conocimiento (SIC) a través de proyectos y programas de Alfabetización Digital que permitan el fortalecimiento de las capacidades de los ciudadanos." (ONGEI, 2016, p. 14)

2.1.3. e-Participación

"Generar la participación activa del ciudadano a través de su Identidad Digital en la gestión pública a través de plataformas de internet como redes sociales, foros, chats en línea u otras formas de interacción a fin de satisfacer eficientemente necesidades de información, control y consultas públicas en nuevas Políticas de Estado." (ONGEI, 2016, p. 15).

2.1.4. e-Servicios

"Habilitar los medios electrónicos necesarios al ciudadano para que pueda acceder a los servicios públicos por medios electrónicos seguros, a través del uso de su identidad digital, con seguridad, comodidad y satisfacción desde cualquier lugar. E-Servicios necesita de un rediseño de los procesos en las entidades del Estado, así como el aseguramiento de estándares tecnológicos en interoperabilidad (web services). Adicionalmente, se requiere construir una plataforma tecnológica intergubernamental que facilite los servicios, trámites y consultas del ciudadano. Finalmente, se necesita apoyar las iniciativas de identidad digi-

tal, firmas y certificados digitales, mecanismo de seguridad para la privacidad y protección de los datos en general y datos personales en particular.” (ONGEI, 2016, p. 15)

2.1.5. Tecnología e Innovación

“Se debe promover el crecimiento de la Tecnología e Innovación a través de la provisión de una infraestructura adecuada a través del desarrollo de plataformas que permitan llevar a cabo innovaciones impulsando la cultura emprendedora y, al mismo tiempo, dando respuesta a problemáticas sociales concretas.” (ONGEI, 2016, p. 15).

2.1.6. Seguridad de la Información

“El paradigma de todo a disposición de todos debe manejarse de la manera más cuidadosa, velando por la integridad, seguridad y disponibilidad de los datos, para ello se debe establecer lineamientos en seguridad de la información a fin de mitigar el riesgo de exposición de información sensible del ciudadano.” (ONGEI, 2016, p. 15).

2.1.7. Infraestructura

“El requisito fundamental para la comunicación efectiva y la colaboración dentro del Estado es contar con una red informática y de telecomunicaciones que integre a todas las dependencias y a sus funcionarios públicos, incluyendo hardware, software, sistemas, redes, conectividad a la Internet, bases de datos, infraestructura para capacitación en línea (e-Learning) y recursos humanos especializados. Asimismo, compartirá recursos metodológicos, de infraestructura y de conocimiento entre los servidores públicos con el objetivo de compartir buenas prácticas para mejorar su aprovechamiento y evitar duplicidades.” (ONGEI, 2016, p. 15)

Gráfico 1: Distribución del gobierno electrónico
Fuente: ONGEI. (2012). Plan nacional de gobierno electrónico 2013 -2017. p. 16
http://www2.pcm.gob.pe/clip/PLAN%20NACIONAL%20DE%20GOBIERNO%20ELECTRONICO.pdf

2.2. Objetivos Estratégicos

"Tomando como base los lineamientos estratégicos: Transparencia, e-Inclusión, e-Participación, e-Servicios, Tecnología e Innovación, Infraestructura y Seguridad de la Información, los objetivos de la Agenda Digital Peruana 2.0, la Estrategia Nacional 2006, el Plan Bicentenario y el Master Plan Perú - Corea 2011, se han establecido los siguientes objetivos estratégicos a fin de garantizar el crecimiento del Perú de cara al 2017 respecto a gobierno electrónico" (ONGEI, 2016, p. 16):

OE1: Lograr el desarrollo y la prestación de mejores servicios TIC para la sociedad, a través de la Interoperabilidad entre las entidades del Estado, el sector privado y la sociedad civil.
OE2: Acercar el Estado al ciudadano a través de mecanismos que aseguren el acceso oportuno e inclusivo a la información y una participación ciudadana como medio para aportar a la gobernabilidad y transparencia de la gestión del Estado.
OE3: Garantizar la integridad, confidencialidad y disponibilidad de la información pública mediante mecanismos de seguridad de la información gestionada.
OE4: Fomentar la inclusión digital de todos los ciudadanos, especialmente a los sectores vulnerables, a través de la generación de capacidades y promoción de la innovación tecnológica, respetando la diversidad cultural y el medio ambiente.
OE5: Proponer y adecuar el marco legal, a fin de asegurar su cumplimiento para el despliegue del Gobierno Electrónico en el

marco del desarrollo de la Sociedad de la Información (ONGEI, 2016, p. 16).

Gráfico 2: Objetivos del Plan Nacional de Gobierno Electrónico en el Peru
Fuente: ONGEI. (2012). Plan nacional de gobierno electrónico 2013 -2017. p. 16
http://www2.pcm.gob.pe/clip/PLAN%20NACIONAL%20DE%20GOBIERNO%20ELECTRONICO.pdf

3. **Ciberjusticia**

La Ciberjusticia es la forma en cómo se imparte justicia desde los sitios virtuales. Ésta es emitida a través de tribunales virtuales especializados que sirven como mediadores de litigios originados por el uso del Internet en operaciones como (propiedad intelectual, comercio electrónico, derecho a la privacidad, entre otros). Estos brindan a ambas partes la elección del lugar donde podrán obtener una solución a u conflicto.

3.1. **Cibertribunales**

Los cibertribunales están basados en la forma en cómo se aplican las leyes de un país por medio del uso de las TICs para la resolución de conflictos referidos a comercio electrónico, autoría, y otros problemas similares. Debido a los conflictos existentes en internet, existen diversas alternativas de solución como la mediación, el arbitraje yla conciliación; por supuesto, todos estos presentan diversos beneficios considerables y ventajas ante los sistemas tradicionales. Algunos de sus principales beneficios son:

- Las partes tienen autonomía de voluntad.
- Las partes pueden elegir un árbitro o conciliador que sea neutro en cualquier país.
- Es posible usar infraestructuras y tecnologías modernas (data-mining, webrobots, sistemas multiagentes, etc.).
- Existe flexibilidad y celeridad en los Procesos extrajudiciales mientras se mantienen los derechos de ambas partes).
- Posibilidad de solución de conflictos en línea a través de discusión y labor en tiempo real.
- No se puede dar una apelación, por lo tanto, no se pueden prolongar los procesos.

- Luego del proceso, se puede respetar la confidencialidad y privacidad.
- Permite una reducción considerable, en las pates, del factor emocional que puede ser hostil.
- Permite la participación de expertos para evaluar, dictaminar y apoyar en los casos. Esto es posible por el uso de las TICs.
- Permite la validez del laudo dictaminado en otros países por medio de tratados internacionales.

3.2. Primeras experiencias

Entre las experiencias de los cibertribunales, se deben tener en cuenta los siguientes ejemplos recopilados por (Tellez, 2008):

3.2.1. VirtualMagistrate

"En marzo de 1996 se inauguró el proyecto VirtualMagistrate, un servicio de arbitraje en línea resultante de la colaboración entre el Cyberspace Law Institute (CLI) y el National Center for Automated Information Research (NCAIR). El objetivo primordial del proyecto era estudiar la manera de resolver las diferencias entre un usuario y un operador de redes, o entre usuarios. El ámbito de aplicación del proyecto se limitaba a los conflictos generados por mensajes o ficheros con contenido ilícito". (Tellez, 2008, p. 43).

3.2.2. Online Ombuds Office

"El proyecto Online Ombuds Office (Oficina de mediadores en línea) es una iniciativa del Center for Information Technology and Dispute Resolution de la Universidad de Massachusetts. Desde 1996 este organismo ofrece servicios de mediación para determinados conflictos que se generan en Internet, en particular, los litigios entre miembros de un grupo de debate, entre competidores, entre proveedores de acceso Internet y sus abonados, así como los relacionados con la propiedad intelectual. El proyecto se prosigue en la actualidad." (Tellez, 2008, p. 44).

3.2.3. CyberTribunal

"El CyberTribunal era un proyecto experimental elaborado por el Centre de Recherche en Droit publique (CRDP) de la Universidad de Montreal, en septiembre de 1996. El proyecto apuntaba a determinar si era viable utilizar mecanismos alternativos para resolver conflictos generados en entornos electrónicos mediante la mediación. Fue mucho más amplio que el Virtual Magistrate y Online Ombuds Office." (Tellez, 2008, p. 44)

3.3. Ejemplos más recientes

(Tellez,2008) hace una recopilación de los casos más recientes y exitosos:

3.3.1. SquareTrade

"SquareTrade fundado en otoño de 1999, funciona casi exclusivamente en el sector del comercio electrónico entre consumidores (C2C). La sociedad estadounidense ofrece dos posibles servicios de solución de diferencias: la negociación directa y la mediación. Su asociación con eBay, uno de los más importantes sitios de subastas en el ciberespacio, ha generado rápidamente un importante volumen de casos." (Tellez, 2008, p. 44).

3.3.2. eResolution

"eResolution fue fundada en el otoño de 1999, inauguró su primer servicio de solución en línea de diferencias el 1º de enero de 2000, en el momento en que recibía la acreditación de la Corporación Internet para Nombres y Números Asignados (ICANN) para administrar la solución de conflictos relativos a nombres de dominio, de conformidad con su política. La plataforma tecnológica de eResolution ha permitido resolver de esta manera varios cientos de asuntos, con alcance mundial." (Tellez, 2008, p. 44)

3.4. Requisitos formales y arbitraje en línea

Por la naturaleza del arbitraje en línea surgen diversas cuestiones a considerar.

3.4.1. Primera cuestión

Un acuerdo de arbitraje llevado a cabo por medio electrónicos es la primera cuestión sobre validez que se plantea. Esto tiene que ver con las formalidades propias de este suceso en los ámbitos nacionales e internacionales, y como estas tienen que ver con la prueba de alguna clausula compromisoria o algún tipo de compromiso. En palabras simples, se pone en duda la validez de los acuerdos que se llevan a cabo por el internet. Por lo tanto es necesaria una interpretación que no sea rígida para que los su validez siga constante con respecto a los textos físicos.

3.4.2. Segunda cuestión

En segundo lugar, se debe considerar el tema de las notificaciones documentarias. Por supuesto, esto representa un obstáculo nada significativo pen comparación de los beneficios de tener procesos arbitrales informatizados. Originalmente, se puede constatar que si las partes están de acuerdo, no habría inconveniente en la notificación electrónica.

3.4.3. Tercera cuestión

Se debe considerar también, la instrucción de la causa. Considerando como puntos clave, la audiencia donde se tiene la causa testimonial y donde se desarrolla el arbitraje. Por este motivo, son las videoconferencias una solución práctica para el problema de los arbitrajes que traspasan fronteras.

3.4.4. Cuarta cuestión

Por último, se debe considerar también la sentencia y su dictamen. Esto se relaciona más con el compromiso que asumen las partes antes de dictaminarse la sentencia. Por otro lado, es un problema también las firmas que deben aparecer en la sentencia; Por lo cual se requiere una interpretación de tipo flexible ara que no sea desestimado su valor; este tema está siendo resuelto con la ayuda de los certificados y las firmas digitales.

3.5. Arbitraje y comercio electrónico

Con respecto a la administración de justicia, sobre el comercio electrónico, es el arbitraje la solución más inmediata y posible cuando se presentan conflictos relacionados con el comercio electrónico entre fuera de un país, y además, este tipo de administración de justicia, de alguna manera equilibra los costos de justicia ara las partes. Por supuesto, estas normas aplicadas en este tipo de litigios, no son exactamente las que se aplican en un sistema jurídico de específico de un solo país.

3.6. Arbitraje de los Asuntos de Propiedad Intelectual

En el caso de la protección material intelectual, se ha llegado a la conclusión que los litigios suscitados por este tipo de conflictos deben ser de tipo arbitral. Por supuesto esto se debe hacer partiendo de la premisa que existe entre las partes un vínculo contractual por medio de una cláusula que los comprometa. Este es el medio por el cual se deben resolver este tipo de conflictos.

3.7. Centro de Arbitraje y Mediación de la OMPI

El centro de Arbitraje y Mediación de la OMPI fue creado en 1994 y como sede a Ginebra, Suiza. Este centro ofrece servicios de mediación y arbitraje derivados de conflictos comerciales que ocurren cuando las partes son de carácter privado teniendo procedimientos diseñados por expertos en el tema para resolver controversias originadas por la propiedad intelectual a nivel mundial. Por su puesto también se encarga de la solución de conflictos originados por los nombres de dominio web.

3.8. Instituto para la Resolución de Conflictos (CPR)

Este instituto fue fundado en 1979, y contribuye una alianza constituida por organismos internacionales y despachos prestigiosos que ofrecen a instituciones públicas y empresas para los procesos judiciales que son tan costosos. Está formado por socios de los mejores despachos, 500 asesores legales de las mejores empresas, instituciones públicas seleccionadas y catedráticos notables; tienen como misión integrar alternativas para resolver conflictos (ADR). Para cumplir con este cometido, el CPR está tiene un área de investigación y desarrollo integrada, abogacía, servicios de solución de conflictos y educación.

3.9. Foro de Arbitraje Nacional (NAF)

Habiendo sido fundado en Minneapolis en 1986, ha sobresalido por su neutralidad para tomar decisiones y aplicar de leyes relevantes en la resolución de casos arbitrales. En los últimos días, el NAF ha estado en investigación por trabajar con compañías de gran tamaño, compañías de seguros, bancos y fabricantes de computadoraspuesto que requeiere a sus clientes renunciar a sus derechos legales y aceptar la autoridad de un árbitro para resolver controversias. Esto, debido a que argumentan el NAF favorece a aquellas compañías que tengan mayor solvencia económica. Se logró la aprobación de los servicio de la NAF en 1999.

3.10. Cibercorte de Michigan

El 2002 se firmó un decreto que establecía una “cibercorte.” Esto lo llevo a cabo Jhon Engler, gobernador de Michigan en este entonces, con la finalidad de resolver los conflictos relacionados con alta tecnología, donde muchos procesos se pueden resolver con una computadora y en línea en lugar de hacerlo de forma presencial en un tribunal. Esto

destaca que los abogados, no necesitaban estar in situ, ni necesitaban una licencia de litigación del estado porque los jueces tienen dominio de tiempo y conocimiento en:

- LOS INFORMES, en línea, "online".
- LA EVIDENCIA, por video.
- LOS ALEGATOS ORALES, con teleconferencias.
- LAS CONFERENCIAS, a través de e-mail.

3.11. Directiva Europea

El artículo 17 de Directiva Europea sobre Comercio Electrónico hace referencia a la solución extrajudicial de litigios y dispone en su apartado primero que los Estados miembros velarán por que, en caso de desacuerdo entre un prestador de servicios de la sociedad de la información y el destinatario de aquellos, su legislación permitirá utilizar de manera efectiva mecanismos de solución extrajudicial, incluso mediante vías electrónicas adecuadas. Este tipo de mecanismos parece en particular útil para determinados litigios en internet, en especial para los de grandes cantidades y de acuerdo con la envergadura de las partes, que pueden renunciar a emplear los procedimientos judiciales debido a sus costos.

3.12. Cibertribunal de Lieja (Bélgica)

Proyecto propuesto a la Fundación Rey Baudouin a finales de 2000, a iniciativa de la barra de abogados de dicha ciudad (programa "Justicia en movimiento") y dentro de los programas pilotos de "E-Justice de la Unión Europea", apoyado por el ministerio de Justicia, que pretende establecer un "cibernexo" entre 800 abogados barristas y los órganos jurisdiccionales (inicialmente está considerada la materia laboral) para intercambiar información entre ambas instancias permitiendo la gestión de litigios por este medio. El proyecto es desarrollado por las facultades de Derecho de Lieja y Namur dentro del rubro Procedimientos y Nueva Tecnologías.

3.13. El Cibertribunal Peruano

El Cibertribunal Peruano dio inicio como iniciativa del Instituto Peruano de Comercio Electrónico, cuyos antecedentes datan del Proyecto americano "Magistrado virtual del Centro Villanova para Derecho Informático y Política". Esta es una organización de resolución controversias de conflictos que derivan de la utilización de las TICs, haciendo uso del arbitraje y conciliación. Su objetivo es ser un ser centro para la prevención y resolución de conflictos en países hispanos. Se justifica su existencia por medio del número de usuarios que tiene.

3.13.1. Funciones del Cibertribunal peruano

Entre Las funciones del Cibertribunal Preruano tenemos:

- Mantener al día el registro de árbitros y conciliadores.
- Establecer los árbitros y conciliadores para un proceso en particular.
- Dar asesoría y ayudar a los usuarios en interntet que tengan dudas sobre el Cibertribunal peruano.
- Desarrollar convenios y propuestas legislativas con respecto al derecho informático y en temas relacionados al uso de las TICs.

- Solicitar legislación o jurisprudencia actual a entidades adecuadas a fin de aplicarlas en cada caso como parte de sus funciones.
- Promover el uso de la conciliación y el arbitraje para resolver conflictos surgidos por el uso de las TICs.

TEMA N° 2: Protección Jurídica de los datos personales

En la actualidad el tema de datos personales de formato virtual se ha convertido en un posible foco de problemas para el derecho. Esto debido al acceso que puedan tener personas sin escrupulos que deseen hacer uso ilegal de estos para lucrar con ellos o simplemente utilizarlos con otros fines perjudiciales. Es por este motivo que se debe conocer la regulación en cuanto su protección y manejo.

1. **Conceptos jurídicos tradicionales: ¿Intimidad, Privacidad o Vida Privada?**

1.1. **El concepto de intimidad:**

El concepto de intimidad tiene origen latino, y tiene como raíz la palabra *intimus*. De la misma palabra también derivan: *intimus consillis eorum* (confidentes de sus secretos) y *amici intimi* (amigos íntimos).

"De ello se desprende que el significado de esta palabra haga alusión a lo íntimo, secreto, recóndito, profundo, propio." (García, 1988, pág. 17).

Esta palabra se usa en países que no son de habla hispana porque se encuentra también incluida en otros idiomas.

- En italiano: intimitá.
- En inglés: intimity.
- En alemán: intimität.
- En francés: intimité.
- En español: intimidad.

1.2. **Otros conceptos**

- Adriano de Cupis nos dice que intimidad es, "la necesidad consistente en la exigencia de aislamiento moral, de no comunicación externa, de cuanto concierne a la persona individual". (García, 1988, pág. 19)

- Miguel Bajo Fernández la considera como "ese ámbito personal donde cada uno, preservado del mundo exterior, encuentra las posibilidades de desarrollo y fomento de su personalidad. Se trata pues, de un ámbito personal reservado a la curiosidad pública, absolutamente necesario para el desarrollo humano y donde enraíza la personalidad". (García, 1988, pág. 19)

- Núñez Ponce J. define el derecho a la intimidad como, "el derecho que compete a toda persona a tener una esfera reservada en la cual desenvolver su vida sin que la indiscreción ajena tenga acceso a ella". (Núñez, 2001, pág. 67).

- García San Miguel L. nos dice que, "definamos como definamos la intimidad, casi todos admitirán que este derecho tiene que ver con la posibilidad de que algo de lo que hacemos o lo que somos (sean

cuales sean los confines de ese algo) no sea conocido por los demás y, si fuera conocido por algunos, éstos no lo den a conocer a otros." (Cuervo, 2001, pág. 33).

1.3. **El concepto de privacidad:**

- Es "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". (RAE, 2016).

- "privado", que en sus diferentes acepciones significa "que se ejecute a vista de pocos, familiar o domésticamente, sin formalidad ni ceremonia alguna" y "particular y personal de cada uno". (RAE, 2016).

- Tambien podemos observar que, "El derecho de los individuos, grupos o instituciones a determinar por sí mismos, cuando, cómo y hasta qué punto se puede comunicar a terceras personas información referida a ellos".(Casacuberta, 1999, pág. 12)

- la privacidad es, "más que un mero sentido estático de la defensa de la vida privada del conocimiento ajeno, tienen una función dinámica de posibilidad de controlar la circulación de informaciones relevantes para cada sujeto". (Ortúzar, 1996, pág. 27).

1.4. **Concepto de DATO:**

Esta palabra se origina etimológicamente del latín *«Datum»* que significa "lo dado".

- "La mayoría de los autores asumen que el investigador desempeña un papel activo respecto de los datos: el dato es el resultado de un proceso de elaboración, es decir, el dato hay que construirlo". (Gil, 1994, Cap. 1).

- Johan Galtung define el término "dato": "Se obtienen datos sociológicos cuando un sociólogo registra hechos acerca de algún sector de la realidad social o recibe hechos registrados para él". (Galtung, 1966, pág. 14).

- "Son un el conjunto básico de hechos referentes a una persona, cosa o transacción. Incluyen cosas como: tamaño, cantidad, descripción, volumen, tasa, nombre o lugar." (Murdick, 2005, pág 157).

- Así también, a cada conjunto de datos se le necesita añadir un valor añadido para ser de utilidad:

    - Se evalúa y analiza su contenido,
    - Se manipula, agrega, y organizada su forma,
    - Se le da un contexto que comprenda un usuario humano.

- Por lo tanto, los datos son el ingrediente en bruto, para obtener información.

- El proceso para la recolección de datos, puede suceder ante una transacción interna o de un evento externo a la compañía.

- Validación (Verificación): Con la finalidad de reducir el número de errores los datos son verificados y corregidos luego de su obtención.

- Almacenamiento: consiste en guardar los datos previamente capturados en un medio de almacenamiento como: disco duro cd, dvd, etc.

- Recuperación: proceso mediante el cual se logra acceder, escoger y extraer datos almacenados.

- Reproducción: Duplicación de los datos o información para el traslado de los mismos de un lugar a otro.

1.5. El derecho a la protección de datos personales

Desde 1968, la Asamblea de los Derechos Humanos expresaba una verídica preocupación de como las TICs podían generar alteraciones en los derechos universales de las personas; a partir de esto, se esbozó un régimen jurídico capaz de afrontar de forma correcta los cambio que esto representaba.

A partir del desarrollo tecnológico que significó la creación de sistemas de información que lograron procesar, transmitir y relacionar información en cuestión de fracciones de segundos a fines de la década de 1960 se originó el derecho a la protección de datos personales. Esto significo el fin de los límites temporales y espaciales para la información que se podía almacenar y utilizar. Hoy en día gracias a estos avance, se puede almacenar información de forma permanente tanto así que, “los recursos tecnológicos no conocen el olvido, ni se detienen ante la lejanía y son capaces de almacenar, relacionar y comunicar en tiempo real ingentes masas de datos de todo tipo, incluidos los de carácter personal y de utilizarlos para las más diversas finalidades” (Castro K, 2008, pág. 36).

“Los recursos tecnológicos no conocen el olvido, ni se detienen ante la lejanía y son capaces de almacenar, relacionar y comunicar en tiempo real ingentes masas de datos de todo tipo, incluidos los de carácter personal y de utilizarlos para las más diversas finalidades”. (Murillo, 2005, pág. 33). Resulta innegable que las tecnologías informáticas han aportado diversos beneficios a la sociedad y que hoy están presentes en casi todas las actividades de nuestra vida. (Serrano, 2003. p. 18).

Debido a la gran capacidad para almacenar información, son los datos personales también parte de este grupo y que tienen un carácter íntimo que debe protegerse por la naturaleza de proceso y transmisión de esta información. Por lo tanto, existe la posibilidad que esta información combinada con otros conjuntos de datos, desvelen rasgos únicos de las personas que puedan dañar su integridad y dignidad afectando sus derechos básicos. Existe por lo tanto una responsabilidad sobre aquellos que recolectan y procesan esta información y se debe garantizar un uso adecuado de la misma.

De esto se desprende que la posesión, manipulación y transmisión sin control de esta información particular y única, genera una manera de controlar a la sociedad que se denomina “poder informático.” De ahí se

debe regular de manera adecuada la información para poder tener control de este poder.

Ahora bien, si partimos de este punto debemos considerar la información como uno de los activos más importantes de toda empresa, y al mismo tiempo lo hace también uno de los más deseables por la competencia u otros agentes que anhelan tenerla. Es por eso que la tutela de la información es vital en el derecho como lo estipula la Constitución Política.

Entre los derechos de protección de datos personales a nivel mundial destacan algunos conceptos relevantes:

1.5.1. Derecho de acceso

Este derecho da facultad a los interesados de solicitar a las instituciones la información y el tipo de información que posean sobre él.

1.5.2. Derecho de rectificación

Por medio de este derecho una persona puede solicitar, habiendo conocido que información se tenga de sí, la modificación, alteración y eliminación de la información que considere irrelevante o inexacta.

1.5.3. Derecho de uso conforme al fin

Este derecho permite a una persona exija que su información solo sea utilizada para los fines para los cuales la proveyó. Por ejemplo, si alguien brinda información para un trámite administrativo, dicha información solo debe ser usar para ese fin.

1.5.4. Derecho para la prohibición de interconexión de archivos.

Este derecho permite al usuario solicitar que su información se guarde en completa reserva y no sea difundida fuera de los alcances de fin para que la dio y no sea comercializada o difundida fuera de los milites de este entorno.

1.6. Los datos personales y los datos sensibles:

- **Dato personal**:
  Se denomina dato personal a toda clase de información de tipo fisiológico o legal que identifica a una persona.

  Ejemplos:

  - El registro de voz que alguien grabe puede ser considerado un dato personal tanto como este sirva para identificarlo.
  - Las huellas dactilares, creencias políticas, dirección, números de seguro, entre otros.
  - Las fotos o imágenes de video que son capturadas por cámaras de video de vigilancia en instituciones del estado o privadas porque permiten la identificación de las personas.

- **Dato sensible:**
  La los datos sensibles permiten reconocer rasgos específicos y bien definidos que son parte del, “núcleo de la personalidad y dignidad humanas.” (Murillo de la Cueva, 2009, pág. 69).

Entre estos datos destacan:

- Datos referidos a la ideología.
- Preferencias sexuales.
- Religión o creencias.
- Origen étnico.
- Información relacionada a la salud.

Para calificar a un dato personal como sensible, se debe considerar que divulgar o comunicar esta información a terceros podría ser motivo de discriminación o segregación de algún tipo. Por lo tanto, "todos aquellos datos personales que por sus connotaciones en el medio social, tengan, en el caso concreto, la aptitud de generar (...) actitudes o conductas de carácter discriminatorio" (Peyrano, 2002, pág. 22) son considerados datos sensibles.

1.7. Ley Nº 29733

Como loe que contempla la protección de datos personales, es necesario considerar la ley peruana en este tema. Por lo tanto, se citarán los puntos más esenciales de la (Ley N° 29733, 2013)

- Según la Constitución Política del Perú en su artículo 2do, numeral 6 leemos que "toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten a la intimidad personal y familiar." (Constitución Política del Perú, 1993).

- El 7 de junio de 2010 se aprobó el Proyecto de Ley N° 4079/2009-PE en el Congreso de la República del Perú y esto dio inicio a la Ley de Protección de Datos Personales.

- Con fecha 3 de julio, 2011 se publicó la Ley Nº 29733 sobre la protección de datos personales en el Diario Oficial "El Peruano"

- Así también se aprobó el Reglamento de Ley N° 29733 con DECRETO SUPREMO N° 003-2013-JUS, que se publicó el 22 de marzo de 2013, el mismo que hacía mención de las disposiciones de esta ley. Esta ley tiene vigencia a partir del 8 de mayo de ese año.

- Luego, la Autoridad Nacional de Protección de Datos, el 11 de octubre de 2013, hace pública la Directiva de SI con la finalidad de dar a conocer las medidas técnicas que se aplicarían.

1.7.1. Título preliminar disposiciones generales:

- **Artículo 1. Objeto de la Ley**
  La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de

respeto de los demás derechos fundamentales que en ella se reconocen.

- **Artículo 2. Definiciones (Básicas)**

  - **Datos personales**: Información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo relativo a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

  - **Banco de Datos Personales:** Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se cree, cualquiera que fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

  - **Titular del dato:** Persona natural a la que corresponden los datos personales (propietario).

  - **Datos sensibles :** Datos de la esfera más íntima de la persona: datos biométricos; origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; características físicas, morales o emocionales; familiar; e información relacionada a la salud o a la vida sexual.

  - **Tratamiento Datos Personales:** Cualquier operación o procedimiento técnico, automatizado o no, que permita la extracción, consulta, registro, organización, almacenamiento, modificación, bloqueo, suspensión, difusión o cualquier otra forma de procesamiento de datos personales

  - **Titular del Banco de Datos Personales**: Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de éstos y las medidas de seguridad.

  - **Responsable del tratamiento:** Aquél que decide sobre el tratamiento de los datos personales.

  - **Encargado del tratamiento:** Realiza el tratamiento de los datos personales, pudiendo ser el titular, el responsable u otra persona por encargo del titular y en virtud de una relación jurídica. Incluye los que lo realizan por cuenta del responsable, cuando el tratamiento se realice sin la existencia de un banco.

- **Transmisión:** Transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado o a

una entidad pública o una persona natural distinta de del titular del banco

1.7.2.Título de principios rectores :

- Principio de legalidad
- Principio de consentimiento
- Principio de finalidad
- Principio de proporcionalidad
- Principio de calidad
- Principio de seguridad
- Principio de disposición de recurso
- Principio de nivel de protección adecuado
- Valor de los principios

1.8. **La Autoridad Nacional de Protección de Datos Personales APDP:**

La Dirección General de Protección de Datos Personales es un organismo dependiente del Despacho Viceministerial de Derechos Humanos y Acceso a la Justicia. Tiene como función hacer cumplir las disposiciones, objeto y demás disposiciones de la Ley de Protección de Datos Personales – Ley Nº 29733 tanto como su reglamento.

Así también, la Autoridad Nacional de Protección de Datos Personales en el Perú es la Dirección General de Protección de Datos Personales. Esta organización, es el encargado de vigilar y controlar la actualización y administración del Registro Nacional de Protección de Datos Personales; así también, dar solución a las quejas y reclamos que presentan los titulares de los distintos datos personales en salvaguarda de sus derechos de acceso, rectificación, uso conforme a fin y cancelación.

1.9. **Dirección de registro nacional de protección de datos personales**

La Dirección de Registro Nacional de Protección de Datos Personales es una unidad orgánica que depende de la Dirección General de Protección de Datos Personales, responsable del registro en el que las entidades públicas y privadas inscribirán sus bancos de datos personales. La Dirección de Registro Nacional de Protección de Datos Personales tiene las siguientes funciones:

- Realizar los registros de bancos de datos personales en instituciones privadas o públicas, así como realizar los registros de datos relacionados que se necesiten para la defensa de los derechos de los titulares.
- También se registran las autorizaciones, sanciones administrativas, medidas cautelares y medidas correctivas que disponen los órganos responsables, de acuerdo a la Ley N° 29733.
- Hacer un registro de códigos en las entidades que representan a los titulares o encargados de bancos de datos personales en la administración privada.
- Realizar la publicación de la relación de bancos de datos personales en el portal institucional (http://www.minjus.gob.pe/proteccion-de-datos-personales/).

1.10. **Dirección de Sanciones**

La Dirección de Sanciones es una unidad orgánica que depende de la Dirección General de Protección de Datos Personales que es la encargada de gestionar procedimientos sancionadores por las acciones de control, fiscalización y supervisión realizadas por la Dirección de Supervisión y Control.

1.10.1. Funciones de la Dirección de Sanciones

La Dirección de Sanciones tiene las siguientes funciones:

- Iniciar los procedimientos administrativos sancionadores como consecuencia de las acciones de fiscalización realizadas por la Dirección de Supervisión y Control y resolverlos en primera instancia.

- Ejecutar las sanciones administrativas impuestas y hacer cumplir las medidas cautelares, medidas correctivas o administrativas aplicadas, cuando sean de su competencia.

- Imponer multas coercitivas frente al incumplimiento de las obligaciones accesorias a las sanciones impuestas en el procedimiento sancionador.

- Suministrar información actualizada a la Dirección de Registro Nacional de Protección de Datos Personales sobre las sanciones, medidas cautelares o correctivas impuestas.

1.11. Dirección de normatividad y asistencia legal

La Dirección de Normatividad y Asistencia Legal es una unidad orgánica que depende de la Dirección General de Protección de Datos Personales que se encarga de elaborar la normatividad relacionada con la protección de datos personales y de ejecutar las campañas de difusión y promoción sobre protección de datos.

Esta oficina es la encargada de generar normas y dar opinión sobre cuestiones puestas a su consideración por la Dirección General de Protección de Datos Personales. Asimismo, Se encarga de elaborar los informes técnicos sobre consultas realizadas por los titulares de los bancos de datos personales y por los titulares de datos personales. Además, diseña y realiza diversas campañas de promoción y difusión sobre la protección de datos personales.

TEMA N° 3: Regulación jurídica del flujo internacional de datos y de internet

La globalización y la incorporación de las tecnologías de la información y de las comunicaciones han ocasionado una migración de datos que no conocen de fronteras y de hitos divisorios entre países. Por esta razón es indispensable establecer los límites jurídicos para poder proteger esta información que como se sabe es en algunas ocasiones de carácter privado y aún secreto

1. Internet: nueva frontera de la información y la comunicación

Sin lugar a duda el Internet es hoy por hoy un fenómeno nunca antes pensado al igual que su relación con las Tecnologías de la información y las comunicaciones a partir de los años noventa. “Internet se presenta como una gran oportunidad en el avance de los sistemas de información y comunicación a gran escala. Debido al Internet cada ciudadano, sin moverse de su

casa, puede acceder a los centros de documentación más importantes del mundo, puede realizar las más diversas operaciones financieras y comerciales, gozar de una enorme oferta de entretenimientos de la más diversa especie, y se puede comunicar con otros usuarios de la red sin limitaciones de número ni distancia. Si hace algunos años parecía que la una comunidad global era el gran un sueño, hoy, la Internet se ha convertido en la realidad presente de una sociedad de la información global. Por este motivo las fronteras son cada vez más invisibles para los países y el cruce de información transfronteriza se desarrolla en un solo lugar, el internet." (Pérez, 2003, pág. 86)

2. Implicaciones generales

Si bien es cierto, se tienen ventajas del uso de internet, también existen ciertas implicancias por un mal uso de las, eso hace que exista una preocupación desde los derechos personales hasta la soberanía nacional y como consecuencia esto se refleja en los ámbitos económicos y sociales de entre las naciones, En este caso esto puede ser positivo o negativo.

2.1. Implicaciones positivas

Las implicaciones positivas brindan considerables beneficios al colectivo nacional, entre los que se pueden considerar los siguientes:

2.1.1. El progreso técnico y el crecimiento

El trabajo conjunto de científicos que componen una comunidad mundial, la competencia industrial y empresarial han permitido que se difundan las técnicas y conocimientos, que permite que el mundo entero sea un proveedor de servicios y productos.

2.1.2. La paz y la democracia

La paz mundial y al democracia como objetivos de los pueblos se ve más tangible debido al intercambio de opiniones y mensajes; por lo que se considera un peligro para la democracia, todo atentado en contra de ella.

2.1.3. La interdependencia económica de las naciones

El proceso de globalización y la expansión transfronteriza de las compañías ha permitido que la economía de uno o varios países se vea afectada de forma positiva y negativa por la influencia que estas empresas tienen; Por lo tanto, algún tipo de presión o restricción sobre estas afecta la economía de los países en cuestión.

2.2. Implicaciones negativas

Del mismo modo, el uso de las TICs, tienen también un lado no tan agradable con respecto a un conjunto de problemas que podría generar verdaderos riesgos, De estos, distinguiremos los siguientes:

2.2.1. La vulnerabilidad social

Nuestra dependencia en las tecnologías de la información y las telecomunicaciones, tiene un potencial riesgo ante una catástrofe, falla natural, técnica, o intervención humana. Esta intervención de las TICs, genera una incertidumbre de cuan seguros están nuestro datos y cuan responsables son las empresas que los tienen para protegerlos.

2.2.2. Amenaza a la identidad cultural

La televisión, radio, prensa, cine, entre otros traspasan fronteras e interfieren con la cultura local de cada lugar donde se hacen presente; y ahora no solo eso, sino que el internet hace que este alcance sea aún mayor. Todo esto ocasiona una mezcla y pérdida de identidad cultural en muchos casos.

2.2.3. Dependencia tecnológica exagerada

Muchas son las empresas que tienen dependencia casi total en las telecomunicaciones y la informática para la mayoría de sus procesos de negocio. Esto obedece la tendencia de utilización de las mismas en el mundo y esto incrementa los riesgos que conlleva su uso.

2.2.4. Incidencia económica notoria

El simple hecho de ser una empresa competitiva, requiere que cada vez más se invierta en TICs para mejorar y automatizar los procesos de la empresa; en muchos casos, ingenuamente pensando que tendrán beneficios por el solo hecho de invertir.

2.3. Diferentes flujos de información

Para poder comprender como se realiza el flujo de información es necesario conocer las diversas formas de como fluye la información. Se tomara como referencia la división que establece (Tellez, 2008) para este propósito.

2.3.1. La información comercial

Esta información se manifiesta según una lógica mercantil de distribución de una vía. Así, se distinguen el flujo de prensa general y especializada: servicios documentarios y bancos de datos, sean de carácter bancario, financiero, industrial, bursátil, comercio de audiovisuales (discos, casetes, películas, programas de televisión), comercio de programas de cómputo y tecnologías, etcétera

2.3.2. La información empresarial

Es aquella sustentada en rasgos distintivos, por ejemplo: pedidos, existencias, control de producción, consolidación financiera, gestión del personal, etc., en un cuadro puramente privado en el seno de consorcios empresariales con notorias repercusiones a nivel de dirección, decisión, administración y operación de ellas.

2.3.3. La información especial

Es aquella que, sin estar necesariamente vinculada con intereses comerciales o empresariales, se convierte en intercambio de conocimientos que permiten un mejor desarrollo de las actividades educativas o de investigación a nivel técnico o científico.

2.4. Las redes de comunicación

Para que la información circule a nivel global, es necesario que exista una súper carretera que lleve la información a nivel mundial. Esto es posible a través de redes de comunicación. La informaion circula por una variedad de redes, esto suele depender del tipo de dato que se transmita, por supuesto, que esto considera su importanciaentre los que destacan: “la red de la Sociedad Internacional de Telecomunicaciones Aeronáuticas (SITA) que permite controlar las tele reservacio-

nes aéreas a nivel mundial, la Red Bancaria de Intercambio de Mensajes Financieros (SWIFT, por sus siglas en inglés) que facilita la comunicación a nivel mundial entre las institucioncs bancarias y financieras, la Red de la Policía Internacional (NICS, por sus siglas en inglés) que favorece el intercambio de información referida a criminales perseguidos por Interpol, etc." (Tellez, 2008, pag. 99) Sin embargo, la red más famosa y utilizada a nivel mundial es internet; es por este motivo que se debe comprender la problemática relacionada a la internet.

2.5. Problemática y riesgos de información transfronteriza

Si bien es cierto, el Internet trae consigo innumerables beneficios para las sociedades del planeta, genera problemas de índole jurídica que merecen consideración.

2.5.1. Utilización ilícita de datos transmitidos al extranjero

La transferencia de información entre países, permite existe una manera de escape a las regulaciones que se establecen en un determinado país si se considera la legislación actual. Ncluso esto puede significar un riesgo grave a la seguridad nacional y de los ciudadanos. Es por este motivo que una regulación internacional es necesaria en estos casos.

2.5.2. Tarifas y régimen fiscal aplicables

Como se discutió anteriormente, el aspecto económico de la información, es de forma visible debido a que se le pone un precio económico y sobre todo si esta va a ser exportada; lo que significa un incremento en las tarifas. Por supuesto eso hace referencia los impuestos aduaneros que son impuestos por el Estado teniendo como base la referencia de las tarifas mencionadas. Esto al largo plazo representa pérdidas para el estado que debería contemplar las importaciones y exportaciones de forma jurídica.

2.5.3. Atenta contra la soberanía de los Estados

De la misma manera que otro tipo de tecnología, la transmisión de información, tiene efecto que incurren en profanar la soberanía de las naciones "(entendida no sólo en lo político, sino también en lo social, cultural y otros órdenes)." (Tellez, 2008, p. 97), lo cual implica tener un control jurídico que evite o al menos limite este tipo de situaciones.

2.5.4. Revestimientos contractuales en torno a la información

La información es considerado un bien objeto de derechos y obligaciones y de esta forma, también ser materia de diversos medios de contratación; por lo tanto, esto implica la consideración de cláusulas en los contratos que contemplen los posibles problemas que esto pueda generar, así también los riesgos que se deben considerar para poder asegurar.

2.5.5. Propiedad intelectual de la información

Como se verá en el siguiente tema, se debe considerar la problemática de disputa de autoría con respecto a la propiedad intelectual de la información. Por supuesto que esto repercutirá económicamente para los interesados en materia de alcance de

difusión que se va a considerar debido a la amplitud de las redes informáticas.

2.5.6. Seguridad jurídica de las empresas informáticas

Es necesario contemplar algún tipo de control penal internacional que permita limitar las acciones de trafico de información de forma correctiva y preventiva debido a que dicha información puede ser utilizada inescrupulosamente como objeto o medio de un ilícito.

2.5.7. La intimidad, la imagen, la dignidad y el honor de las personas

Al tener acceso a información, se puede también tener acceso a datos personales y sensibles y por ende se puede transmitir de forma ilegal, promover la difamación, promover el acoso informático fomentar injurias y calumnias, la segregación y el racismo.

2.5.8. La libertad sexual

Al ser posible la propagación de información de forma instantánea y de fácil manera, también se pueden difundir imágenes o información de índole sexual como forma de exhibicionismo, provocación sexual, o que fomente la pornografía infantil, grooming, trata de menores entre otros.

2.6. Organismos gubernamentales y no gubernamentales relacionados

A nivel internacional existen diversos organismos encargados de salvaguardar la información. Según (Tellez, 2008) tenemos:

- Organización para la Cooperación del Desarrollo Económico (OCDE) interesada en la problemática derivada de la protección y seguridad de datos.
- Centro de Corporaciones Transnacionales de las Naciones Unidas (UNCTC) interesado en el problema de las tarifas y el régimen fiscal aplicable a este tipo de información.
- Comisión de Comercio y Desarrollo de las Naciones Unidas (UNCTAD) interesada en la problemática contractual y propiedad de la información.
- Organización Mundial de la Propiedad Intelectual (OMPI) interesada en el problema de la propiedad de la información y el registro de nombres de dominio, al igual que el ICANN.
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) interesada en la trascendencia social, cultural y educativa del FDT.
- Unión Europea (UE) en cuanto a las implicaciones que pueda traer
  consigo a los países miembros de la Unión.
- Organización Mundial del Comercio (OMC) respecto a las tarifas y régimen fiscal aplicable.
- Organización Internacional de Telecomunicaciones Vía Satélite (INTELSAT) en referencia a los problemas jurídicos por la transmisión de información vía satélite.
- Unión Internacional de Telecomunicaciones (UIT) respecto a que sean transmitidas por medios que no usen satélites. Banco Mundial, la privacidad y confidencialidad de datos.

2.7. **Regulación jurídica de internet**

El internet como red principal y más popular del mundo a través de los años ha sido materia de regulación por diversos estados desde su creación en los años 70 a partir del proyecto ARPA el cual fue una división científica del ejército de los Estados Unidos, el cual inició creo una red computacional capaz de sobrevivir ante una catástrofe. En más de 40 años de evolución de internet, se han tenido varios intentos para regular el internet.

Cuando se habla de regulación internacional de Internet, no existe un único instrumento jurídico que regule a la red, ni todos ellos tienen la misma naturaleza. Por una parte, cada capa de la red partió siendo regulada, además de su código, mediante instrumentos específicos, atendido el origen histórico e institucional de cada una de ellas. Esto conlleva a utilizar un tipo regulación considerando las diversas capas de modelo OSI para trasmisión de datos. Partiendo de este punto, existen varias iniciativas llevadas a cabo por organismos como ICANN, la UIT, y países asociados que crean políticas para cada país e internacionales como la ley de protección de datos personales para que puedan tutelar el tránsito de información.

2.8. **La autoregulación de Internet**

En el entorno de la sociedad civil existen empresas que son pioneras en internet y que ya han creado e implantado ciertas normas de "Autocensura", eso sucede en empresas que ofrecen servicios web de forma gratuita y por ende no tiene permitido publicar imágenes obscenas ni pornográficas y también se alienta a dejar de lado los comentarios que contengan lenguaje vulgar e inadecuado. Todo esto con la finalidad de que el internet tenga información relevante que supla las necesidades de la comunidad en general. Con respecto a estos principios, uno de los primeros países en introducir códigos deontológicos de buena conducta en la red es Francia con su concepto de "netiquette" o reglas de etiqueta en la red. Lo mismo sucede en país como Inglaterra que cuentan con legislación y otras técnicas de regulación del uso de internet de modo que se sancione a aquellos que propongan contenido inapropiado e ilícito en la red; asimismo, Existen programas que sirven como un filtro antes estos problemas y que impiden o limitan el acceso a contenido que no cumpla con las regulaciones.

TEMA N° 4: El derecho a la propiedad intelectual y las TICs

El aumento de tecnologías relacionadas con la información que se relaciona con software y nombres de dominio ha generado una necesidad por proteger esta propiedad jurídica. Por lo tanto, debemos conocer cuáles son las medidas necesarias para hacerlo.

1. **Protección jurídica de los programas de computación (software):**

Los programas de cómputo se caracterizan por ser un medio necesario en el día de hoy y el aumento de la producción de software hace necesario su protección; sin embargo, se necesita considerar dos aspectos: el técnico y el económico.

1.1. **Aspecto técnico**

Los programas de cómputo como un conjunto de procedimientos para poder utilizar las máquinas que permiten el procesamiento de información se dividen en los siguientes tipos:

1.1.1. Los programas fuente o de explotación

También se les conoce como sistemas operativos y están conectados al funcionamiento de las máquinas.

1.1.2. Los programas objeto o aplicación

Son los programas que se escriben con el fin de satisfacer las necesidades de usuarios. Algunos de estos programas resuelven las necesidades de un gran número de usuarios y otros responden a medida a necesidades específicas de determinados usuarios.

1.2. Aspecto Económico

Desde el punto de vista económico los programas de computador se han vuelto una fuente de ingresos para programadores y compañías en general. Sin embargo, la producción desmedida con poco o nulo control ocasionado que la exista una pugna constante por tener dominio sobre el mercado de software y como consecuencia, se tiene una rivalidad entre empresas de mismo rubro que compiten por ser propietarios de aspectos técnicos incurriendo así a métodos de obtención de información de la competencia de forma no licita en muchos casos, esto sin duda afecta a los pequeños programadores y desarrolladores destre que buscan una solución ante el tema de creación de programas informáticos. La protección técnica no es suficiente. Hay que considerar necesariamente al derecho, aun si en primera instancia pueda derivarse una comprobación de insuficiencia.

1.3. Régimen jurídico aplicable

Por lo tanto, se necesita una protección jurídica para este bien económico y existen formas de tratar con este tema de acuerdo a las circunstancias.

1.3.1. Vía civil

En el ámbito de la vía civil se consideran:

- **Contratos**, En los contratos se establece un conjunto de cláusulas para proteger la integridad y seguridad de los programas, en las que se puede estipular el acceso no autorizado, modificaciones, mal uso, destrucción de información, etc. Todo esto con una política de mantenimiento en secreto y confidencialidad. Esto prohíbe a una persona a:

    - Obtener informaciones que "pertenezcan" al contratante (ya se trate de copia, duplicación de archivos o "robo" de programa).
    - Modificar las informaciones contenidas en un soporte magnético o modificar su programa.
    - Destruir informaciones, borrar el contenido de un disco o una banda magnética o escribir en una banda que contenga información.
    - Utilizar los recursos de un sistema sin autorización.
    - Explotar un programa en el que el uso esté reservado por contrato.

- **Competencia desleal**, para que un individuo (o una empresa) pueda ser objeto de una acción en esta acción se necesita causar un daño al momento de "tomar" de una empresa algún tipo de secreto de forma ilegal. Por tanto, este tipo de acción no se puede concretar cuando se adquiere algún secreto por medio de un tercero; puesto que ellos no adquieren el secreto en conocimiento desleal del hecho. De por sí, lo que conlleva a la naturaleza jurídica este tipo de acciones esta acción se identifica con la responsabilidad legal de la misma.

- **Enriquecimiento sin causa**, Para tener éxito de esta manera, el afectado necesita probar se hizo uso de su idea o creación y que esta le ha permitido a este generar ganancias y del mismo modo le ha afectado al demandante económicamente. Sin embargo, la obtención de pruebas de este tipo es difícil de conseguir y estos casos son muy difíciles de atestiguar.

1.3.2. Vía penal

Según la vía legal se considera a los delitos como el fraude, robo, exposición de secretos comerciales se presentan como medios de solución frente al problema; sin embargo, Debido a que estos tienen naturaleza física, no se ha podido integrar los modelos de forma completa. Por lo tanto se deben considerar términos afines.

- **Marcas**
  La marca es un signo distintivo que permite a su titular (fabricante o comerciante) distinguir sus productos o sus servicios de los de la competencia. Desde el punto de vista económico, la marca es un signo que tiende a procurar a la clientela, la mercancía o el servicio que busca y paralelamente a la empresa una clientela apegada a la marca. La Organización Mundial de la Protección Intelectual (OMPI) define por marca "un signo visible protegido por un derecho exclusivo concedido en virtud de la ley, que sirve para diferenciar las mercancías de una empresa de las mercancías de otra empresa". (Tellez, 2008, pag. 117)

- **Patentes**
  Todo tipo de invención puede ser merecedor de una patente, y esto necesita considerar alguna actividad inventiva o novedad de uso industrial. Por supuesto, en cada país existe un órgano responsable del registro de patentes: en el Perú, es el INDECOPI; sin embargo, el tema de patentes necesita consideración en cuanto al software debido a que no se puede patentar ideas relacionadas a programas informáticos en el Perú, mientras que en otros países esto si está contemplado por su normativa. Por otro lado, el registro de patentes debe realizarse en el país donde se quiera poseer el derecho de patente.

1.4. Autor de un programa de ordenador

Las leyes relacionadas a la propiedad intelectual parten, como principio general, de que el autor es siempre persona física; y que, sólo por ex-

tensión, las personas jurídicas pueden, en determinados casos, ser consideradas autores. Por lo tanto, son aquellas que se crean "por iniciativa y bajo la coordinación de una persona física o jurídica que la edita y divulga la obra bajo su nombre y está constituida por la reunión de aportaciones de diversos autores cuya contribución personal se funde en una creación única y autónoma para la cual ha sido concebida sin que sea posible atribuir separadamente a cualquiera de ellos un derecho sobre el conjunto de la obra realizada. Salvo pacto en contrario, los derechos sobre la obra colectiva corresponderán a la persona que la edite y divulgue bajo su nombre." (Segundo, 2007, p. 154) Además, para comercializar un programa de cómputo es indispensable diseñar y aplicar una política que garantice la protección del mismo y el respeto a los derechos de otras personas.

1.5. Ley sobre el Derecho de Autor: Decreto Legislativo Nº 822

"Esta Ley, tienen por objeto la protección de los autores de las obras literarias y artísticas y de sus derechohabientes, de los titulares de derechos conexos al derecho de autor reconocidos en ella y de la salvaguardia del acervo cultural. Esta protección se reconoce cualquiera que sea la nacionalidad, el domicilio del autor o titular del respectivo derecho o el lugar de la publicación o divulgación." (Diaz, 2007, pág. 135)

1.6. El INDECOPI:

En esta sección se tomará como referencia la descripción disponible en la página web de INDECOPI, "El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI- fue creado mediante Decreto Ley N° 25868 en noviembre del 1992, para promover en la economía peruana una cultura de leal y honesta competencia y para proteger todas las formas de propiedad intelectual: desde los signos distintivos y los derechos de autor hasta las patentes y la biotecnología. El INDECOPI es un Organismo Público Descentralizado adscrito a la Presidencia del Consejo de Ministros por disposición de la Ley N° 27789, que goza de autonomía técnica, económica, presupuestal y administrativa y tiene por finalidades las establecidas en el la Ley de Organización y Funciones del INDECOPI, el Decreto Ley No. 29299 y el D.L. 807." (INDECOPI, 2016)

1.7. La piratería en el Perú

En nuestro país se encuentran los más altos índices de piratería en Sudamérica. Según la Alianza Internacional de la Propiedad Intelectual se informó en 2010 que ya no había un mercado viable para las copias físicas de grabaciones sonoras en Perú. La distribución digital legítima se enfrenta a retos de servicios en línea como eMule y Ares. La piratería de software en Perú sólo ha disminuido tres puntos porcentuales desde el año 2003 al 65% en el informe de 2013 de la Business Software Alliance. Esto se compara con 18% en los Estados Unidos (2013). El INDECOPI, solo, no puede emprender acciones de ejecución suficientes debido a la falta de recursos. Al mismo tiempo, los criterios de selección deben ser mejorados para los evaluadores de patentes del INDECOPI con el fin de contratar a los mejores evaluadores, que podría ser costoso a corto plazo. (The Economist, 2015) Sin embargo, si se desea un cambio, esto se hace necesario.

2. Protección jurídica de los nombres dominio

En los años 60, al tener los computadores conectados a red direcciones numéricas que eran difíciles de recordar, Paul Mockapetris diseño un esquema denominado DNS (Domain Name Systern) con el propósito d simplificar la operación de comunicación entre ordenadores. Este tenía el objetivo de volverse más conveniente, y de gran facilidad de uso porque brindaba una forma más fácil de entender para los usuarios y las computadoras, sin la necesidad de recordar direcciones IP complejas de los equipos con los que querían comunicarse. Por ejemplo, en vez de: 192.168.1.17, se tiene www.dominio.com.

Consecuentemente, el esquema DNS, cumplió a cabalidad con su propósito y, aún más, estos nuevos nombres no solamente sirvieron como una forma simplificada de conectar una red de equipos en lugares diferentes, sino que sirvió también como una representación de productos, ideas, empresas, servicios, organismos, etc. Posteriormente se utilizó el WWW dentro del registro de dominios para acelerar este proceso; sin embargo, surgieron problemas relacionados a este registro puesto que se terminó creando problemas con a de los nombres de dominio existentes, en este punto ya no se podía volver atrás debido a su popularidad de internet,

2.1. Tipos de Dominios de Primer nivel

Se debe seguir esa asignación de niveles en el esquema de dominios.

2.1.1. Genéricos conocidos como GTLD (Generic Top Level Domain)

Entre los más importantes están los siguientes: ".aero, .biz, .com, .coop, .edu, .gov, .info, .int, .mil, .museum, .name, .net, .org y .pro" (Tellez, 2008, pag 127)

2.1.2. Códigos de país conocidos corno CCTLD (Country Code Top Level Domain)

Algunos de los más importantes son los que siguen: ".ar-Argentina; .au-Australia; .be-Bélgica;.bo-Bolivia; .br-Brasil; .ca-Canadá; .ch-Suiza; .cl-Chile; .cn-China; .co-Colombia; .cr-Costa Rica; .cu-Cuba; .de-Alemania;.ec- Ecuador; .es-España; .fr-Francia; .gt-Guaternala; .hn-Honduras; .il-Israel; .it-Italia; .jp-Japón; .lu-Luxemburgo; .mx-México; .ni-Nicaragua; .nl-Holanda; .no-Noruega; .pa-Panamá; .pe-Perú; .ru-Federación Rusa; .uk-Reino Unido; .us-Estados Unidos; .uy-Uruguay entre otros." (Tellez, 2008, pag 127)

2.2. Registro de los nombres dominio

El manejo de los nombres de dominio genéricos de primer nivel (GTLD) se realizó como una labor académica que se llevó a cabo por el "Instituto de Investigación de Stanford en Menlo Park (SRI)" y fue denominado como SRI-NIC. Posteriormente, la administración de dominios de este tipo llego a estar a cargo de la "Internet Corporation for Assigned Names and Numbers (ICANN)" que fue fundada a finales de 1998. Esta organización salvaguarda los intereses de todos los usuarios de internet a través de una estructura enfocada en los intereses de sus usuarios. Adicionalmente, la IANA (Internet Assigned Numbers Authority), se encarga de asignar los números IP a los usuarios de internet.

2.3. Conflictos entre nombres de dominio idénticos o similares a marcas

En el caso de disputas con respecto a nombres de dominio, se evidencio el registro del dominio mcdonalds.com como primer caso de disputa por un nombre de dominio. Este caso llevó a la Organización Mundial de la Propiedad Intelectual (OMPI) a comenzar un proceso equitativo que tenga todos los interesados en el caso de registro de dominios para poder recomendar de forma uniforme en este para resolver problemas causados por nombres marcas registradas y de dominio, dar recomendaciones a favor de marca reconocidas, considerar los posibles riesgos de generar nombres de dominio genéricos nuevos diferentes a .com, .org, .net y poder crear la UDRP (Política Uniforme de Resolución de Disputas). Cuando la OMPI finalizó su trabajo con el informe final de este caso, éste fue sometido a estudio de la ICANN. Habiendo terminado su labor en octubre de 1999, el Consejo Directivo de ICANN dio el visto bueno a la Política Uniforme de Resolución de Disputas (UDRP) para nombres de dominio. Existen diferencias sustanciales en los casos de nombre de dominio y marcas que se deben considerar.

Tabla 1: Diferencias entre marcas y nombres de dominio

Nombres de dominio	Marcas
Un nombre de dominio sólo puede tener caracteres numéricos, letras del alfabeto inglés y el guion medio.	Una marca puede tener cualquier carácter representable en el alfabeto oficial del país.
Los nombres de dominio (todos) son alcanzables o visibles desde cualquier punto en internet, sin importar si son GTLD, CCTLD, abiertos o restringidos.	Las marcas están sujetas a una territorialidad, y la marca tiene protección sólo en el país que se registra.
La administración de los dominios en el mundo la hacen en 95% instituciones privadas (Cuba, Argentina y otros países son administrados por el gobierno).	La gestión de marcas la hace algún , organismo público.
El registro de un dominio cuesta aproximadamente entre 20 y 50 dólares anuales dependiendo del país.	El registro de una marca en México cuesta 125 dólares por 10 años. En el Perú el costo por registro es aún mayor y se realiza en: http://www.marcaria.pe/
Existen 26 millones de nombres dominio ubicados bajo los GTLD y 14 millones bajo las restantes 244 CCTLD.	
Debajo de cada TLD puede haber un número indefinido de SLD o subclasificaciones.	La clasificación marcaria utiliza 42 códigos.
No puede haber dos nombres de dominio idénticos con la misma clasificación.	Pueden coexistir nombres de marcas idénticos en la misma clasificación
El criterio de identidad entre dos nombres es estrictamente matemático, comparación letra por letra.	El criterio de identidad incluye el concepto de similitud en grado de confusión.
La mayoría de los registros de dominios con algún TLD tarda sólo unos minutos.	El registro de marcas tarda meses.

Fuente: Tellez (2008)

LECTURA SELECCIONADA N° 1: Estrategia Nacional de Gobierno Electrónico, Visión y Objetivo General

ONGEI. (2006). Estrategia Nacional de Gobierno Electrónico. Disponible en: http://www.ongei.gob.pe/Bancos/banco_normas/archivos/Estrategia_Nacional_Gobierno_Electronico.pdf

LECTURA SELECCIONADA N° 2: El Precio de los Datos Personales: La Regulación de la Ley No. 29733

Gamarra, S. (2015). El Precio de los Datos Personales: La Regulación de la Ley No. 29733. IUS 360. Disponible en: http://www.ius360.com/publico/constitucional/el-precio-de-los-datos-personales-la-regulacion-de-la-ley-29733/

LECTURA SELECCIONADA N° 3: Insider Trading o tráfico con información privilegiada

Nieto Martín, A. (2016). Insider Trading o tráfico con información privilegiada. Almacén de Derecho. Disponible en: http://almacendederecho.org/insider-trading-o-trafico-con-informacion-privilegiada/

LECTURA SELECCIONADA N° 4: Dominios y cómo registrarlos

Alvarez, M. A. (2001). Dominios y cómo registrarlos. Desarrolloweb.com. Disponible en: http://www.desarrolloweb.com/articulos/8.php

ACTIVIDAD N° 1

Instrucciones

- Ingrese al foro y participe con comentarios críticos y analíticos del tema Gobierno Electrónico; debe incluir su opinión clara y precisa sobre qué opina del gobierno electrónico y el proceder del país en su desarrollo. Debe sustentar su opinión.
- Para esto Lea y analice el tema N° 1 y la Lectura 1
- Responda en el foro a las siguientes preguntas acerca del gobierno electrónico:

  ¿Cuál es el objetivo de gobierno electrónico?

  ¿Cuál es la finalidad del gobierno electrónico?

  ¿Cuáles son las dificultades para poder implementar completamente el gobierno electrónico en el país?

ACTIVIDAD N° 2

Instrucciones

1. Ingrese al foro y participe con comentarios críticos y analíticos acerca del tema Protección de datos personales; debe incluir su opinión clara y precisa sobre cuál es la problemática en nuestro país sobre el tema en cuestión; ade-

más debe sugerir algunas alternativas para poder fortalecer este punto. Debe sustentar su opinión. Para esto Lea y analice el tema N° 2 y la Lectura 2

2. Responda en el foro a las preguntas acerca del Protección de datos personales:

   ¿Cuáles son las áreas que contempla la ley de protección de datos personales?

   ¿Qué tipos de datos existen? De 3 ejemplos de cada uno.

   ¿Qué tipos de violaciones a los datos personales se dan en nuestro país y cómo cree que se puede controlar esta situación?

ACTIVIDAD N° 3

Instrucciones

1. Ingrese al foro y participe con comentarios críticos y analíticos acerca del tema flujo de datos transfronterizos, regulación jurídica de internet; debe incluir su opinión clara y precisa sobre el problema del tráfico de información de carácter privado (Información de carácter secreto) o prohibido (Información índole delictivo y/o con contenido ilegal) y de información privilegiada (Información a la cual alguien tiene acceso por su cargo laboral). Utilice un párrafo para cada uno; además debe plantear algunas ideas para evitar este problema. Debe sustentar su opinión. Para esto Lea y analice el tema N° 3 y la Lectura 3 y se le recomienda investigar acerca del tema.

2. Responda en el foro a las preguntas acerca del flujo de datos transfronterizos, regulación jurídica de internet:
   ¿Por qué es tan complicado plantear una regulación de internet?
   ¿Qué ideas se podrían plantear ante el problema de tráfico ilegal de información?
   ¿Desde un punto de vista personal, como se puede ayudar a menores de edad y personas vulnerables que son involucrados en pornografía y delitos relacionados a las TICS?

ACTIVIDAD N° 4

Instrucciones

1. Ingrese al foro y participe con comentarios críticos y analíticos acerca del tema el derecho a la propiedad intelectual y las nuevas tecnologías de la información y comunicación; debe incluir su opinión clara y precisa sobre cuál es la problemática en nuestro país sobre el tema de piratería; además debe sugerir algunas alternativas para poder luchar contra este problema tan común en nuestra realidad. Debe sustentar su opinión. Para esto Lea y analice el tema N° 4 y la Lectura 4 y se le recomienda investigar acerca del tema.
2. Responda en el foro a las preguntas acerca del derecho a la propiedad intelectual y las nuevas tecnologías de la información y comunicación:
   ¿Cuál la función del INDECOPI en Perú, mencione al menos 5 funciones?
   ¿Cuál la función de la ICANN e IANA con respecto a los nombres de dominio, mencione al menos 5 funciones por cada uno?
   ¿Qué procedimiento debo seguir si deseo registrar un dominio?

GLOSARIO DE LA UNIDAD II

1. Gestión Pública:

Es la aplicación de todos los procesos e instrumentos que posee la administración pública para lograr los objetivos de desarrollo o de bienestar de la población. También se define como el ejercicio de la función administrativa del gobierno. (Tellez, 2008, pag 543)

2. TICS:

Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. (Olamendi, 2015, pág. 23)

3. ONGEI:

Es el Órgano Técnico Especializado que depende jerárquicamente del Despacho de la Presidencia del Consejo de Ministros, y, en su calidad de Ente Rector del Sistema Nacional de Informática, se encarga de dirigir e implementar la política nacional de Gobierno Electrónico e Informática (ONGEI, 2016).

4. Cibertribunal

Institución cuyo objeto es la investigación, desarrollo y difusión del derecho de las nuevas tecnologías. El cibertribunal peruano es una asociación civil que se constituye el 29 de setiembre del año 1999. Su objeto es resolver los problemas surgidos por un registro abusivo y de mala fe de un nombre de dominio y tiene por objeto la cancelación o la transferencia del mismo. (Tellez, 2008, pag 543)

5. Bancos de Datos

Es un conjunto de datos, de informaciones que son agrupadas y mantenidas en un mismo soporte a modo de facilitar su acceso. Cuando hablamos de un banco de datos estamos señalando que esa información está clasificada y ordenada de acuerdo a diferentes parámetros ya que la misma puede ser solicitada muy a menudo con diversos fines. (Olamendi, 2015, pág. 7)

6. Grooming

El grooming (en español «acicalar») es una serie de conductas y acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, creando una conexión emocional con el mismo, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él. (Olamendi, 2015, pág. 22)

7. Modelo OSI

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos cumplen con los lineamientos del Modelo OSI. (Olamendi, 2015, pág. 33)

8. Nombre de Dominio

Un nombre de dominio (a menudo denominado simplemente dominio) es un nombre fácil de recordar asociado a una dirección IP física de Internet. Se trata de un nombre único que se muestra después del signo @ en las direcciones de correo electrónico y después de www en las direcciones web. (Olamendi, 2015, pág. 38)

9. ICANN

ICANN es una organización que opera a nivel multinacional/internacional y es la responsable de asignar las direcciones del protocolo IP, de los identificado-

res de protocolo, de las funciones de gestión del sistema de dominio y de la administración del sistema de servidores raíz. (ICANN, 2016)

10. IANA

Autoridad de Asignación de Números de Internet: Entidad que supervisa la asignación global de Dirección IP, la asignación de Números de Sistemas Autónomos, la gestión de la zona radicular en el Domain Name System (DNS), los tipos de medios, y otros símbolos y números relacionados con el Protocolo de Internet. IANA es operada por la Internet Corporation for Assigned Names and Numbers (Corporación de Internet para la Asignación de Nombres y Números de Internet), también conocida como la ICANN. (IACANN, 2016)

REFERENCIAS DE LA UNIDAD II

1. Drucker, P. (1989). The New Realities: in Government and Politics, in Economics and Business, in Society and World View. Harper & Row.
2. Castoldi, P. (2000). El gobierno electrónico como un nuevo paradigma de administración. Disponible en: http://200.16.86.50/digital/34/revistas/pi/castoldi55.pdf
3. Ocampo, F. (2003). El gobierno electrónico: ¿reforma de última generación?. Revista Electrónica de Derecho Informático (REDI). Disponible en: www.alfa-redi.org
4. ONGEI. (2012). Plan nacional de gobierno electrónico 2013 -2017. http://www2.pcm.gob.pe/clip/PLAN%20NACIONAL%20DE%20GOBIERNO%20ELECTRONICO.pdf
5. Tellez, J. Derecho Informático. (2008). 4ta edición McGRAW-HILL/Interamericana Editores, S.A.
6. Gaston Concha, A. (2011). El gobierno electrónico en la gestión pública. Naciones Unidas. http://www.cepal.org/es/publicaciones/7330-el-gobierno-electronico-en-la-gestion-publica
7. Castro Cruzatt, K. (2008). El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú. IUS La revista N° 37.
8. Gil Flores, J. (1994). Análisis de Datos Cualitativos. Aplicaciones a la Investigación Educativa, Barcelona, Edit. PPU
9. García Aspillaga, R. (1988). La vida privada y la intimidad de las personas, Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile. Disponible en: http://www.alfa-redi.org/sites/default/files/articles/files/coronel.pdf
10. Núñez Ponce, J. (2001)., La acción constitucional de Habeas Data y la comercialización de información judicial, en pág. 4 de texto publicado en http://vlex.com/redi/No._38_-_Septiembre_del_2001/14
11. Cuervo, J. (2001) La intimidad informática del trabajador de texto publicado en: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=106971, visitada en diciembre de 2001
12. RAE, Diccionario de la Real Academia de la Lengua Española. (2010). Disponible en: http://www.rae.es
13. Casacuberta, D. (1999). citando a Alan F. WESTIN en La privacidad en los nuevos medios electrónicos. Publicado en

http://v2.vlex.com/global/redi/redi_numero.asp?numero=%2311&fecha=Junio+1999
14. Ortúzar Villaroel, M. C. (1996). El nuevo concepto de Derecho a la Intimidad y su protección en la era tecnológica, Tesis de grado de la Escuela de Derecho de la Universidad Católica de Valparaíso.
15. GALTUNG, J. (1966). Teoría y Método de la Investigación Social., Eudeba, Buenos Aires.
16. Agencia Catalana de Protección de Datos. (2005). Conferencia. Disponible en: http://www.apd.cat
17. Serrano Pérez, M. M. (2003) El derecho fundamental a la protección de datos. Derecho español y comparado. Madrid: Civitas.
18. Frosini, V. (1982) Bancos de datos y tutela de la persona. En: Revista de Estudios Políticos (Nueva época), Número 30, noviembre-diciembre de 1982.
19. Peyrano, G. (2002). Régimen Legal de los Datos Personales y Habeas Data. Buenos Aires, LexisNexis-Depalma.
20. Ley N° 29733. (2013). Diario oficial El Peruano. Lima, Perú. 22 de Marzo de 2013
21. Pérez Luño, A. (2003). Internet y los derechos humanos. Universidad de Sevilla, España.
22. Segundo H., Ángel S., Martín Pérez, E., Rodríguez Andrés, M. Á. (2007) Cómo proteger los derechos de Propiedad Industrial e Intelectual en el Sector TIC. Gráficas Muriel. Disponible en: http://www.oepm.es/comun/documentos_relacionados/Publicaciones/monografias/proteccion.pdf
23. Díaz Guevara, J. J. (2007). Régimen de la propiedad intelectual en el Perú. Disponible en: http://www.derechoycambiosocial.com/revista017/propiedad%20intelectual.htm
24. INDECOPI. (2016). Disponible en: https://www.indecopi.gob.pe/sobre-el-indecopi
25. The Economist. (2015). Situación de los derechos de Propiedad Intelectual en el Perú. Disponible en: http://posgrado.pucp.edu.pe/wp-content/uploads/2014/10/EIU-MS-Peru-IP-Environment-2014.pdf
26. ONGEI. (2006). Estrategia Nacional de Gobierno Electrónico. Disponible en: http://www.ongei.gob.pe/Bancos/banco_normas/archivos/Estrategia_Nacional_Gobierno_Electronico.pdf
27. Gamarra, S. (2015). El Precio de los Datos Personales: La Regulación de la Ley No. 29733. IUS 360. Disponible en: http://www.ius360.com/publico/constitucional/el-precio-de-los-datos-personales-la-regulacion-de-la-ley-29733/
28. Nieto Martín, A. (2016). Insider Trading o tráfico con información privilegiada. Almacén de Derecho. Disponible en: http://almacendederecho.org/insider-trading-o-trafico-con-informacion-privilegiada/
29. Alvarez, M. A. (2001). Dominios y cómo registrarlos. Desarrolloweb.com. Disponible en: http://www.desarrolloweb.com/articulos/8.php
30. (Olamendi, G. (2015). Diccionario de informática e internet. Disponible en: http://www.internetglosario.com/

AUTOEVALUACIÓN Nº 2

1. ¿Cuál es la función del ONGEI?

a. Recibir las quejas de se tienen contra el estado con respecto a la información difundida por el portal del gobierno.
b. Formular las políticas públicas en Gobierno Electrónico, así como de elaborar el Plan Nacional de Gobierno Electrónico y los indicadores de desarrollo del Gobierno Electrónico.
c. Elaborar el resumen de uso de las TICS, regular el uso de Internet y contenido virtual.
d. Involucrar a los ciudadanos para crear aplicaciones relacionadas con las TIC y apoyar al gobierno.

2. ¿Cuál es la finalidad del gobierno electrónico?

a. Incluir el uso de las TICs en el sector privado para un mejor gobierno.
b. Fortalecer el gobierno a través de planes de inclusión social y proyectos relacionados con las TICs.
c. Mejorar y simplificar los procesos de soporte institucional para aumentar la transparencia y la participación ciudadana.
d. Involucrar a las organizaciones privadas y públicas en el uso de las TICs para el gobierno de sus servicios.

3. ¿Cuál es el proposito de los cibertribunales?

a. Resolver conflictos de índole familiar, y social por medio del internet
b. Servir de mediadores para conflictos diversos donde las partes están distanciadas geográficamente
c. Servir de mediadores en los litigios derivados del uso de internet
d. Resolver conflictos entre empresas con una página web.

4. El VirtualMagistrate es:

a) Un software de creación XML.
b) Un modelo de gobierno electrónico del Perú
c) Un ejemplo de ciber-corte para resolver conflictos de familia en colaboración entre el Cyberspace Law Institute (CLI) y el NCAIR.
d) Una página web de consulta para magistrados de la colaboración entre el Cyberspace Law Institute (CLI) y el NCAIR.
e) Un servicio de arbitraje en línea resultante de la colaboración entre el Cyberspace Law Institute (CLI) y el NCAIR.

5. ¿A quiénes están sujetos todos los datos personales?

a) La Ley de Protección de Datos Personales y todo su reglamento……
b) Ley de la implementación de la Norma.
c) Ley de Procesamiento de Datos Personales.
d) Ley de Telecomunicaciones.

6. ¿Cuál es el objetivo de la normativa en materia de protección de datos personales?

a) Soporte material de una persona.
b) La medida de disminución de incertidumbre del sujeto respecto a los objetos.
c) Informar el proceso de nuestra vida cotidiana.
d) Garantizar el derecho fundamental a los datos personales

7. ¿Qué es marca según la OMPI?

a) Signo visible protegido por un derecho exclusivo concedido en virtud de la ley.
b) Es un signo abstracto de lo que se desea representar.

c) Sirve para diferenciar las mercancías dentro de una empresa.
d) Es un elemento de restricción y de acceso limitado para la empresa
e) A y b son correctas
f) A y c son correctas

8. ¿Qué es DNS?

a) Es la asignación de una dirección numérica de un host que se encuentra en una red.
b) Es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes.
c) Es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea.
d) Etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz de un dispositivo dentro de una red que utilice el protocolo IP.

9. Señale lo incorrecto sobre la Autoridad Nacional de Datos Personales

a) Es la Autoridad Nacional de Protección de Datos Personales.
b) Supervisa la administración y actualización de registro nacional de protección de datos personales.
c) Resuelve reclamaciones formuladas por los titulares de datos personales en tutela de sus derechos.
d) Emite opinión técnica vinculante respecto de los proyectos de norma que regulen los datos personales
e) Vela por el cumplimiento del objeto y demás disposiciones de la ley de derechos humanos.

10. Para el tratamiento de los datos personales se necesita un consentimiento del titular. El consentimiento debe tener las siguientes características.

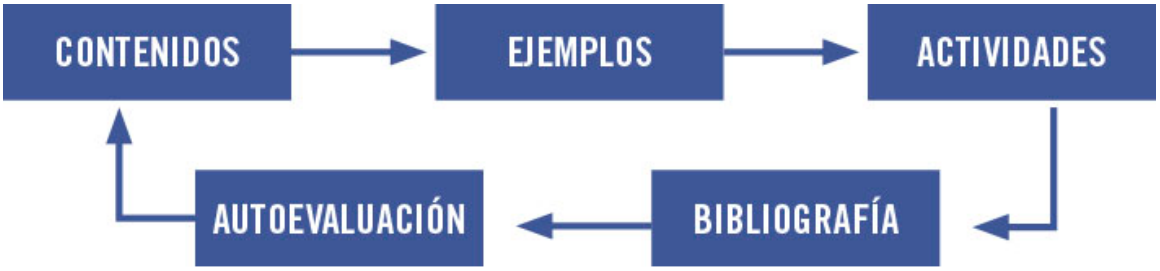
a) Informado
b) Condicionado
c) Bajo amenaza
d) Extenuado
e) Equívoco

ANEXO Nº 1
Respuestas de la Autoevaluación de la Unidad 2

Número	Respuesta
1	b
2	c
3	c
4	e
5	a
6	d
7	a
8	b
9	e
10	a

UNIDAD III: Los contratos informáticos y riesgos informáticos

DIAGRAMA DE ORGANIZACIÓN DE LA UNIDAD III



ORGANIZACIÓN DE LOS APRENDIZAJES

Resultado de aprendizaje de la Unidad III:

Al finalizar la unidad, el estudiante será capaz identificar y describir los diversos tipos de contratos informáticos, considerar los riesgos informáticos, identificar y tipificar los diferentes delitos informáticos e identificar los componentes y factores que contribuyen en el comercio electrónico, demostrando dominio teórico adecuado.

CONOCIMIENTOS	HABILIDADES	ACTITUDES
• **Tema N° 1:** Contratos informáticos. 1. Conceptos relacionados 2. Los bienes informáticos y su clasificación. • **Tema N° 2:** Riesgos informáticos. 1. Los riesgos y su clasificación • **Tema N° 3:** Delitos informáticos. 1. Conceptos relacionados 2. Clasificación y tipología 3. Manejo de los delitos informáticos • **Tema N° 4:** Comercio electrónico **1.** Conceptos generales 2. Características y clasificación del comercio electró-	1. Interpreta y analiza la normatividad vigente de los contratos informáticos. 2. Reconoce los riesgos existentes en materia informática, haciendo uso de las normas existentes. 3. Interpreta y analiza la Ley de Delitos Informáticos. 4. Analiza las características y seguridad de internet en el uso del comercio electrónico. **Actividades Propuestas** • Los estudiantes Participan en el Foro de discusión sobre contratos informáticos. • Los estudiantes Participan en el Foro de discusión sobre riesgos informáti-	• Asume una actitud responsable y crítica sobre las normas vigentes para los contratos informáticos, seguridad de la información, delitos informáticos y comercio electrónico.

nico. **3.** Componentes del comercio electrónico. **Lecturas seleccionadas:** • Contratos Informáticos • Gestión del Riesgo • Sobre la nueva ley de delitos informáticos • El Comercio Electrónico debe garantizar la Seguridad en Internet **Autoevaluación de la Unidad III**	cos. • Los estudiantes Participan en el Foro sobre delitos informáticos • Los estudiantes Participan en el Foro comercio electrónico. **Control de lectura y/o tarea académica** Los alumnos deberán concluir las asignaciones de cada uno de los temas de esta unidad.	

TEMA N° 1: Contratos Informáticos

El aumento que s e tienen de la tecnología y del ámbito informático en el entorno social ha generado un aumento en la comercialización de bienes y servicios relacionados con la tecnología; estos, son regulados mediante figuras jurídicas actuales como los contratos informáticos. Este tipo de contratos, que surgen principalmente del derecho civil contractual, tienen serie de formas específicas establecidas que dificultan su adecuada negociación en la práctica. De este modo, esta nueva categoría contractual requiere un tratamiento minucioso, sobre todo en cuanto a las diversas nuevas implicaciones que se combinan con las actuales, a fin de lograr un régimen jurídico efectivo.

1. Conceptos:

- Un contrato se define como “el acuerdo de dos o más partes para crear, regular, modificar o extinguir una relación jurídica patrimonial” (Artículo 1351° del Código Civil Peruano).

- El contrato entra en vigencia cuando se cumplan las condiciones establecidas en las bases y podría incorporar modificaciones, esto si no implica variación alguna en los aspectos técnicos, precio, plazo, calidad ofrecidas en el proceso de selección. (Artículo 36° de la ley de Contrataciones y adquisiciones del Estado)

- Los contratos de bienes y servicio u obras deben incluir cláusulas con respecto a garantías de la misma para asegurar el cumplimiento y buena ejecución del mismo, así como penalidades por incumplimientos. Además tendrá una cláusula de resolución de controversias para la resolución de discrepancias que se originen en el proceso; del mismo modo, cláusulas de resolución del contrato por incumplimiento para poder resolver de forma total o parcial el contrato por falla en la ejecución (Artículo 41° de la ley de Contrataciones y adquisiciones del Estado)

- “Un contrato informático es un concepto jurídico claramente indeterminado, su ambigüedad viene determinada por el contenido del mismo ya que puede entenderse tanto la prestación de un servicio informático, es decir, pactos cuyo objeto sea un bien o servicio informático, hasta incluir en un sentido mucho más formalista todos aquellos contratos que se perfeccionan por vía informática” (Contratos Informáticos, 2016).

- "El criterio para determinar si nos encontramos ante un contrato informático es atender a su objeto. El objeto de éstos debe recaer siempre sobre bienes y/o servicios informáticos" (Gotzone, 2003, pág. 56).

- "Los contratos informáticos son aquellos que tienen por objeto la contratación de un bien o servicio informático" (INEI, 2003)

  Como ya se estableció, un contrato informático debe estar basado en el que objeto del contrato debe ser un bien o un servicio informático para que pueda caer en esta categoría.

2. Bienes y servicios informáticos

Se definen como bienes informáticos a los elementos que conforman a un ordenador comprendiendo el hardware, el procesador, memorias, tarjetas internas y externas entre otros periféricos, así como las redes y todos los componentes que conforman todo la infraestructura física del elemento informático. Del mismo modo se consideran como bienes informáticos a todas las instrucciones, procedimientos, datos, procesos que se dan a la información y que se encuentra comprendido en el software.

Se entiende como servicios informáticos a "todos aquellos que sirven de apoyo y complemento a la actividad informática en una afinidad directa con ella" (Dávara, 2005, pág. 88). En otras palabras, son aquellas actividades que permiten que los bienes informáticos funciones correctamente; entre estos tenemos, los servicios que tienen que ver con los recursos humanos como la preparación del personal para desempeñarse apropiadamente. Se considera además en este rubro la consultoría general y la planeación de locales de instalación de equipos de cómputo y similares; así como el uso de equipos por tiempo limitado para propósitos específicos, la explotación de programas bajo licencia, la consulta y manejo de archivos y bancos de datos, el mantenimiento preventivo, correctivo y la conservación de equipos informáticos, la auditoría y diagnóstico de sistemas, entre otros afines. (Tellez, 2008, pág. 136) Un ejemplo de esto es el acceso a las redes y el internet, el mantenimiento de software y hardware.

3. Partes de un contrato informático

Existen diversos aspectos a considerar dentro de un contrato de índole informático que intervienen en él según el INEI:

3.1. Los contratantes

Esto hace referencia las partes que tiene relación con la identificación personal y profesional de voluntad y participación de cada uno. A estos se les conoce como clientes, usuarios, interesados, adquirientes, etc. Y son los que se benefician del contrato. Por otro lado tenemos a los desarrolladores, también conocidos como proveedores, licenciantes, distribuidores, fabricantes, etc que son los que prestan los servicios o bienes informáticos y poseen los conocimientos técnicos que se relacionan con el objeto del contrato.

3.2. El objeto del contrato

Este es el interés del acuerdo que especifica las necesidades de los clientes y la oferta de los proveedores. Por supuesto esto debe definir de forma clara y especifica lo que ofrece uno y lo que el otro acepta.

3.3. Las clausulas

Estas establecen las obligaciones para ambas partes donde el proveedor debe colaborar con el cliente y el cliente debe colaborar con el proveedor. Esto involucra el cliente debe respetar y seguir los lineamientos concernientes al bien contratado y su implementación debida, así como su uso adecuado. Esto exonera al proveedor, en caso de incumplimiento o mal uso por parte del cliente. Las clausulas deben incluir:

- Cláusulas de garantía
- Obligaciones claras y específicas de ambas partes
- Sustitución de equipo
- El deber de asesoramiento
- El cumplimiento del plazo
- Prohibiciones de uso
- Mantenimiento
- La capacitación del usuario

3.4. Anexos

Como en todo contrato es necesario que existan anexos que brinden información adicional de carácter obligatorio y o técnico necesaria para el contrato.

4. Tipos de los contratos informáticos

Considerando los diversos ámbitos de los contratos informáticos, se deben tener en cuenta aspectos como su complejidad, su naturaleza y el constante cambio del mundo informático; por lo tanto, según (Gotzone, 2003), se establecen 4 criterios de clasificación:

- Atendiendo al objeto sobre el que recaigan los contratos tendremos contratos sobre bienes informáticos y contratos sobre servicios informáticos.
- Atendiendo a la naturaleza de los bienes informáticos tendremos contratos que recaen sobre bienes materiales, esto es, el hardware, los que recaen sobre bienes inmateriales, software, y por otro lado, los que recaen sobre bienes informáticos.
- Atendiendo a las relaciones reales que recaen sobre la informática los dividiremos en contratos de hardware, contratos de software, contratos de datos, contratos de servicios y contratos complejos.
- Atendiendo al negocio jurídico que se celebre la clasificación sería la siguiente: contrato de venta, tanto de equipos como de programas, contrato de leasing, contrato de locación sobre equipos o programas, contratos de cesión de uso, contratos de mantenimiento y contratos de prestaciones intelectuales como los de estudios previos, formación de personal, contrato llave en mano etc. (Gotzone, 2003, pág. 6)

5. Clasificación de contratos informáticos

Los contratos informáticos se pueden clasificar de dos maneras, de acuerdo al objeto y de acuerdo al orden jurídico.

5.1. Clasificación respecto al objeto

En este caso, se observan características especiales de distintos objetos sobre los que se realizan los contratos, puesto que llevan a la necesidad de su estudio y tratamiento particular. Se tendrá en cuenta la división que ofrece (Tellez, 2008, pág. 160).

5.1.1. Contratos de Hardware

"Para estos contratos se debe conceptuar como hardware todo lo que físicamente forma parte del equipo, y se considera de es-

te tipo, también, a los equipos de telecomunicaciones u otros elementos auxiliares para el funcionamiento del sistema que se va a implementar." (Tellez, 2008, pág. 160).

5.1.2. Contratos de Software

"Con el tema de software, se debe diferenciar en el momento de analizar una contratación, si se trata de un software de base o de sistema, o se trata de un software de utilidad, o de aplicación o usuario, puesto que el último debe responder a unas necesidades particulares, las del propio usuario, y por tanto, tendrán que quedar claramente especificadas en el contrato; sin embargo, el software de base o sistema y el software de utilidad responden a unas características generales que son las del propio de un sistema o las de la utilidad a la que sirven y es un producto ya conformado de antemano que no se somete a peticiones o particularidades del usuario." (Tellez, 2008, pág. 161).

5.1.3. Contratos de instalación llave en mano

"En los que irán incluidos tanto el hardware como el software, así como determinados servicios de mantenimiento y de formación del usuario." (Tellez, 2008, pág. 161).

5.1.4. Contratos de servicios auxiliares

"Como pueden ser, el mantenimiento de equipos y programas o la formación de las personas que van a utilizar la aplicación respecto a equipos, sistema o aplicaciones." (Tellez, 2008, pág. 161).

5.2. Clasificación respecto al orden jurídico

En el orden jurídico se contemplan adaptaciones de los modelos comerciales aplicados a la informática según lo muestra (Gotzone, 2003, pág. 58).

5.2.1. La compraventa informática.

En primer lugar, se debe tener en consideración si el contrato se trata de un una transacción con características ordinarias. Una compraventa informática es una transacción donde se tienen bienes informáticos, y no tiene una propia autonomía. Este tipo de transacción se realiza sobre la idea de compraventa pero se le da un tratamiento diferente por tratarse de un objeto en particular. "En cuanto al hardware, no hay problema alguno en considerarlo objeto del contrato de compraventa. Los problemas se plantean al hablar de la venta de software, es decir, de los programas de ordenador." Gotzone (2003, pág. 58).

Existe un número de entendidos en el tema que argumentan que no se puede realizar la venta de software como tal; esto se debe a que la persona que realiza la transacción económica, no siempre la persona que posee los derechos del software. En realizada lo que se da es un contrato de licencia por el uso que se le da. Para este caso, se considera relevante el principio de buena fe debido a lo mencionado anteriormente con respecto al vendedor y usuarios.

El rol que desempeña un vendedor dentro de un contrato de compraventa informática es el mismo que de cualquier otro tipo de vendedor; con la diferencia que el vendedor informático debe tener especial atención al tema de asesoría cuando se da la venta de grandes equipos, aunque se debe otorgar una especial atención al deber de asesoramiento que tiene el vendedor, sobre todo, con equipos grandes. Se debe asesorar al cliente sobre cuál debería ser la mejor elección según las necesidades del cliente. Por lo tanto, se espera que el objeto, producto del contrato se encuentre en condiciones óptimas cuando esté en funcionamiento.

5.2.2. Los contratos sobre el software

El software se compone de los programas de computadora y cuando estos interactúan con el hardware son capaces de procesar, para poder ejecutar o alcanzar, una tarea, función, o resultado esperado. Habiendo comprendido esto se debe hacer un estudio de cada tipo de software.

- **Contrato de consultoría**, A este contrato se le considera de servicio debido a que se pacta entre el denominado consultor y el cliente sobre la realización de un estudio de requerimientos y análisis de necesidades para poder ofrecer soluciones a sus problemas particulares. Para este tipo de contrato se tiene que el cliente puede ser un cliente cualquiera o la misma empresa que desarrolla software. Este contrato debe celebrarse antes de la realización del estudio.

- **Contrato de desarrollo de software**, Por medio de este contrato se contacta a una persona calificada en la materia que sea capaz de crear un programa informático que de solución a sus necesidades en particular. Ahora bien, no interesa si el contratado es un programador que trabaja solo o una empresa del rubro de desarrollo de software. En estos contratos, es crucial contar con un documento denominado “Documento de especificaciones” puesto que contempla el objeto del contrato y especifica lo que hará el programa. Es también importante establecer quien retiene los derechos de titularidad del software y los límites de las partes del software.

- **Contrato de licencia de uso de software**, Por este contrato se da autorización a una persona o empresa a utilizar un programa informático a cambio de una compensación económica; esta autorización la brinda el que posea los derechos de explotación del software. Para el caso del licenciamiento, el titular mantiene los derechos de propiedad del software. El contrato puede especificar si es de uso exclusivo y de ser el caso que se requiera reproducir o transformar cuando sea necesario, no se necesitará solicitar autorización al titular del software si se ha establecido esto así. Este tipo de contrato es considerado, por la doctrina, como un contrato mixto con características de compraventa y arrendamiento. Men-

cionaremos varios tipos de licencias a considerar en los contratos.

- **Licencia de sistema:** un usuario tiene la facultad de usar el programa cuando lo requiera en cualquier procesador con una licencia de sistema básica, o quizá en una computadora de una determinada clase con una licencia de clase, o también en un computador especifico con una licencia de NODO.

- **Licencia de uso concurrente:** Solo se puede hacer uso del programa en un número específico de usuarios simultáneamente.

- **Licencia temporal:** El programa informático se usa por un periodo de tiempo definido.

- **Licencia runtime:** El usuario final no tienen autorización a utilizar los módulos de programación, empero si los de ejecución.

5.2.3. El leasing informático

Estos contratos tienen características de un contrato común de leasing; el cual es una transacción por la cual usuarios, profesionales y empresas puede comprar material costoso por medio de los beneficios que tienen al usarlo. El usuario o cliente puede usar un componente e ir pagando el valor total en cuotas que si pueda cubrir y al concluir el tiempo convenido, si se desea, se puede optar por adquirirlo con un pago adicional o simplemente terminar el contrato con la devolución del bien. En el leasing informático, no es común que se adquiera al final el software debido a los cambios tecnológicos que sufren los programas y sus actualizaciones. Uno de los escenarios más comunes es que el usuario se encargue de las reparaciones del equipo porque el leasing más común es el de hardware.

5.2.4. El contrato de mantenimiento informático

Este contrato se realiza con la finalidad de poder garantizar el correcto funcionamiento de un bien que se ha comprado, ajustar el producto a medida o actualizar el mismo con mejoras. Este es un contrato de 2 partes, de tracto sucesivo y oneroso. En este contrato existe un problema con respecto al precio que debe fijado con anticipación para los trabajos que se realicen. Puede suceder que un problema considerado en realidad no sea uno que requiera atención y eso exonere de responsabilidad a una de las partes. Esto conlleva a dejar al usuario desprotegido porque no podría establecer actividades determinadas si se contrata en el tiempo tal como lo haría una compañía de seguros, donde se paga por algo que no se tiene idea de cuando se utilizará.

Sería mejor considerar este tipo de contratos tan solo como un contrato de servicios pero que deba contemplar resultados básicos para el funcionamiento del equipo que muestren explícitamente que se desarrolla el servicio. O también se podría incluir el mantenimiento del equipo contrato en una cláusula de otro

contrato o simplemente realizar un contrato que especifique los servicios. En el caso de contratos informáticos, la entrega no garantiza que el equipo esté funcionando como debería, para estos se deben establecer 2 fases: la recepción temporal o de prueba y la definitiva donde se revisaron posibles errores que le proveedor ya ha solucionado.

5.2.5. La auditoría informática

Los contratos de auditoría informática contemplan la verificación de que los sistemas informáticos funcionen en su entorno. Esto considera lo que debería ser en contraste de lo que se tiene en realidad. Es, en forma simple, una supervisión y control que se da sobre los contratos de tipo informático y como estos se cumplen según lo pactado. El auditor, encargado de este proceso, debe contar con la objetividad e independencia necesaria, experiencia y preparación técnica en diversos sistemas informáticos; estos pueden ser internos y externos. Si son externos, se debe celebrar un contrato de auditoria.

5.2.6. El contrato de outsourcing

Este es un contrato de colaboración entre una empresa de desarrollo y un cliente para proveer una solución para las necesidades específicas del cliente. El o los encargos de proveer la solución se encargan de conseguir su propio equipo de software y hardware, la conectividad, el desarrollo, mantenimiento-mejoramiento, copias de seguridad, entre otros. El cliente espera recibir la solución tecnológica que satisfaga su necesidad empresarial con una reducción de sus costos. Al hacer esto, el cliente podrá dar prioridad a centro de su negocio; esto permitirá una mayor posibilidad de competencia.

5.2.7. El contrato de escrow

Este contrato norteamericano permite al usuario tener acceso al código fuente de un programa informático ante ciertas situaciones. Podemos considerar varios tipos de contrato escrow:

- Considerando el depósito, se dividen en escrow privado, y sucede cuando se realiza el depósito a una persona en quien ambas partes confíen y que no se desarrolle como depositario profesional; también puede ser escrow institucional si el depositario se dedica a eso.
- También se puede dividir en escrow titular si se desea probar quienes el titular del software depositado o escrow usuario si se desea permitir el acceso al código fuente.
- Por la contratación, se considera independiente, o de mantenimiento, o integrado, considerando la licencia.
- Considerando la cantidad de usuarios que tienen acceso al código, puede ser un escrow plural o unitario.

5.2.8. El contrato de llave en mano (turn key manage)

En este acuerdo, una empresa usuaria, no cuenta con los recursos o la capacidad suficiente para poder desarrollar un proyecto informático de gran envergadura; por lo cual, contrata los servicios de una empresa tecnológica de desarrollo para lograr la satisfacción de las necesidades de la empresa cliente. Esto lo hace en vez de firmar contratos diversos por obtener lo mismo; en

este caso, es más recomendable tener un contrato que especifique los detalles de posibles sub contratos. Si el caso lo requiere la empresa tecnológica puede sub contratar a otras empresas para poder cubrir ciertas necesidades.

La encargada de afrontar la responsabilidad de terceros frente al cliente es la empresa tecnológica. Con este contrato se busca que la empresa cliente es que la empresa tecnológica le dé resultados concretos en un plazo determinado.

5.2.9. El contrato de seguro informático

Este tipo de contrato no difiere mucho con respecto al de seguro común; sin embargo, se debe considerar que en el caso de uso de la comercialización y uso de tecnologías de la información, existen riesgos de diversas consecuencias dependiendo de lo que se afecte. Todo esto nace por la naturaleza de los sistemas informáticos y su puesta en marcha; por lo tanto se debe considerar un tipo de contrato que considere la responsabilidad que se tendría que asumir por esta actividad. Por ejemplo, las consecuencias económicas para una empresa dependerán de lo que se vea afectado, si son los equipos o la misma información y como esta afecte a otras personas.

5.2.10. Los contratos relativos a internet

Este es un contrato de naturaleza técnica aun cuando tengan similitud con los contratos ordinarios donde se podrían aplicar las normas contenidas en el código civil, la diferencia es que se deben contemplar cláusulas que regulen el objeto del contrato, los derechos y obligaciones. Por supuesto, es común que en este tipo de contratos se proceda por acuerdos con condiciones genéricas de contratación establecidos en el código civil.

5.2.11. Contrato de acceso a internet

En este contrato, el proveedor de acceso a Internet, facilita al cliente o usuario el acceso al internet. La empresa que provee el internet brinda al cliente este acceso a cambio de un pago periódico y le da al cliente la posibilidad de poder aprovechar los beneficios del internet. Este es un contrato diferente puesto que se considerará lo concertado entre las partes. Entre lo que se debe considerar, se tiene el precio a pagar, el ancho de banda de concesión, uso de programas que ofrece el proveedor, la fiabilidad de servicio, entre otros relacionados a la responsabilidad de perdida de información.

5.2.12. Contratos de alojamiento de internet

En este tipo de contratos se considera brindar un espacio de almacenamiento al cliente en su servidor para poder almacenar información en el que almacenar información. Como es de suponer, las partes establecen el contenido del contrato; sin embargo, existen ciertas características que se deben incluir como el precio del servicio, los servicios del proveedor de forma detallada, cláusulas de revisión y control esporádico que realizará el proveedor, también se puede incluir información técnica que permita al cliente migrar a otra plataforma de servicios cuando culmine el contrato y la obligación puesta sobre el cliente con respecto a lo que ponga su sitio web.

5.2.13. Contratos de publicidad

Estos contratos publicitarios son pagados específicamente. Y no tienen diferencia con los de radio y televisión. El responsable de un sitio web decepciona ofertas solicitando publicida en su sitio web para mostrar su marca o logotipo por una compensación monetaria; también se considera un hipervínculo a la pagina web del anunciante. En el contrato se incluye información como el tamaño del anuncio, su ubicación, la forma, intervalo de anuncios, informes a entregar, entre otros.

TEMA N° 2: Riesgos informáticos

Desde una perspectiva jurídica, la idea de riesgo informático es un concepto nuevo, es por este motivo que no existe una definición específica al respecto. El riesgo se relaciona a la probabilidad de que algo perjudicial ocurra o se realice una eventualidad que puede estar prevista. Por este motivo, se puede afirmar que el riesgo es la contingencia de un posible daño. Ahora bien, podemos aseverar que los riesgos informáticos tienen relación con la probabilidad de ocurrencia de una posible materializaciones de un riesgo conectado con una amenaza respecto a servicios o bienes informáticos como equipos informáticos, periféricos, instalaciones, proyectos, software, archivos, información, datos confidenciales, y lo que esto ocasiona frente a terceros por la prestación de un servicio informático.

1. Riesgos informáticos

1.1. Concepto

El diccionario de la Real Academia de la lengua Española define riesgo como “Contingencia o proximidad de un daño” (RAE, 2016).

“El riesgo se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad” (UNISDR, 2009).

1.1.1. Amenaza

Es un fenómeno, sustancia, actividad humana o condición peligrosa que puede ocasionar la muerte, lesiones u otros impactos a la salud, al igual que daños a la propiedad, la pérdida de medios de sustento y de servicios, trastornos sociales y económicos, o daños ambientales. La amenaza se determina en función de la intensidad y la frecuencia.

1.1.2. Vulnerabilidad

Son las características y las circunstancias de una comunidad, sistema o bien que los hacen susceptibles a los efectos dañinos de una amenaza. Con los factores mencionados se compone la siguiente fórmula de riesgo

Basados en la norma ISO/IEC GUÍA 73:2009 se define el riesgo como “Efecto de la incertidumbre sobre la consecución de los objetivos… con frecuencia, el riesgo se caracteriza por referencia a sucesos potenciales y a sus consecuencias, o a una combinación de ambos… con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su probabilidad” (Frayssinet, 2012, pág. 133).

"Riesgo se puede definir como aquella eventualidad que imposibilita el cumplimiento de un objetivo. De manera cuantitativa el riesgo es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado. Así definido, un riesgo conlleva dos tipos de consecuencias: ganancias o pérdidas. En lo relacionado con tecnología, generalmente el riesgo se plantea solamente como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida (por ejemplo el riesgo de perder datos debido a rotura de disco, virus informáticos, etc.)." (Sena y Tenzer, 2004, pág. 125).

La Organización Internacional por la Normalización (ISO) da como definición de riesgo: "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole pérdidas o daños". En la definición anterior se pueden identificar varios elementos que se deben comprender adecuadamente para, por ende, comprender integralmente el concepto de riesgo manejado. Estos elementos son: probabilidad, amenazas, vulnerabilidades, activos e impactos" (Sena y Tenzer, 2004, pág. 125).

1.2. Prevención de riesgos

Es menester conocer que la gestión de riesgos dentro de una empresa las actividades coordinadas para dirigir y controlar una organización en relación al riesgo. La prevención contra riesgos diversos tiene como finalidad la protección de las personas, equipos y trabajos vinculados con la actividad informática. Según Tellez (2008, pág. 163), en la protección se distinguen tres niveles básicos:

1.2.1. La protección amplia

Esta debe ser eficaz y concierne a los locales de procesamiento y sus anexos. En algunos casos también los locales de disposición de las informaciones de entrada y los de almacenamiento y archivo disfrutan de esta protección.

1.2.2. La protección media

Los efectos deben ser compensadores y complementarios. Se instala en los locales de control y de disposición de resultados.

1.2.3. La protección restringida

Se establece en función del grado seleccionado de vulnerabilidad. Es conveniente para los locales de gestión y para los de análisis y programación.

Tomando estas protecciones en consideración se deben implementar medidas concernientes a la implementación de equipos; selección de medios de protección como alarmas, sensores, entre otros; control de accesos al personal; circulación de información y su control respectivo.

1.3. Proceso de continuidad del negocio

El principal objetivo de la gestión de riesgos es garantizar la continua existencia de la organización tratando en todo momento de minimizar los costos derivados de los riesgos. Por lo tanto, la gestión de riesgos involucra los siguientes aspectos.

- La lista de los objetos en cuestión, su valor, su vulnerabilidad y las consecuencias de su deterioro.

- La lista de los medios de prevención, alarma, servicio y recuperación. Los criterios de repartición de los equipos y trabajos entre los diferentes niveles de protección.
- Las consignas generales de puesta en operación de las protecciones y acciones
- Las pérdidas posibles de explotación y los costos correspondientes.
- Los controles de aplicación de los reglamentos.

1.4. Clasificación de riesgos informáticos

Teniendo en cuenta lo mencionado con respecto a los riesgos, se pueden identificar cuatro categorías de riesgos:

1.4.1. Riesgos provenientes del equipo

En este tipo de riesgo, se pueden identificar:

- Pérdida o cambio de mensajes durante el proceso de transmisión.
- Desastres e interrupciones (sean temporales o prolongadas) en la capacidad de funcionamiento del equipo o sus líneas. Éstos pueden ser causados por fuego, inundaciones, terremotos, disturbios, terrorismo, pérdida de energía eléctrica, fallas en el sistema de aire acondicionado, etc. (sean fenómenos de la naturaleza o del hombre).
- Falta de facilidad de respaldo al equipo, líneas de comunicación y personal en el seno de la empresa.
- Fallas del equipo, las cuales pueden provocar la aparición de datos erróneos, omisiones, pérdida de información y problemas similares.

Este tipo de riesgos se relaciona en su mayoría con los problemas que pueden causar el agua y el fuego producto de múltiples factores y se debe contar con las previsiones necesarias para evitar la ocurrencia de los problemas.

1.4.2. Riesgos provenientes de los programas

En este ámbito se tienen:

- Fraude o desfalco mediante la afectación de los activos de la empresa (incluida información), por persona no autorizada y en su proyecto, que puede ser un empleado en la compañía o una persona ajena a ésta.
- Robo de programas, que podrá ocurrir mediante el apoderamiento físico o por medio del copiado ilícito de éstos.
- Falta de posibilidad de recuperación y reinicio del proceso o comunicación de datos.
- Modificaciones no autorizadas, ya sean de carácter temporal o permanente o aun las realizadas por personal normalmente autorizado, ya sea por dolo o por imprudencia.
- Alteración de secuencias. Al no contar con medios para rastrear la .información en el proceso de datos, éste se puede alterar o perder de manera indebida, lo cual pro-

voca, entre otras cosas, complejidad y pérdida de tiempo al tratar de rehacer los movimientos en proceso.

- Deficiente validación de datos-programa. Esto es, la edición de datos, la comprobación de cálculos y las acciones específicas que el sistema pueda generar y cualquier otra función relacionada con la entrada o salida controlada por programa puede no estar debidamente planteada, lo cual puede hacer que continúe el proceso con base en datos erróneos.
- Falta de comprobación intermedia. Es decir, la falta de un control debido a los diferentes pasos del proceso puede provocar no estar en condiciones de saber si se procesan' bien o no los datos o si no se ha perdido la integridad de la información durante el proceso.

1.4.3. Riesgos relacionados con los trabajos

En este ámbito encontramos:

- Riesgos en los proyectos informáticos. Realizar un examen estadístico al respecto pone en relieve la frecuencia de perjuicios y problemas para las empresas o clientes, dada la inejecución O deficiencias en cuanto a la realización de este tipo de proyectos.
- Riesgos contra los datos. Éstos son 'los provocados por la destrucción voluntaria o involuntaria de los soportes que contienen la información, como las cintas, discos, etc., lo cual genera la desaparición o distorsión de datos. En cuanto a esto, también existe la divulgación intencional u imprudencial de datos confidenciales, así como otro tipo de manifestaciones caracterizadas por su alto grado de repercusión económica, datos relacionados con una persona o un asunto de la empresa. Estas acciones se relacionan con el control del flujo, proceso y archivo de la información.
- Provocación accidental o intencionada de errores y omisiones durante el proceso informático, que puede constituir información incompleta o inexacta, mal funcionamiento del equipo o cualquier otra irregularidad que afecte los archivos de la empresa, o falta de control de documentos negociables; esto es, el manejo indiscriminado de documentos negociables (cheques en el banco, pagarés, letras de cambio, etc.) puede provocar su extravío o mal uso.
- Acceso indebido a los sistemas. El acceso no autorizado a los sistemas en desarrollo y en operación expone a la empresa a otra serie de riesgos, como fraude, robo, sabotaje, chantaje, etcétera.
- Acceso indebido a las instalaciones. Similar a lo anterior, el acceso no controlado al equipo o a las terminales representa una posibilidad muy amplia de alteración o conocimiento de información confidencial.

1.4.4. Riesgos de ámbito ilícito

Entre los riesgos de origen ilícito que pueden provocar problemas en la organización, se pueden encontrar:

- Huelga con ocupación de los locales, con los consecuentes riesgos de destrucción o alteración de la información fundamental.
- Destrucción de los soportes de información por agentes físico-químicos no detectables de inmediato, como limaduras de hierro, cenizas de cigarro, imanes permanentes, etcétera.
- Alteración o sustracción de datos.
- Espionaje industrial.
- Robo de fondos, de tiempo-máquina y de programas.
- Falta de respeto voluntario de las consignas de protección.

1.4.5.Riesgos respecto a las personas

En la actualidad, y considerando estudios realizados en la gestión de la seguridad de la información; se ha encontrado que uno de los puntos más vulnerables para que un riesgo se torne en un desastre, es el factor humano. Los riegos vinculados con las personas son los que más influencia tienen con respecto a otros tipos de riesgos. Por lo tanto, incluyen de manera simultánea una acción de sensibilización, formación y control. La acción de sensibilización es más que informativa y se debe trabajar en la cultura de seguridad de la información con un enfoque compartido de las políticas; además, se presenta al personal los diferentes peligros a los cuales hay que enfrentarse y los medios que están a su disposición para combatirlos; por lo tanto, el personal, cualquiera que sea su posición jerárquica, debe conocer a la perfección las políticas que debe consignar la seguridad de la información. Todos deben ser advertidos de sus responsabilidades en materia de seguridad respecto a sus colegas, equipos y trabajos.

1.4.6.Los seguros informáticos

En una empresa informática existen tratamientos preventivos para suprimir o disminuir los riesgos, por ejemplo: la protección del centro de cómputo contra factores externos, control de cargas caloríficas en ellas o cualquier agente transmisor de circuitos o sobrecalentamientos, emplazamiento de extintores y muros contra fuego, supresión de aparatos o vías que canalicen agua hacia el interior del local, estrechamiento de seguridad contra sabotaje, empleo de técnicos expertos para el buen funcionamiento de los equipos, aseguramiento de los soportes que contienen o reproducir la información y el control en archivos separados, instalación de protecciones técnicas para los programas, supervisión adecuada de equipos y programas, entre otros.

Sin embargo, todo esto debería ir acompañado de una o varias pólizas de seguro que puedan ayudar a proteger en materia económica la continuidad de la organización ante algún tipo de pérdida o desastre como consecuencia de un riesgo. La evaluación del monto de dichos gastos estará a cargo de los informáticos de la empresa previa evaluación de la empresa aseguradora y se debe considerar detalladamente las partes de la póliza para efectos de una protección efectiva. De este modo, el problema financiero resultante de un desastre puede compen-

sarse por un apoyo bancario del que algunas aseguradoras aceptan pagar sus intereses.

TEMA N° 3: Los delitos informáticos

El aumento de las tecnologías de la información y la creación de la sociedad de la información que facilita el crecimiento de las TICs, no solo ha generado nuevas oportunidades de crecimientos personal como corporativo, también ha servido como incentivo para que personas relacionadas con actividades delictivas también utilicen las TICs como un medio para cometer sus fechorías. Es por este motivo, y en conocimiento de esta realidad que muchos países alrededor del mundo están adoptando medidas para disuadir, corregir y castigar a aquellas personas que quieran hacer de la sociedad de la información un rentable mercado para el crimen. Por este motivo se debe conocer cómo es que todos estos actos que atentan contra la integridad de las personas, es tratado según el ámbito jurídico.

1. Conceptos

Los delitos informáticos son actividades criminales que han sido contempladas por muchos países y adaptar dentro de sus figuras jurídicas tradicionales, como fraudes, hurto, estafa, falsificaciones, perjuicios, sabotaje, entre otros. No obstante, se destaca que el uso de las tecnologías de la información y las telecomunicaciones ha generado posibilidades nuevas de crimen que nacen a partir del indebido uso que se les da a las computadoras; esto ha generado una necesidad latente de regular este tema en el ámbito del derecho. Internacionalmente se considera que no se ha definido debidamente al delito informático; sin embargo, existe un esfuerzo conjunto de muchos que han tratado de dar una definición general considerado diversos puntos de vista.

Tellez define al delito informático como las "actitudes ilícitas que tienen a las computadoras como instrumento o fin" o las "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin” (Tellez, 2008, pág. 188).

Callegari N. afirma que el delito informático es, “aquel que se da con la ayuda de la informática o de técnicas anexas”. Este concepto tiene la desventaja de solamente considerar como medio de comisión de esta clase de delitos a la informática, olvidándose la autora que también que lo informático puede ser el objeto de la infracción (Callegari, 1985, pág. 113).

Davara Rodríguez nos dice que es, “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.” (Davara, 1997, pág. 39).

Parker brinda la siguiente definición: “todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio” (Parker, 1976, pág. 86).

En palabras de Acurio del Pino, la “delincuencia informática es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o

poner en peligro un bien jurídico cualquiera." (Acurio del Pino, 2000, pág. 12).

Así mismo, Huerta M. y Líbano C. definen al delito informático como, "todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro" (Huerta, Líbano, 1998, p. 135).

En resumen, y considerando los conceptos expresados por diversos autores, se puede afirmar el delito informático es aquel que se encuentra relacionado de forma directa o indirecta con un componente de las TIC para realizar una actividad con la finalidad de beneficiarse de esto.

2. Características del derecho informático

(Tellez, 2008), nos muestra una distribución de características de los delitos informáticos que ayuda a entender cómo es que estos operan:

- "Son conductas criminales de cuello blanco (white collar crimes) en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden cometerlas.
- Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto está trabajando.
- Son acciones de oportunidad porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.
- Ofrecen facilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física.
- Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica a nivel internacional.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, por su carácter técnico.
- En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales.
- Ofrecen a los menores de edad facilidades para su comisión.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional." (Tellez, 2008, p. 188)

3. Clasificación de los delitos informáticos

(Tellez, 2008) muestra una división de los delitos informáticos considerando el enfoque del ataque y la orientación del mismo, se puede clasificar a los delitos informáticos en 2 tipos:

3.1. Como instrumento o medio

En esta categoría se encuentran aquellas conductas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

- “Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera).
- "Robo" de tiempo de computadora.
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema con instrucciones inapropiadas (esto se conoce en el medio como método del caballo de Troya).
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como técnica de salami.
- Uso no autorizado de programas de cómputo.
- Inclusión de instrucciones que provocan "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios.
- Alteración en el funcionamiento de los sistemas.
- Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.” (Tellez, 2008, pág. 191)

3.2. Como fin u objetivo

“En esta categoría se evidencian las conductas dirigidas en contra de la computadora, accesorios o programas como entidad física. Algunos ejemplos son los siguientes:

- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas por cualquier método.}
- Daño a la memoria.
- Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etcétera).” (Tellez, 2008, pág. 192)

4. Sujetos del Delito Informático

El derecho penal expone 2 tipos de sujetos en el delito informático, el sujeto activo y el sujeto pasivo, y estos pueden ser personas o empresas. Considerando esto, el bien objeto del delito será el que identifique de que sujetos se está haciendo referencia. El sujeto pasivo será por ende, quien es afectado en su bien jurídico; por supuesto que este podría ser diferente del prjudicado directamente, quien podría ser un tercero, como en el caso de información robada. La otra cara de la moneda es el sujeto activo, quien es aquel que haga uso ilícito del bien.

4.1. Sujeto activo

Aquel que realiza parte o toda la acción de tipo penal es denominado sujeto activo. De manera más práctica, quien comente el delito informático. Para ser un criminal informático, se deben reunir ciertas carac-

terísticas no tradicionales, si hablamos de los crímenes cotidianos, como por ejemplo, tener experiencia en programación, manejo de equipos de cómputo, redes y telecomunicaciones, conocimiento de lenguajes de programación diverso, posicionamiento estratégico en relación al bien en cuestión entre otros.

4.1.1. Perfil del ciberdelincuente

El perfil del ciberdelincuente, sujeto activo, en esta modalidad delictual requiere ciertas habilidades y conocimientos, por ello también se les ha calificado como delincuentes de "cuello blanco", que tienen como características:

- Poseer importantes conocimientos informáticos.
- Tener un posicionamiento ventajoso en el área de trabajo que le permita tener acceso a información sensible; a estos delitos se les denomina, delitos ocupacionales debido a que utilizan este espacio laboral.

Se pueden identificar diferentes sujetos activos que se les denomina de diferente manera dependiendo del modo como actúan y que conductas son las que realizan:

Hackers, son individuos con conocimientos informáticos que por interés propio o afición rompen la seguridad de programas y sistemas que tienen cierto grado de protección, conocido como "delincuente silencioso o tecnológico". Les gusta indagar por todas partes, conocer el funcionamiento de los sistemas informáticos; son personas que realizan esta actividad como reto intelectual, sin producir daño alguno con la única finalidad de descifrar y conocer los sistemas informáticos. Para (Sieber, 1992, p. 77) los hacker son "personas que acceden sin autorización a un sistema de proceso de datos a través de un proceso de datos a distancia, no cometido con finalidades manipuladoras, fraudulentas, de espionaje, ni sabotaje, sino sencillamente como paseo por placer no autorizado".

Crackers, son los individuos que no solo penetran en los programas informáticos remotos con la intensión destruir, cambiar, corromper quitar el acceso, en general, causar problemas a las redes informáticas, sistemas, entre otros y que también son conocidos como piratas informáticos. Una diferencia tangible con los hackers es que los crackers consiguen en internet programas creados por otros; mientras que los hackers crean sus propios programas, tiene mucho conocimiento sobre los programas y conocen muy bien los lenguajes informáticos. Por otra parte, (Morant Vidal, 2002, p. 44) define a estos sujetos como "personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas.

4.2. Sujeto Pasivo

El sujeto pasivo es aquel que tiene la titularidad del bien objeto del delito y que es afectado por el sujeto activo. Es necesario también diferenciar entre la victima directa del delito y el sujeto pasivo, Esto debido a que el titular puede no ser la victima directa del delito pero también se ve afectada por el hecho, las victimas directamente afectadas

pueden ser personas, empresas, organizaciones, gobiernos que utilizan sistema de información interconectados. Los sujetos activos son de vital relevancia para la lucha contra los delitos informáticos, debido a que de otra manera no podrían conocerse los accionares de los sujetos activos o simplemente tardaría mucho en conocerse.

Además, la persona jurídica sí puede ser considerada como sujeto pasivo, como por ejemplo, empresas públicas y privadas (bancos, instituciones públicas, industrias, seguros, etc.), aunque en ciertos casos, estas personas jurídicas no denuncien los delitos del que son víctimas por cierto temor al desprestigio o al impacto entre sus clientes y consecuentes efectos económicos desfavorables.

5. Delitos informáticos reconocidos por la organización de las naciones unidas (ONU)

Según una clasificación realizada por la ONU, podemos ver los siguientes tipos de delitos que menciona (Tellez, 2008, p. 193):

5.1. Fraudes cometidos mediante manipulación de computadoras.

5.1.1. Manipulación de los datos de entrada

A este tipo de fraude se le conoce también como sustracción de información y ejemplifica uno de los delitos informáticos mas comunes puesto que se puede hacer con facilidad, pero es difícil de que se descubra porque no requiere de un extenso conocimiento técnico de las TIC y puede ser realizado por cualquier individuo con acceso a los datos.

5.1.2. Manipulación de programas

Debido a que el delincuente tiene condominitos concretos de informática y uso de computadores, este delito puede pasar desapercibido. Los programas o sistemas existentes son modificados, alterados, se insertan programas nuevos o sub procedimientos por el criminal; Entre los métodos más comunes de los atacantes informáticos se tienen, los gusanos, caballos de Troya e incluso se hace uso de la ingeniería social para poder tener acceso y control del sistema que modificaran posteriormente, Por medio de estas técnicas, logran insertar instrucciones de computadora que no bloqueen el funcionamiento de los programas informáticos y de esta manera quedan encubiertos.

5.1.3. Manipulación de los datos de salida

Para este delito se selecciona estratégicamente un objetivo del sistema informático. Uno de los casos más comunes es el que sucede en cuentas de banco , y en especial en los cajeros automáticos donde se ingresan instrucciones fraudulentas cuando se solicitan los datos de verificación En sus inicios estos fraudes eran realizados por medio de tarjetas clonadas pero en la actualidad, los atacante informáticos, tratan de burla la seguridad de los portales web de banco y de usuarios con los que puedan insertar su código malicioso y obtener ganancia de estos.

5.1.4. Fraude efectuado por manipulación informática

Esta es una técnica en la cual se hacen transferencias sistemáticas de pequeñas cantidades de dinero casi imperceptibles de cuentas de banco de uno o varios clientes a una cuenta desig-

nada por el criminal y de este modo se obtiene un botín muy sustancioso aprovechando procesos automáticos del sistema.

5.2. Falsificaciones informáticas

5.2.1. Como objeto

Esto se realiza cuando se cambia la información depositada equipos de cómputo.

5.2.2. Como instrumentos

Así también, los equipos de cómputo pueden utilizarse para realizar copias de documentos comerciales. Este proceso de obtener copias ilegales, surgió a partir de la invención de las fotocopiadoras láser puesto que con esta tecnología se puede ahora realizar copias con tal fidelidad y calidad que aun confundirían a un experto en la materia.

5.3. Perjuicios o cambios de datos o programas computarizados

5.3.1. Sabotaje informático

Consiste en alterar o eliminar información sin la autorización necesaria con el propósito de estorbar el correcto funcionamiento de un programa o sistema informático. Entre las técnicas más utilizadas tenemos:

- **Virus:** Es un conjunto de instrucciones de computadora que lograr incrustarse en programas legales para multiplicarse en sistemas o programas informáticos. La finalidad de los virus varía según quien los crea, pero en muchos casos se ha perdido información por una infección de virus en el sistema que se propago sin control.

- **Gusanos:** Tienen la misma manera de elaboración que los virus y se diseñan con la finalidad de infectar los sistemas de información y de este modo alterar o destruir la información que se encuentra en estos; sin embargo, los gusanos no necesitan de un transportador para replicarse. Pues aprovechan algún medio de transporte del sistema para hacerlo. Los gusanos pueden también traer consigo instrucciones de conexión remota que permita a un ciber delincuente a tener acceso completo al sistema y de este modo hacerse con información para cambiarla o destruirla.

- **Ramsonware**: el caso de ramsonware es un tema nuevo en el mundo de los programas informáticos que dañan la información; esta técnica consiste en descarga un programa de computadora de tipo encriptador por medio de algún gusano o troyano y cifrar la información de un usuario para luego solicitar un rescate para que esta información se libere. En muchos de los casos se han reportado pérdidas considerables para las empresas y los individuos que sufrieron la encriptación de su información sin poder luego recuperarla muy a pesar de haber realizado el pago que lesolicitaron.

- **Bomba lógica o cronológica:** El caso de la bomba lógica es muy diferente al de los virus y gusano, pero tiene algu-

na relación con el ransomware puesto que se necesitan conocimientos avanzados de computación y programación debido a que se puede programar la modificación o destrucción de información en un futuro que el criminal designe. Considerando que son difíciles de detectar y que solo el criminal informático sabría cuando harían explosión es que se les considera devastadoras; puesto que no solo pueden explotar mucho tiempo después de que el criminal las haya dejado, sino que también puede servir como medio de extorsión por el cual se demande un rescate a cambio de dar a conocer donde y cuando explotará la bomba; es ahí donde radica la similitud con el ransomeware.

5.3.2. Acceso no autorizado a servicios y sistemas informáticos

Este acceso tiene motivaciones diversas tales como el espionaje informático, sabotaje empresarial, ataques informáticos, o la curiosidad de hacerlo.

5.3.3. Destrucción de datos

Es lo que sucede cuando se introducen gusanos, virus, bombas lógicas o malware en general.

5.3.4. Infracción al copyright de bases de datos

Esto sucede si se accede a una base de datos sin tener la autorización necesaria.

5.3.5. Interceptación de correo electrónico

Consiste en leer mensajes de correo que no son propios.

5.3.6. Estafas electrónicas

Se hace uso de la red para delinquir y obtener beneficio económico.

5.3.7. Transferencias de fondos

Se realizan transferencias bancarias electrónicas utilizando la red.

5.3.8. Espionaje

Se accede a información confidencial por medio de la red, sistemas informáticos u otro medio con el propósito de conocer las debilidades y fortalezas de una empresa, gobierno, organización o persona para beneficiarse de esta.

5.3.9. Terrorismo

Se utiliza la red para propagar mensajes de grupos terroristas y planear o transmitir sus planes y actividades.

5.3.10. Narcotráfico

Se usa la red para compartir información relacionada al mundo del narcotráfico y sus actividades ilícitas.

5.4. Delitos informáticos contra la indemnidad y libertad sexuales

Entre los más preocupantes delitos a considerar tenemos los relacionados con menores de edad. Las leyes de todos los países condenan el

uso de las TIC para tomar ventaja de la inocencia de menores de edad. Entre estos delitos se debe destacar:

5.4.1. Delitos contra la libertad sexual

Son acciones destinadas a vulnerar tanto la indemnidad sexual como la libertad sexual del menor. Este delito se consuma con la sola proposición, a un menor de edad con fines sexuales, ya sea para obtener material pornográfico o para acceder a la actividad sexual, esta conducta es sancionable porque afecta la indemnidad del menor y la libertad sexual y el medio utilizado para facilitar el contacto es la informática.

5.4.2. Pornografía infantil

Debido a que el carácter de lo que es obsceno se vincula con las variantes culturales que existen en el mundo, el concepto de pornografía infantil difiere también conforme a las prácticas de comportamiento sexual, las creencias religiosas y los valores morales que tiene cada sociedad. Dicha situación motiva que tanto la definición como las medidas que establecen los distintos países en sus legislaciones para evitar la pornografía infantil tengan alcances diferentes. En esta conducta tipificada se denota la intención del legislador de proteger penalmente varios bienes jurídicos, cuya titularidad corresponde a menores de edad, cuales son los adecuados procesos de formación y socialización de unos y otros y, su intimidad.

5.4.3. Convenciones internacionales

(Tellez, 2008) nos muestra su recopilación de las diversas convenciones a nivel mundial con respecto a los derechos del niño con el objetivo de prevenir la explotación y el abuso.

- Declaración de Ginebra sobre los Derechos del Niño (1924).
- Declaración Universal de los Derechos Humanos (1948).
- Declaración de los Derechos del Niño (1959).
- Convención sobre los Derechos del Niño (1989).
- Declaración Mundial sobre la Supervivencia, la Protección y el Desarrollo del Niño (1990).
- Declaración de la Organización Mundial del Turismo sobre la Prevención del Turismo Sexual Organizado (1995).
- Declaración de Estocolmo contra la Explotación Sexual infantil con Fines Comerciales (1996).
- Declaración y Plan de Acción de los Niños y Jóvenes Víctimas de la Explotación Sexual (1998).
- Convenio núm. 182 de la OIT, junto con su Recomendación núm. 190, sobre la prohibición dc las peores formas de trabajo infantil y la acción inmediata para su eliminación (1999).
- Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la delincuencia organizada transnacional (2000).
- Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (2000).

- Convenio sobre el Delito Cibernético del Consejo de Europa (2001).
- Compromiso mundial de Yokohama (2001).
- Decisión marco 2004/68IJAI del Consejo de Europa, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil (2003). (Tellez, 2008, p. 198)

6. La ley n° 30096

Ahora se hará referencia al contenido general de la Ley 30096 publicada el 22 de Octubre del 2013 en el diario oficial El Peruano. Esta ley tiene como propósito prevenir y sancionar los delitos que afectan la información y los sistemas informáticos cometidos utilizando las tecnologías de la información y las comunicaciones (TICS), para afirmar la lucha eficaz contra la ciber delincuencia. Esta ley está distribuida de la siguiente manera y si se desea un conocimiento completo de la misma, se recomienda acceder a ella:

CAPÍTULO I- FINALIDAD Y OBJETO DE LA LEY
Artículo 1. Objeto de la Ley

CAPÍTULO II -DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS
Artículo 2. Acceso ilícito
Artículo 3. Atentado contra la integridad de datos informáticos
Artículo 4. Atentado contra la integridad de sistemas informáticos

CAPÍTULO III-DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES
Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

CAPÍTULO IV- DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES
Artículo 6. Tráfico ilegal de datos
Artículo 7. Interceptación de datos informáticos

CAPÍTULO V- DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO
Artículo 8. Fraude informático

CAPÍTULO VI- DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA
Artículo 9. Suplantación de identidad

CAPÍTULO VII- DISPOSICIONES COMUNES
Artículo 10. Abuso de mecanismos y dispositivos informáticos
Artículo 11. Agravantes

TEMA N° 4: El comercio electrónico

La globalización y la implementación de las TICs en diferentes actividades de la vida humana generan cambios económicos en todo el mundo puesto que están cambiando la manera de hacer negocios. Lo que genera estos cambios son los avances tecnológicos, el aumento de la competitividad y competencia, el cambio constante de preferencias de los clientes y consumidores, el aumento de capacidad de los proveedores, entre otros.

Así mismo, el Internet, también ha generado la creación de nuevas formas de comercio, entre ellos el denominado comercio electrónico o E-business, que no es más

que realizar las transacciones comerciales y negocios utilizando las TICs. Por lo tanto, el núcleo de todo el comercio electrónico es, sin duda, el internet.

1. Conceptos generales

A continuación veremos algunos conceptos relacionados con el comercio electrónico en palabras de personas conocedoras del tema:

- De Ros M. afirma que el comercio electrónico es, "un fenómeno jurídico y se concibe como la oferta y la contratación electrónica de productos y servicios a través de dos o más ordenadores o terminales informáticos conectados a través de una línea de comunicación dentro del entorno de red abierta que constituye Internet. Representa un fenómeno en plena expansión con votos de crecimiento extraordinario en número de conexiones, clientes y operaciones" (De Ros, 2000, p. 68).
- (Davara, 2001) define por separado lo que él considera comercio y lo que significa que sea electrónico: "…en un sentido amplio, es comercio toda aquella actividad que tenga por objeto o fin realizar una operación comercial y que es electrónico cuando ese comercio se lleva a cabo utilizando la herramienta electrónica de forma que tenga o pueda tener alguna influencia en la consecuencia del fin comercial, con el resultado de la actividad que está desarrollando" (Davara, 2001, p. 36).
- Igualmente, García del Poyo precisa que es, "el intercambio electrónico de datos e informaciones correspondientes a una transacción con contenido económico" (García del Poyo, 2001, p. 82).
- Aparicio Vaquero, tiene una idea diferente con respecto a lo que es la "contratación electrónica" puesto que no desea crear una nueva categoría contractual, mas bien se trata de un, "concepto bajo el cual se regulan y estudian de forma sistemática todos aquellos contratos que tienen como característica común la forma en que son concluidos: entre personas que no se encuentran físicamente en el mismo lugar y que emiten sus declaraciones negóciales mediante máquinas informáticas que tienen a su disposición." (Aparicio, 2002, p. 105). También nos indica el contrato electrónico es un contrato celebrado a distancia y que surge de la denominada sociedad de la información.
- Desde otra perspectiva, Guisado Moreno menciona el comercio electrónico es, "aquel que abarca las transacciones comerciales electrónicas compraventa de bienes y prestación de servicio realizados entre empresarios, o bien entre empresarios y consumidores, a través de los soportes electrónicos proporcionados por las nuevas tecnologías de la información y la comunicación, básicamente Internet, así como también las negociaciones previas y posteriores estrechas y directamente relacionadas con aquellos contratos (ofertas contractuales, contra ofertas, pago electrónico)" (Guisado, 2004, p. 95).

Por lo mencionado el comercio electrónico se define en general como toda aquella actividad comercial que tiene como finalidad el intercambio electrónico de bienes y servicios como el internet y las TICs para facilitar el comercio.

2. Características del comercio electrónico:

2.1. Transacción de bienes y/o servicios

El fin del comercio electrónico es la comercialización de productos y servicios tales como bienes de consumo y servicios de todo tipo u categoría incluyendo los radiocanales a través del uso de las TICs.

2.2. Utilización de medios electrónicos

Como se menciona anteriormente, el principal medio pro el cual se desarrolla el comercio electrónico es la red (local y el internet). Esto facilita las transacciones comerciales y brinda también beneficios como las páginas web, servicios de correo electrónico, chat, video lamadas, etc.

2.3. Reducción de costes de transacción

Para poder celebrar un contrato, se tienen costos que deben ser asumidos por las partes, a estos se les denomina costos de transacción; entre ellos se tienen los costos para transporte, costos para encontrar información, costos de negociación, costos de profesionales y expertos, etc. Estos costos en el comercio electrónico disminuyen debido a las ventajas que ofrecen las TICs y el internet, como por ejemplo la flexibilidad de tiempo y lugar.

2.4. Apertura de un nuevo mercado: "el mercado Virtual"

Existe una interacción entre un vendedor y un comprador en un lugar real determinado y de forma presencial y física en el modelo del mercado tradicional. Esta interacción hace posible que el vendedor conozca sobre las necesidades del comprador y de este modo utilizar las técnicas que requiera para atraer al comprador a su negocio. Sin embargo, en un mercado electrónico o virtual se rompen los esquemas del mercado tradicional con respecto a contacto entre comprador y vendedor, el lugar y el tiempo donde se realiza la transacción.

3. Los sujetos intervinientes en el comercio electrónico.

Desde el punto de vista legal, el comercio electrónico se considera como un contrato especial en el que la interacción entre los participantes del contrato se realiza por medios electrónicos. A partir de esto podemos discernir que en un contrato electrónico, existen 2 o más participantes. En primer lugar tenemos al proveedor, quiene es la persona o empresa que brinda el producto o servicio; también se tiene al consumidor que puede ser de 2 clases, consumidor final e intermediario, también se tiene al estado conformada por todos los organismos del gobierno. Ahora bien, debemos considerar estos participantes base para poder comprender la interacción entre ellos.

4. Clasificación del comercio electrónico:

4.1. Según la participación de los sujetos o agentes económicos

4.1.1. Comercio entre empresas (b2b):

Se le denomina así al comercio que toma lugar entre empresas y hace referencia, en particular, a las transacciones electrónicas entre empresas. En este rubro se consideran aquellas operaciones donde las empresas realizan pedidos o copras, pagan por ellas, solicitan modificaciones, etc.; en otras palabras, se relacionan con los otros sujetos utilizando las TICs. Por supuesto, que el comercio entre empresas va mucho más allá que una simple venta por internet, puesto que involucra aspectos como la conexión interacción de procesos de empresas que permitan que los negocios se realicen.

4.1.2. Comercio entre empresa y consumidor (b2c):

El comercio entre empresa y consumidor contempla los negocios que se suscitan entre un consumidor final que solicita a una empresa. Un ejemplo de este tipo de transacciones son las compras que realizan los consumidores en internet; por supuesto que lo que se ve hoy es solo una pequeña proyección de lo que estima a futuro. Lo más relevante y de por sí, la ventaja más grande que posee el comercio electrónico es que les permite a las empresas expandirse y tener contacto (virtual) directo con el consumidor final sin la necesidad de contar de una locación y tiempo específicos. Como consecuencia, la empresa obtiene crecimiento y el consumidor un servicio mejorado.

4.1.3. Comercio entre las empresas y la administración (b2a):

Este tipo de comercio electrónico se realiza entre el estado, que solicita bienes y servicios de empresas proveedoras.

4.1.4. Comercio entre consumidores (c2c):

Esta es una nueva tendencia de comercio electrónico por medio de la cual los consumidores interactúan con otros consumidores; esto lo hacen a través de páginas web o aplicaciones para dispositivos móviles que les permiten realizar ventas e intercambios de bienes, servicios e información. Este tipo de comercio funciona como una comunidad virtual de intercambio sin necesitar de algún tipo de intermediario.

4.1.5. Comercio entre administración y consumidor (a2c):

En la actualidad se utilizan las TICs para promover los pagos de servicios de la administración estatal a través de medios electrónicos; un ejemplo de esto son los impuestos, los tramites documentarios con pagos en línea entre otros que en algunos países se realiza de forma electrónica y cuya acogida es creciente.

4.2. En función al medio utilizado

4.2.1. Comercio electrónico directo o comercio electrónico on-line:

Este tipo de comercio electrónico es aquel que utiliza las TICs para realizar transacciones comerciales de bienes no tangibles como por ejemplo música, videos, películas, series, software entre otros similares.

> "El comercio electrónico directo es aquel que puede perfeccionarse contractualmente y completarse la ejecución del contrato y la satisfacción de los contratantes únicamente a través de la red, utilizando solamente medios electrónicos. La entrega de bienes se produce sin soporte físico, únicamente a través de la red. Por tanto el contrato se perfecciona por medios electrónicos (título), pero también la "cosa" o, generalmente, el servicio se entregan o satisfacen electrónicamente". (Piaggi, 2001, pág. 27).

4.2.2. Comercio electrónico Indirecto o comercio electrónico off-line:

En este tipo de transacción se realizan transacciones electrónicas donde el bien es de tipo tangible. Aun cuando la transacción se realice en línea, la distribución de los productos comprados se realiza de forma presencial; por supuesto que Tiendas como

Amazon, están innovando este servicio y distribuyendo compras por medio de drones, pero aun así la entrega es directamente con el cliente, "…por lo que la ejecución de esa obligación coincide con la que tendría lugar de haberse concluido la transacción por medio del comercio tradicional". (De Miguel, 2002, pág. 45)

4.3. En Atención al entorno tecnológico en que se desenvuelve la actividad comercial.

4.3.1. Comercio electrónico abierto.

Este tipo de comercio se realiza a través de medios electrónicos, más específicamente, e internet.

4.3.2. Comercio electrónico cerrado.

En este tipo de transacción solo intervienen los que tienen acceso a la red que se utiliza. El uso de una red y sistema privado que restringe el acceso a otros usuarios, es la figura que describe este tipo de comercio.

5. Esquemas de seguridad.

En el mundo de internet se tienen usuarios de todo tipo y experiencia, pero entre ellos se puede identificar a 2 que son característicos y en este tipo se pueden integrar todos los demás. En primer lugar, se tiene al usuario que utiliza el internet para fines correctos y que no busca ver más allá de lo que le permiten los sistemas; además en este grupo se encuentran aquellos que por deseo de conocimiento buscan enlerdar como es que funciona el internet; por supuesto, que esta persona no desea hacer daño ni perjudicar a nadie, solo que busca medir los límites de lo que va conociendo. Por otro lado tenemos a aquellos que utilizan el internet como fuente de ganancia ilícita y para satisfacer sus deseos descontrolados, y para lograr su propósitos hurtan información, roban contraseñas, realizan fraudes, ingeniería social, realizan copias y ventas ilegales, etc. En este grupo también se encuentran aquellos que solo por el hecho que pueden hacerlo, destruyen fuentes de datos y ocasionan problemas a los usuarios legítimos de la red.

5.1.1. Seguridad en internet.

El internet no fue diseñado en sus comienzos con la seguridad que requiere ni se consideraron los protocolos de transmisión necesarios cuando se implementó en sus inicios, por lo tanto es una red insegura que requiere de mecanismos especiales, para poder tener cierto grado de seguridad. Con eta premisa, se sabe que las fugas de información son posibles y también comunes. Por lo tanto cuando uno realiza una transacción en internet siempre tiene ciertas dudas sobre la seguridad:

- Siendo un comprador en línea, como podría tener la seguridad que la página web a la cual estoy accediendo es en realidad la página real y no una copia creada para confundir y engañar al os usuarios.
- Siendo una tienda en línea o un vendedor el línea, como se podría tener la certeza que de que el posible cliente es quien dice ser y no un suplantador que se hace pasar por alguien más.
- En el caso de los compradores, como podría haber la seguridad de enviar mi información a través de la red sin que otra persona intervenga este envío y haga posesión

de mi información personal para realizar alguna actividad ilegal. Ante este problema se utiliza el estándar de codificación de información denominado SSL por sus siglas en inglés que permite al usuario y al vendedor establecer una conexión de transmisión de datos segura que no permite que otros intervengan en la misma.

5.1.2. Seguridad del sitio web.

Podemos identificar 4 formas de tener seguridad en internet:

- Implementar sistemas de protección en el sitio web que eviten cambios o daños en el contenido que puedan afectar a los usuarios.
- Implementar medidas que permitan mantener la integridad de los datos a través de copias de respaldo y sistemas de protección.
- Dar protección a la información que se distribuye en la red.
- Mantener con debido recelo toda la información y componentes de un sitio web para evitar las copias de estos.

Considerando que en general se tienen en cuenta los tres primeros, se debe tomar conciencia de que la información y componentes de un sitio web pueden ser utilizados para fines no legales y por lo tanto tambein debe ser protegida. A continuación se mostrarán las formas más comunes por las cuales se afecta la seguridad:

- Control de acceso físico inadecuado.
- Deficiente valoración de información importante.
- No existen medidas de prevención de pérdida de información en los equipos de cómputo.
- No existe una política de seguridad de la información en la empresa.
- Asignación de contraseñas y asignaciones de seguridad débiles o innecesarias.
- No existen registros de acceso ni pistas de auditoria.
- Pobre o inexistente capacitación del personal respecto a la seguridad.

5.1.3. Técnicas de seguridad

La seguridad de la información es una labor complicada y esta realidad se aplica especialmente para los sitios web. Por lo tanto se deben considerar ciertas técnicas y estrategias de seguridad para evitar riesgos relacionados a los sitios web. Sin embargo, una de las más efectivas, es evitar exponer información que no se pueda recuperar; además, se debe considerar que solo las personas con la adecuada autorización puedan acceder. Además, se debe tener en mente que los niveles de seguridad deben estar presente desde la construcción de un servidor o el sitio web y esta debe proseguir periódicamente.

5.1.4. Amenazas para el sitio Web

Existen amenazas que atentan contra la seguridad de la información que se encuentra en un sitio web y estas incluyen, las amenazas internas, externas y por malware.

- Cuando las amenazas se originan dentro de la empresa se les considera amenazas internas. Esto sucede por descuido de los usuarios del sistema que no bloquean sus equipos y pueden originar que un extraño manipules sus terminales para poder causar daño o lucrar on el acceso del empleado.

- Cuando existe una amenaza que se origina en la infraestructura del internet como infiltraciones de personas que pueden acceder al sistema para acceder a información privilegiada para copiarla, modificarla o eliminarla, introducir malware, etc.

- El caso de software malicioso o malware puede resultar en un serio problema de seguridad si no es controlado. Para el caso de malware, el uso de antivirus no es suficiente, se deben implementar sistemas de cortafuegos y i es posible algún otro tipo de protección para internet con la finalidad de evitar que algún tipo de malware se introduzca por la web. También se debe considerar, cualquier otro medio de acceso que pueda traer malware como usuarios que introduzcan el programa por si mismos, o acceso de extraños a los terminales, por supuesto, los tres tipos de amenazas esta relacionados.

5.1.5. Medidas de protección del sitio Web

Existen muchas formas de proteger la información que ponemos en las páginas web, pero entre las recomendadas tenemos, perímetro físico limitado para el servidor web, considerar varias capas de protección, contraseñas fuertes, control de accesos, modificaciones en las políticas de seguridad y operativas del sitio web, encriptamiento de información y monitoreo constante de os accesos físico y lógico. También se recomienda tener planes de contingencia ante emergencias y desastres y políticas referidas a las coipas de seguridad.

- **Protección de contraseña**
  Uno de los métodos más efectivos y comunes para evitar intrusiones no deseadas es el uso de contraseñas fuertes; es decir que no tengan palabras y números comunes ni consecutivos. Además, una buena práctica del uso de contraseñas es el cambio de estas periódicamente para evitar que caigan en manos inescrupulosas. Por último se debe considerar la eliminación de las credenciales de acceso de aquellos trabajadores que nos forman parte de la empresa.

- **Encriptamiento**
  El encriptamiento es la utilización de un algoritmo matemático que permita que la información sea transformada en una serie de caracteres que sean ilegibles a simple vista y solo quien tenga la clave de cifrado pueda acceder a ella. Por supuesto que existen 2 tipos de encriptación: simétrica y asimétrica. Para la simétrica, donde DES es una de las más conocidas, la clave para cifrar y descifrar es la misma, mientras que en la criptografía asimétrica, se hace uso de

una clave privada y una publica que se puede utilizar para encriptación y desencriptación; en este caso RSA es una de las más utilizadas.

- **Cambios de política ocasionales**
  Utilizar cambios repentinos es una buena manera de poder evitar problemas de seguridad. Como es bien sabido, el punto más vulnerable en todo sistema de seguridad es el lado humano que se combina con encriptamiento, las mejores contraseñas y sistemas de protección de información. Por lo tanto, los cambios son necesario porque de esta manera no se podrá prever lo que no se conoce y lo que cambia constantemente. Por otro lado, se debe seguir una línea de consistencia al trabajar con estos cambios debido a que estos cambios pueden ser negativos si no se capacita correctamente al personal con respecto a lo que le concierne.

- **Firma digital de mensajes**
  Un símbolo que ha sido creado electrónicamente es considerado una firma electrónica y se utiliza para dar validez a un documento de la misma manera que lo haría una firma hecha a mano. La firma electrónica tuvo sus inicios como una técnica de criptografía asimétrica donde se consideran la llave privada y la llave pública.

  En el Perú, el uso de firmas digitales se encuentra amparada en la Ley Nº 27269, el cual es la Ley de firmas y certificados digitales, como figura en sus artículos 3, 4 y 5. Expresamente se regula el uso de firmas digitales brindándole el mismo valor que las firmas manuscritas. Por medio de esta ley se estipula la integridad y autenticidad de los documentos electrónicos.

- **Certificado digital**
  Este documento electrónico tiene el mismo valor que un documento de identidad virtual; puesto que al ser emitido por una autoridad certificadora, da fe a que el certificado digital representa a la persona a través de su clave pública. La función primordial que cumple un cetificado digital es garantizar la validez de la llave pública; por lo tanto, debemos confirmar que la clave pública que usemos sea la misma que aparece en el certificado para evitar problemas de confidencialidad de documentos.

  El contenido de los certificados digitales es el siguiente:
  - El identificador del dueño del certificado.
  - El identificador de la entidad certificadora que emitió el certificado.
  - La forma para firma electrónica del suscriptor.
  - Periodo de vigencia, La fecha de emisión y de caducidad del certificado. Esto significa que luego de la fecha de caducidad no se debería utilizar la llave pública del certificado.
  - El número de serie o identificador único para cada certificado que emite la autoridad certificadora.

- La llave pública de la persona cuyo nombre figura en el certificado digital.
- La firma electrónica de la autoridad certificadora n cada campo del certificado para dar seguridad de su validez.

LECTURA SELECCIONADA N° 1: CONTRATOS INFORMÁTICOS

Carrión, H.D. (2002). Contratos informáticos. Disponible en: http://www.delitosinformaticos.com/ecommerce/contratos.shtml

LECTURA SELECCIONADA N° 2: GESTIÓN DE RIESGO

Lefcovich, M. (2004). La gestión de riesgo. Disponible en: http://www.degerencia.com/articulo/la_gestion_del_riesgo

LECTURA SELECCIONADA N° 3: SOBRE LA NUEVA LEY DE DELITOS INFORMÁTICOS

Montezuma Panez, O. (2013). Sobre la nueva ley de delitos informáticos. Disponible en: http://www.blawyer.org/2013/09/19/sobre-la-nueva-ley-de-delitos-informaticos/

LECTURA SELECCIONADA N° 4: EL COMERCIO ELECTRÓNICO DEBE GARANTIZAR LA SEGURIDAD EN INTERNET

Hernandez Diaz, A. (2013). El Comercio Electrónico debe garantizar la Seguridad en Internet. Disponible en: http://alfredohernandezdiaz.com/2013/06/06/seguridad-internet-protege-negocio-electronico/

ACTIVIDAD N° 1

Instrucciones

- Ingrese al foro y participe con comentarios críticos y analíticos del tema contratos informáticos; debe incluir su opinión clara y precisa sobre cuáles son los probables problemas que se presentan en los contratos informáticos. Debe sustentar su opinión.
- Para esto lea y analice el tema N° 1 y la Lectura 1
- Responda en el foro a las siguientes preguntas acerca de contratos informáticos:
  ¿Cuál es el propósito de los contratos informáticos?
  ¿Qué consideraciones generales y específicas se deben tener en cuenta antes de realizar un contrato informático en el ámbito de software? ¿Y en el de hardware?
  ¿Por qué se da énfasis a los certificados digitales y firmas electrónicas con relación a los contratos informáticos?

ACTIVIDAD N° 2

Instrucciones

1. Ingrese al foro y participe con comentarios críticos y analíticos acerca del tema de riesgos informáticos; debe incluir su opinión clara y precisa sobre cómo

se puede atenuar el impacto cuando un riesgo se concretiza; brinde ejemplos que apoyen su idea. Debe sustentar su opinión. Para esto Lea y analice el tema N° 2 y la Lectura 2

2. Responda en el foro a las preguntas acerca de riesgos informáticos:
   ¿Por qué es importante un análisis y manejo de riesgos de la información?
   ¿Cuáles cree Ud. que son los riesgos de mayor relevancia para el ámbito informático? ¿Por qué? Sustente.
   En el proceso de asegurar los bienes informáticos, ¿Qué consideraciones se deben tener en cuenta al momento de hacer el inventario de estos?

ACTIVIDAD N° 3

Instrucciones

1. Ingrese al foro y participe con comentarios críticos y analíticos acerca del tema delitos informáticos; debe incluir su opinión clara y precisa sobre la problemática actual de los delitos informáticos, en especial en el área de abuso de menores por medio del uso de las TICs; además debe proponer una solución coherente con respecto a la aplicación de la ley de delitos informáticos. Debe sustentar su opinión con ejemplos. Para esto Lea y analice el tema N° 3 y la Lectura 3; se le recomienda también investigar acerca del tema.

2. Responda en el foro a las preguntas acerca de delitos informáticos:
   ¿Por qué motivo se aprobó la ley 30096?
   ¿Cuál es la clasificación que se da con respecto a delitos informáticos?

ACTIVIDAD N° 4

Instrucciones

1. Ingrese al foro y participe con comentarios críticos y analíticos acerca del tema comercio electrónico; debe incluir su opinión clara y precisa sobre cual es la situación actual del comercio electrónico en el Perú; debe considerar ejemplos actuales para sustentar su respuesta. Para esto Lea y analice el tema N° 4 y la Lectura 4 y se le recomienda también investigar acerca del tema.
2. Responda en el foro a las preguntas acerca del comercio electrónico:
   ¿Cuáles son las implicancias de la seguridad de la información en el comercio electrónico?
   Como usuario electrónico ¿Cuáles serían algunas consideraciones a tener en cuenta l realizar una transacción comercial de índole electrónico? (Mencione 5)

GLOSARIO DE LA UNIDAD III

1. Leasing

Sistema de arrendamiento de bienes de equipo mediante un contrato en el que se prevé la opción de compra por parte del arrendatario. (Diccionariojuridico, 2016, en línea)

2. Seguro

Es una fórmula eficaz de cobertura que implica pagar una cierta cantidad por una prestación o indemnización futura en caso de que se presente una situa-

ción adversa, que en algunos casos, puede ser extrema (por ejemplo, si se incendia un coche) (Diccionariojuridico, 2016, en línea).

3. Póliza

Una póliza es la denominación que recibe aquel documento en el cual se plasma el contrato de seguro, por un lado y por el otro, las obligaciones y derechos que corresponderán tanto a la aseguradora como al asegurado, que son las dos partes intervinientes en este tipo de contrato (Diccionariojuridico, 2016, en línea).

4. Delito

Un delito es un comportamiento que, ya sea por propia voluntad o por imprudencia, resulta contrario a lo establecido por la ley. El delito, por lo tanto, implica una violación de las normas vigentes, lo que hace que merezca un castigo o pena (Diccionariojuridico, 2016, en línea).

5. Figura jurídica

Una figura jurídica es una actividad, documento o cualquier otro concepto que se encuentra contemplado en las leyes (Diccionariojuridico, 2016, en línea).

6. Bienes tangibles:

Son todos aquellos bienes físicamente apreciables, es decir, que se pueden tocar y ocupan un espacio (Diccionariojuridico, 2016, en línea).

7. Secure Sockets Layer (SSL):

Es un protocolo diseñado para permitir que las aplicaciones para transmitir información de ida y de manera segura hacia atrás. Las aplicaciones que utilizan el protocolo Secure Sockets Layer sí sabe cómo dar y recibir claves de cifrado con otras aplicaciones, así como la manera de cifrar y descifrar los datos enviados entre los dos. (Olamendi, 2015, pág. 77)

8. Secure Electronic Transaction (SET):

Es un protocolo estándar para proporcionar seguridad a una transacción con tarjeta de Identificación en redes de computadoras inseguras, en especial Internet. (Olamendi, 2015, pág. 77)

9. File Transfer Protocol (FTP)

En informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo. (Olamendi, 2015, pág. 31)

10. Data Encryption Standard (DES)

Es un algoritmo de cifrado, es decir, un método para cifrar información. (Olamendi, 2015, pág. 25)

11. Clave pública

Una clave es pública y se puede entregar a cualquier persona. (Olamendi, 2015, pág. 18)

12. Clave privada

La clave privada de carácter privado y el propietario debe guardarla de modo que nadie tenga acceso a ella. (Olamendi, 2015, pág. 18)

REFERENCIAS DE LA UNIDAD III

1. Contratos Informáticos. (2016). Del contrato informático a la firma electrónica del abogado. Disponible en: http://contratosinformaticos.com/contrato-informatico/del-contrato-informatico-a-la-firma-electronica-del-abogado/

2. Gotzone Múgica, A. (2003). Los contratos informáticos. Saberes, Vol 1. Universidad Alfonso X el Sabio, Madrid, España.

3. INEI. (2003) Guía para la administración pública sobre la elaboración de contratos informáticos. Lima, Perú, INEI

4. Dávara Rodriguez, M. (2005). Manual del derecho informático. 7ª. Ed., Arazandi.

5. Tellez, J. Derecho Informático. (2008). 4ta edición McGRAW-HILL/ Interamericana Editores, S.A.

6. RAE. (2016). Diccionario de la Real Academia de la lengua española en línea. Disponible en: http://dle.rae.es/?id=DgIqVCc

7. UNISDR. (2009). Terminología sobre Reducción de Riesgo de Desastres.

8. Frayssinet Delgado, M. (2012). Taller de Gestión de Riesgos. ONGEI

9. Sena, L., Tenzer, S. M. (2004). Introducción a Riesgo Informático

10. Callegari, N. (1985). Delitos informáticos y legislación. Oficina eficiente.

11. Davara Rodríguez, M. A. (1997). Manual de Derecho Informático. Editorial Aranzadi, Pamplona

12. Tellez Valdés, J. (1996). Los Delitos informáticos. Situación en México, Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida

13. Parker, D.B. (1976). Crime by computer, New York

14. Acurio Del Pino, S. (2000). Delitos informáticos: generalidades. PUCE

15. Huerta Miranda, M., Líbano Manzur C (1998) Los Delitos Informáticos. Editorial Jurídica Cono Sur.

16. Sieber, Ulrich. (1992). Criminalidad informática: peligro y prevención. pág. 77

17. Morant Vidal, J; (2002). Protección penal de la intimidad frente a las nuevas tecnologías. Ed. Práctica de derecho, Valencia, pág. 44.

18. De Ros, M. (2000). El Consentimiento y el Proceso de Contratación Electrónica. Derecho de Internet, contratación Electrónica y firma Digital, Aranzadi, Pamplona.

19. DAVARA & DAVARA Asesores Jurídicos. (2001). Microsoft Central Facebook: Comercio Electrónico, Aranzadi. Elcano, Navarra.

20. García Del Poyo, R. (2001). Aspectos mercantiles y fiscales del comercio electrónico. La Ley, Madrid.

21. Aparicio Vaquero, J.P. (2002). Los contratos electrónicos en el derecho español. El marco establecido por la ley de servicios de la sociedad información y comercio electrónico. Comercio electrónico. Salamanca.

22. Guisado Moreno, A. (2004). La Formación y Perfección del Contrato en Internet, Marcial Pons, Madrid.

23. Piaggi, A. (2001). El comercio electrónico y el nuevo escenario de los negocios. Instituciones de Derecho privado – Contratación contemporánea. Vol. II, Temis, Bogota.

24. Fernandez Fernandez, R. (2001). Contratación Electrónica: La prestación del Consentimiento en Internet, Bosch edit. Barcelona.

25. De Miguel Ascencio, P. (2002). Derecho Privado de Internet, 3era. Edic, Civitas, Madrid.

26. Carrión, H.D. (2002). Contratos informáticos. Disponible en: http://www.delitosinformaticos.com/ecommerce/contratos.shtml

27. Lefcovich, M. (2004). La gestión de riesgo. Disponible en: http://www.degerencia.com/articulo/la_gestion_del_riesgo

28. Montezuma Panez, O. (2013). Sobre la nueva ley de delitos informáticos. Disponible en: http://www.blawyer.org/2013/09/19/sobre-la-nueva-ley-de-delitos-informaticos/

29. Hernandez Diaz, A. (2013). El Comercio Electrónico debe garantizar la Seguridad en Internet. Disponible en: http://alfredohernandezdiaz.com/2013/06/06/seguridad-internet-protege-negocio-electronico/

30. Diccionario Jurídico. (2016). Diccionario Jurídico. Disponible en: http://www.diccionariojuridico.mx/

31. (Olamendi, G. (2015). Diccionario de informática e internet. Disponible en: http://www.internetglosario.com/

AUTOEVALUACIÓN Nº 3

1. ¿Cuál es el concepto de un contrato informático?

a. Los contratos informáticos son aquellos que tienen por objeto la contratación de un bien o servicio por correo electrónico solamente.
b. Los contratos informáticos son aquellos que permiten la búsqueda virtual de un bien o servicio informático.
c. Los contratos informáticos son aquellos que tienen por objeto la contratación de un bien o servicio informático.

d. Los contratos informáticos son aquellos que tienen por objeto la contratación de un bien o servicio.

2. ¿Cuáles son los componentes de un contrato inforrmático?

a. Contratantes, el objeto del contrato, las clausulas, anexos.
b. Contratantes, el arrendador, el arrendatario, las clausulas.
c. El notario, las clausulas, el estatuto legal, los anexos.
d. El notario, las clausulas, el objeto de contrato, los anexos

3. ¿A qué se refiere el leasing informático?

a. Es una operación que utilizan los arrendatarios de software para alquilar material temporalmente.
b. Es una operación que utilizan los empresarios y profesionales para adquirir material caro pagándolo con los beneficios que obtienen de su uso.
c. Es una operación que utilizan los profesionales de TI para publicitar su trabajo con los beneficios que obtienen de su uso.
d. Es una operación jurídica que usan los profesionales de TI para utilizar software sin realizar ningún pago.

4. ¿Cuál es la mejor definición de un riesgo?

a. La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generando ganancia para la empresa.
b. La factibilidad de que una amenaza se identifique, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generando ganancia para la empresa.
c. La factibilidad de que una amenaza se identifique, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole pérdidas o daños
d. La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole pérdidas o daños

5. ¿Cuál es la principal causa de riesgos informáticos?

a. Las políticas de la empresa
b. Los propios trabajadores
c. Los aparatos de protección ineficientes
d. Los ataques de DOS

6. ¿Cuál es la finalidad de los seguros informáticos?

a. Brindar un respaldo económico para aliviar la perdida en el sector informático
b. Dar protección a los equipos informáticos para evitar ataques
c. Dar seguridad perimetral a los equipos informáticos
d. Brindar un respaldo lógico y técnico en caso de perdida
e. Brindar protección te tipo monitoreo ante ataques de índole económico

7. ¿Cuáles son las clases de delitos informáticos?

a. Como instrumento o medio y como fin u objetivo
b. Como instrumento u objetivo y como fin o medio
c. De acceso, de ejecución y de consulta
d. De acceso, de intrusión y de ejecución

8. ¿Qué es un sujeto pasivo?

a. Se entiende como sujeto pasivo a la persona perpetra la actividad típica del sujeto activo.
b. Se entiende como sujeto pasivo a la persona titular del ataque y sobre la cual recae la responsabilidad típica del sujeto.

c. Se entiende como sujeto pasivo a la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo.
d. Se entiende como sujeto pasivo a la persona directamente relacionada con el bien atacado sobre la cual recae la responsabilidad de velar por la seguridad de dicho bien.

9. ¿Cuál es la clasificación del comercio electrónico en función al medio utilizado?

a. Comercio electrónico on-line y el comercio electrónico Off-line.
b. Comercio electrónico indirecto y el comercio electrónico Offline.
c. Comercio electrónico abierto y el comercio electrónico cerrado.
d. Comercio electrónico abierto y el Comercio electrónico On-line.

10. La siguiente definición: "Es el documento electrónico generado y firmado digitalmente por una entidad", corresponde al concepto de:

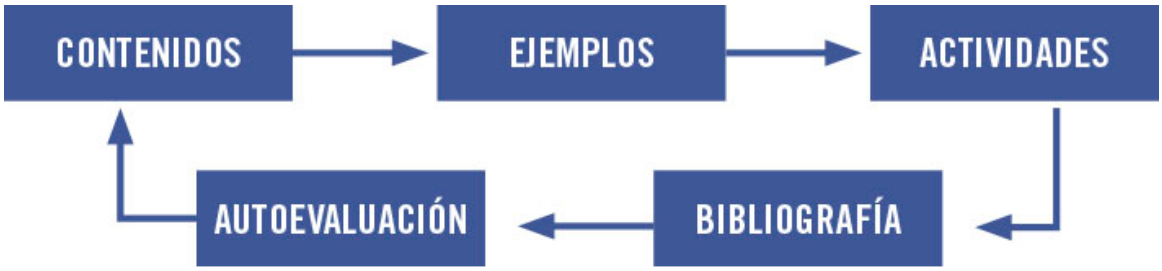
a. Firma digital.
b. Encriptamiento.
c. Cifrado de mensajes.
d. Certificado digital.

ANEXO Nº 1
Respuestas de la Autoevaluación de la Unidad 3

Número	Respuesta
1	c
2	a
3	b
4	d
5	b
6	a
7	a
8	c
9	a
10	d

UNIDAD IV: Riesgos del spam y aspectos laborales informáticos

DIAGRAMA DE ORGANIZACIÓN DE LA UNIDAD IV



ORGANIZACIÓN DE LOS APRENDIZAJES

Resultado de aprendizaje de la Unidad IV:

Al finalizar la unidad, el estudiante será capaz identificar y describir los componentes y características de lo concerniente al SPAM, teletrabajo y sus implicancias y la apreciación probatoria de documentos, demostrando conocimiento teórico de los temas.

CONOCIMIENTOS	HABILIDADES	ACTITUDES
• **Tema N° 1:** Regulación Jurídica Del Spam 3. Conceptos básicos 4. Fuentes y clasificación de SPAM 5. Ley N° 28493 • **Tema N° 2:** Implicancias del teletrabajo 1. Conceptos generales 2. Implicancias del teletrabajo 3. Ley N° 30036 • **Tema N° 3:** Sistemas de apreciación probatoria. 1. Conceptos relacionados 2. Medios de prueba 3. Sistemas de apreciación probatoria • **Tema N° 4:** Valoración probatoria documental 1. Conceptos relacionados 2. Características y clasificación de los documentos electrónicos 3. Firmas y documentos electrónicos **Lecturas seleccionadas:** • Política anti-SPAM, un caso práctico. • La regulación del Teletrabajo • Comentario a la Ley de firm@s y certific@dos digit@les, Ley Nº 27269 **Autoevaluación de la Unidad IV**	5. Interpreta la normatividad vigente sobre el manejo del SPAM. 6. Incentiva el uso del Teletrabajo en las organizaciones 7. Valora los documentos electrónicos. **Actividades Propuestas** • Los estudiantes Participan en el foro de discusión sobre regulación jurídica del SPAM. • Los estudiantes Participan en el foro de discusión sobre implicancias del teletrabajo. • Los estudiantes Participan en el foro de discusión sobre sistemas de apreciación probatoria. • Los estudiantes Participan en el foro de prueba documental **Control de lectura y/o tarea académica** Los alumnos deberán concluir las asignaciones de cada uno de los temas de esta unidad.	Asume una actitud responsable y crítica sobre las normas vigentes relacionadas al SPAM, Teletrabajo y los documentos electrónicos

TEMA N° 1: Regulación Jurídica del SPAM

Como es bien sabido, el internet ha permitido unificar países y erradicar fronteras para tener diversos tipos de tecnologías relacionadas con la información para las

comunicaciones; entre estas tecnologías, una de las más populares es el correo electrónico. Sin embargo, este medio sirve como un instrumento para que compañías mal intencionadas, en un afán de llevar su publicidad a más posibles clientes, envíen correos electrónicos no deseados, generado problemas a los usuarios de las cuentas de correo afectadas. Considerando esta realidad es importante conocer la normativa para la protección de los usuarios en caso de SPAM.

1. Conceptos básicos:

Para poder entender el tema es importante conocer componentes relacionados al mundo del SPAM y de este modo comprender sus implicancias en el derecho.

1.1. Correo electrónico

"Es todo mensaje, archivo, dato u otra información electrónica que se transmite a una o más personas por medio de una red de interconexión entre computadoras o cualquier otro equipo de tecnología similar. También se considera correo electrónico la información contenida en forma de remisión o anexo accesible mediante enlace electrónico directo contenido dentro del correo electrónico." (Ley N° 28493, 2005)

1.2. SPAM

El NACPEC nos da una definición acerca del SPAM: el spam es "el correo comercial no solicitado, generalmente enviado a las direcciones electrónicas de los consumidores sin su autorización y consentimiento; suele ser enviado por empresas de mercadeo o telemercadeo, compañías legítimas o por individuos comisionados sólo para dicho fin" (NACPEC, 2006).

1.3. SCAM

El término Junk mail (correo chatarra) o scam es utilizado para referirse a correos relacionados con publicidad fraudulenta como por ejemplo formas de enriquecerse al instante, imágenes y videos obscenos, premios de concursos, cadenas que solicitan ser renviados a otras personas con consecuencias positivas o negativas al hacerlo o no hacerlo, entre otros.

1.4. SPIM

Este concepto es muy similar al spam, puesto que este ataque cibernético, denominado spim, en vez de enviar información no requerida por el usuario a través de correos electrónicos, lo realiza por mensajería instantánea en los teléfonos celulares y aun las redes sociales.

1.5. Phishing

Esta es una nueva modalidad de fraude en internet que utiliza sitios web que se parecen a los de los bancos, sistemas de pago o u otros medios donde por lo general se señala una falla o problema, que la información ha caducado o que se tiene una oportunidad, por lo tanto, solicitan al cliente acceder a una página web por medio de un hipervínculo o enlace. Al abrirlo, se le solicita información de carácter personal como datos personales, números de cuenta de tarjeta de crédito o débito, contraseñas o PIN (número' de identificación personal), dirección, teléfono o cualquier otro tipo dc información confidencial que pueda facilitar el accionar delictivo de los planearon esto.

1.6. SPAMMERS

Son personas naturales o jurídicas (empresas) que envían los mensajes de tipo SPAM utilizando diversas técnicas para adquirir enormes listas de correos que son indispensables para llevar a cabo su actividad. Muchos de estos SPAMMERS utilizan programas automatizados que buscan direcciones de correo electrónico en diversas fuentes del internet.

1.7. Spam por ventanas emergentes (Pop ups)

Estos mensajes no solicitados emergen cuando nos conectamos a Internet o ingresamos a alguna página web en particular. Se muestran en forma de una ventana de diálogo o una ventana de navegador de internet. "Su contenido es variable, pero generalmente se trata de un mensaje de carácter publicitario que podría ser fraudulento." (AEPD, 2009).

1.8. Hoax

"Este es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena. Algunos hoax informan sobre virus, otros invocan a la solidaridad, o contienen fórmulas para ganar millones o crean cadenas de la suerte. Los objetivos que persigue quien inicia un hoax son normalmente captar direcciones de correo o saturar la red o los servidores de correo." (AEPD, 2009).

Estos son algunos conceptos relacionados al uso de mensajería en la red que utiliza en su mayoría, el correo electrónico como una herramienta de internet para promover su material nocivo y perjudicial debido a que el correo electrónico es de fácil manejo y a que no requiere equipos sofisticados. El envío indiscriminado y persistente de correo spam causa molestia en muchos usuarios, puesto que esto satura el espacio disponible en los servidores de correo electrónico, al igual que se incrementa el riesgo de infección por virus a través de algún archivo o código malicioso incrustado en el e-mail. A raíz de esto, en la actualidad se van adoptado medidas legales en distintos países con el propósito de limitar y regular esta práctica para así proteger a los usuarios.

2. Tipos de SPAM

De acuerdo al contenido que llevan consigo los correos electrónicos, Julio Tellez (2006, p. 1), nos ofrece una tipología del SPAM:

2.1. Productos

Son los correos electrónicos que ofrecen o aconsejan el uso de un determinado producto. Por ejemplo, electrodomésticos, automóviles, viajes, computadores, etc.

2.2. Financieros

Son los correos electrónicos que contienen ofertas relacionadas con el ámbito económico y financiero. Ejemplos: préstamos, oportunidades económicas, acciones, etc.

2.3. Adultos

Son los correos electrónicos que tienen o están referidos a productos o servicios dirigidos a público mayor de edad (mayores de 18 años); Estos suelen ser contenidos ofensivos o inapropiados. Ejemplos: pornografía, anuncios de servicios personales, consejos maritales, etc.

2.4. Salud

Son correos electrónicos que se relacionan con productos o servicios relacionados con la salud. Ejemplos: Medicamentos farmacéuticos, tratamiento médico, medicina alternativa, etc.

2.5. Engaños

Estos correos son contienen información falsa, intencionadamente equivocada, o de corte ilegal por parte quien lo desarrolla. Ejemplos: cadenas, fraudes piramidales, esquemas de negocio, etc.

2.6. Internet

Son los correos que ofrecen o aconsejan servicios o productos de relacionados con el Internet. Ejemplos: Diseño de páginas web, servicios de host, creación de sistemas de cómputo, software, etc.

2.7. Ocio

Son los correos relacionados con el entretenimiento; estos ofrecen premios, descuentos, cupos promocionales, ofertas, etc. Ejemplos: Viajes de vacaciones, casinos en linea, juegos, videos, etc.

2.8. Fraudes

Son correos que aparentan ser de compañías reconocidas, sin serlo. Esto es conocido como "Phising". Estos mensajes suelen contener trucos para que los usuarios de correo revelen información personal, como información financiera, contraseñas, nombres, etc. Ejemplos: Verificación de tarjetas de crédito, notificación de cuentas de banco, conflictos de usuarios con sus cuentas de servicio, etc.

2.9. Políticos

Son los mensajes de correo que aconsejan votar por un candidato político en época de campaña, piden donar dinero a un partido o a una agrupación política, ofrecen productos relacionados a la campaña electoral, etc.

2.10. Religión

Son correos electrónicos con información o servicios religiosos, evangelización o de tipo esotérico. Ejemplos: Psíquicos, Astrología, religión organizada, etc.

2.11. Otros

Son correos electrónicos de otra índole.

3. Impacto del SPAM en las empresas

Como todo tipo de amenaza en la red, se puede distinguir resultados económicos, legales y sociales negativos para la empresa causados por la llevada del SPAM en cualquiera de sus formas, estos impactos pueden generar no solo problemas temporales sino permanentes, entre ellos se pueden encontrar:

3.1. Reducción en la productividad de los empleados

Según estudios realizados por Panda software, las perdidas en productividad que el SPAM genera se genera por tener que borrar correo basura o no deseado por un tiempo insignificante en un día pero el acumulado anual es realmente por empleado y aún mayor por todos los trabajadores. Si consideramos el supuesto que eliminar un correo no deseado nos toma 10 segundos, donde en promedio se tienen 100 correos no deseados al mes, en una empresa que tiene aproximadamen-

te 1000 empleados; en promedio esto representarían casi tres horas y media de trabajo desperdiciado.

3.2. Aumento de trabajo en el área de TI

El área de Ti que contempla los trabajadores de soporte técnico, los administradores de correo electrónico y redes, deben aumentar a su trabajo asignado la responsabilidad de prevenir y de proveer a los usuarios de los sistemas formas de poder confrontar el problema del SPAM. Por su puesto, esto genera pérdidas para las empresas.

3.3. Aumento del consumo de recursos de red

La cantidad de SPAM que ingresan por las redes de las empresas repercute en los costos relacionados al soporte de red. De este modo, según Panda Software, si consideramos que tres de cada cinco correos entrantes son SPAM, esto significaría que estos ocupan las tres quintas partes de nuestro ancho de banda de conexión a internet y redes locales, nuestro servidor de correo electrónico, y de otros dispositivos relacionados en la empresa que tienen que procesar datos basura.

3.4. Riesgos de seguridad

En términos de seguridad de la información, la parte más débil de los sistemas de seguridad en las empresas es el factor humano. Los criminales informáticos utilizan también el SPAM para poder infiltrarse en las empresas y de este modo poder robar información como cuentas de acceso, contraseñas y con estas credenciales, tener acceso al sistema de la empresa debido a que algún trabajador imprudentemente decidió abrir un correo electrónico no deseado que contenía malware causando una brecha de seguridad para toda la empresa.

3.5. Riesgos legales

Como es bien sabido, la información que se incluye en los correos electrónicos no deseados contiene material publicitario, proselitista, sexual, ofensivo, violento, etc. que pueda afectar la sensibilidad de los empleados y como consecuencia, algún trabajador podría presentar una denuncia por que la empresa no le provee un entorno de trabajo agradable y digno.

4. Métodos de captura de direcciones para spam

(Sanz de las Heras, 2009) nos brinda un compendio de las tácticas más comunes que los spammers utilizan para recoger direcciones de correo electrónico se tienen:

4.1. Compra de bases de datos selectivas

“Son bases de datos de direcciones de correo-e clasificadas por temáticas de interés. Estas bases de datos son creadas por responsables web sin escrúpulos que recogen direcciones de los usuarios que pasan por su portal.” (Sanz de las Heras, 2009, p. 2)

4.2. Listas Opt-In

“Son servicios a los que cualquier se puede suscribir de forma voluntaria. Muchas veces marcando la casilla que dice “No me envíe ofertas”, al final las recibes. Evidentemente la mayor parte de las listas opt-in son legales pero hay mucho engaño e incumplimiento de lo que ellos mismos dicen y además difícil de demostrarlo.” (Sanz de las Heras, 2009, p. 2)

4.3. Páginas web

"Se utilizan bots capaces de hacer barridos en Internet o determinadas zonas para localizar miles de direcciones de correo electrónico. Los spammers los usan día y noche." (Sanz de las Heras, 2009, p. 2)

4.4. Servidores de correo-e

"Son robots que extraen direcciones de correo de los servidores de correo, simulando una transacción SMTP y preguntando si tal usuario es o no correcto. Hacen barridos automáticos de nombres de usuario con diccionarios." (Sanz de las Heras, 2009, p. 2)

4.5. Virus y códigos maliciosos

"Son virus que se propagan por correo-e consistiendo su actividad en capturar los datos de la libreta de direcciones del usuario contaminado y enviarlos determinadas direcciones para su procesamiento y almacenamiento." (Sanz de las Heras, 2009, p. 2)

5. La normativa anti SPAM en Perú, La ley N° 28493

A continuación, se mostrará en entero la Ley normativa anti SPAM en el Peru, Ley N° 28493 con vigencia desde el 12 de Julio de 2005 y modificada a través de la ley N°29246 el 24 de mayo de 2008, regula el uso del correo electrónico comercial no solicitado (SPAM) en el Perú. El contenido de la ley ha sido actualizado con las nuevas modificaciones para este estudio:

LEY QUE REGULA EL USO DEL CORREO ELECTRÓNICO COMERCIAL NO SOLICITADO (SPAM)

Artículo 1.- Objeto de la Ley

La presente Ley regula el envío de comunicaciones comerciales publicitarias o promocionales no solicitadas, realizadas por correo electrónico, sin perjuicio de la aplicación de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor.

Artículo 2.- Definiciones

Para efectos de la presente Ley se entiende por:

- **Correo electrónico:**
  Todo mensaje, archivo, dato u otra información electrónica que se transmite a una o más personas por medio de una red de interconexión entre computadoras o cualquier otro equipo de tecnología similar. También se considera correo electrónico la información contenida en forma de remisión o anexo accesible mediante enlace electrónico directo contenido dentro del correo electrónico.

- **Correo electrónico comercial:**
  Todo correo electrónico que contenga información comercial publicitaria o promocional de bienes y servicios de una empresa, organización, persona o cualquier otra con fines lucrativos.

- **Proveedor del servicio de correo electrónico:**
  Toda persona natural o jurídica que provea el servicio de correo electrónico y que actúa como intermediario en el envío o recepción del mismo.

- **Dirección de correo electrónico:**

Serie de caracteres utilizado para identificar el origen o el destino de un correo electrónico.

Artículo 3.- Derechos de los usuarios
Son derechos de los usuarios de correo electrónico:

- Rechazar o no la recepción de correos electrónicos comerciales.
- Revocar la autorización de recepción, salvo cuando dicha autorización sea una condición esencial para la provisión del servicio de correo electrónico.
- Que su proveedor de servicio de correo electrónico cuente con sistemas o programas que filtren los correos electrónicos no solicitados.
- El reenvío del correo electrónico al emisor del correo electrónico comercial no solicitado, con la copia respectiva a la cuenta implementada por el INDECOPI. Dicho reenvío será considerado como prueba de que el usuario rechaza la recepción de correos electrónicos comerciales no solicitados.

Artículo 4.- Obligaciones del proveedor
Los proveedores de servicio de correo electrónico domiciliados en el país están obligados a contar con sistemas o programas de bloqueo y/o filtro para la recepción o la transmisión que se efectúe a través de su servidor, de los correos electrónicos no solicitados por el usuario.

Artículo 5.- Correo electrónico comercial no solicitado
Todo correo electrónico comercial, promocional o publicitario no solicitado, originado en el país, debe contener:

- La palabra "PUBLICIDAD", en el campo del "asunto" (o subject) del mensaje.
- Nombre o denominación social, domicilio completo y dirección de correo electrónico de la persona natural o jurídica que emite el mensaje.
- La inclusión de una dirección de correo electrónico válido y activo de respuesta para que el receptor pueda enviar un mensaje para notificar su voluntad de no recibir más correos no solicitados o la inclusión de otros mecanismos basados en Internet que permita al receptor manifestar su voluntad de no recibir mensajes adicionales.

Artículo 6.- Correo electrónico comercial no solicitado considerado ilegal
El correo electrónico comercial no solicitado será considerado ilegal en los siguientes casos:

- Cuando no cumpla con alguno de los requisitos establecidos en el artículo 5 de la presente Ley.
- Contenga nombre falso o información falsa que se oriente a no identificar a la persona natural o jurídica que transmite el mensaje.
- Contenga información falsa o engañosa en el campo del asunto (o subject), que no coincida con el contenido del mensaje.
- Se envíe o transmita a un receptor que haya formulado el pedido para que no se envíe dicha publicidad, luego del plazo de dos (2) días. En este caso, el receptor o usuario queda expedito para

presentar su denuncia cuando reciba el correo electrónico comercial no solicitado luego de haber expresado su rechazo mediante el reenvío señalado en el literal d) del artículo 3° de la presente Ley, o por cualquier otra forma equivalente, debiendo adjuntar a su denuncia copia del correo electrónico de dicho rechazo y del nuevo correo enviado por el remitente.

Artículo 7.- Responsabilidad
Se considerarán responsables de las infracciones establecidas en el artículo 6 de la presente Ley y deberán compensar al receptor de la comunicación:

- Toda persona que envíe correos electrónicos no solicitados conteniendo publicidad comercial.
- Las empresas o personas beneficiarias de manera directa con la publicidad difundida.
- Los intermediarios de correos electrónicos no solicitados, tales como los proveedores de servicios de correos electrónicos.

Artículo 8.- Derecho a compensación pecuniaria
El receptor de correo electrónico ilegal podrá accionar por la vía del proceso sumarísimo contra la persona que lo haya enviado, a fin de obtener una compensación pecuniaria, la cual será equivalente al uno por ciento (1%) de la Unidad Impositiva Tributaria por cada uno de los mensajes de correo electrónico transmitidos en contravención de la presente Ley, con un máximo de dos (2) Unidades Impositivas Tributarias.

Para tales efectos, el usuario afectado deberá adjuntar a su demanda copia certificada de la resolución firme o consentida emitida por el órgano competente del INDECOPI, donde se establezca la ilegalidad de la conducta del remitente del correo electrónico recibido. Mientras no se expida resolución firme sobre dicha infracción se suspende el plazo de prescripción para efectos de reclamar el derecho a la compensación pecuniaria

Artículo 9.- Autoridad competente
El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI, a través de la Comisión de Protección al Consumidor y de la Comisión de Represión de la Competencia Desleal, será la autoridad competente para conocer las infracciones contempladas en el artículo 6 de la presente Ley; cuyas multas se fijarán de acuerdo a lo establecido en el Decreto Legislativo Nº 716, Ley de Protección al Consumidor, o en el Decreto Legislativo Nº 691, Normas de la Publicidad en Defensa del Consumidor, según corresponda.

Artículo 10.- Reglamento
El Poder Ejecutivo mediante decreto supremo, refrendado por el Ministro de Transportes y Comunicaciones, reglamentará la presente Ley en un plazo máximo de noventa (90) días desde su vigencia.

Artículo 11.- Vigencia
La presente Ley entrará en vigencia a los noventa (90) días de su publicación en el Diario Oficial "El Peruano."

Nota: Tomado de la ley N° 28493. Ley que regula el uso de correo electrónico comercial no solicitado (SPAM). Disponible en: http://www.inen.sld.pe/portal/documentos/pdf/normas_legales/NUEVA_leyes/2005/28042010_LEY_N_28493.pdf

TEMA N° 2: Implicancias del teletrabajo

En la actualidad, no solo las comunicaciones y la información han cambiado por el internet; existen nuevas formas de poder trabajar a distancia pero al mismo tiempo ser productivos a través de internet; este es el caso del teletrabajo, que cada día muestra cada vez más adeptos por las ventajas que ofrece. Sin embargo, existe un grupo de personas que no coindicen con este tipo de trabajo. En esta sección se presentará la modalidad del teletrabajo y sus implicancias en la sociedad y el derecho.

1. **Conceptos relacionados al teletrabajo:**

   La palabra teletrabajo tiene dos raíces, tele y trabajo; por supuesto, entender su significado no es tan complicado debido a que tele significa a distancia; de donde se puede concluir que el teletrabajo es aquel trabajo que se realiza a distancia.

   Este concepto tuvo sus orígenes en Europa en la década de los 70, donde se tenía a trabajadores con ciertas características laborando desde sus domicilios y desempeñando su labor por medios tecnológicos a una distancia considerable de su centro regular de labores. Se puede afirmar sobre el teletrabajo que este: "... consiste en desarrollar trabajos desde el domicilio particular o desde cualquier otro sitio, fuera del centro de trabajo, que no requieran la presencia física del trabajador" (Barriuso, 1996, p. 13).

   Así mismo, se considera que el teletrabajo hace uso de las TICs como herramienta productiva; en otras palabras, es utilizar las tecnologías de la información y las comunicaciones para automatizar procesos de la empresa y operarlos a distancia

   Del mismo modo, existen algunos autores que esbozan diversos conceptos para teletrabajo, por ejemplo: "Todas aquellas actividades profesionales desarrolladas a través de equipos informáticos que hacen uso del teletratamiento y la telecomunicación para enviar información en tiempo real al centro de trabajo, producción o servicios y que genera un valor añadido a sus usuarios". (No-Luis y Caballero, 1994, p. 37)

   En otras palabras, el teletrabajo es la combinación entre los sistemas informáticos de las empresas y las diferentes redes de comunicación en un ámbito laboral, con la simple finalidad de crear un espacio de trabajo en casa denominado teletrabajo, working-house o e-work, que se conceptualiza como: "…la actividad profesional desarrollada por personas –teletrabajadores– que no están presentes físicamente en la empresa para la que trabajan" utilizando, desde luego, redes de telecomunicaciones. Sin embargo debemos acotar que, según la relación contractual del teletrabajo, éste debe ser realizado por trabajadores inscritos y pertenecientes a las planillas de las empresas, bajo condiciones laborales muy especiales que analizaremos más adelante. (Núñez, 1996, p. 31)

   En nuestro país la (Ley N° 30036, 2013) menciona que "el teletrabajo se caracteriza por el desempeño de labores sin la presencia física del trabajador, denominado "teletrabajador", en la empresa con la que mantiene vínculo laboral, a través de medios informáticos, de telecomunicaciones y análogos, mediante los cuales se ejercen a su vez el control y la supervisión de las labores. Son elementos que se juntan para tipificar el carácter de esta modalidad de trabajo donde el empleador provee los medios físicos y métodos informáticos y la dependencia tecnológica y la propiedad de los resultados, entre otros." (Ley N° 30036, 2013, art. 2)

Del mismo modo se deben considerar ciertos principios que van a orientar la aplicación del teletrabajo.

1.1. Voluntariedad

Se puede efectuar el cambio del trabajo regular al teletrabajo siempre y cuando sea justificado y que el trabajador este de acuerdo con el cabio.

1.2. Reversibilidad

Si se tienen el caso que la producción del teletrabajador no es la que se espera al no poder alcanzar los objetivos, se puede volver a la modalidad de trabajo normal a solicitud del emperador.

1.3. Igualdad de trato:

Se debe promover equidad entre los trabajadores normales y los teletrabajadores para que no se afecte la productividad de ninguno.

1.4. Conciliación entre la vida personal, familiar y laboral:

El teletrabajo debe ser capaz de brindar balance entre las diferentes facetas de la vida del teletrabajador como el laboral, familiar y personal. Por lo tanto, la carga laboral dese ser asignada correctamente para no interferir con los otros ámbitos de la vida del empleado.

2. Impacto en la gestión empresarial y laboral

El teletrabajo necesariamente obliga a realizar cambios desde la pesrpectiva del derecho laboral, puesto que el cambio del lugar de trabajo conlleva a cambiar del lugar físico donde se realiza el trabajo; también, el cambio de posición del empleado con respeto su empleador al no hallarse presencialmente, “apareciendo la figura de la dependencia y supervisión virtual del trabajo. Asimismo se esfuma la forma rígida del horario laboral, pudiendo el teletrabajador programar su jornada a su conveniencia y satisfacción, concordante con los requerimientos del empleador.” (Núñez, 1996, p. 26)

Además, se brindan considerables beneficios para los trabajadores por medio del teletrabajo, debido al nivel de confort que ahora tienen el empleado, “...lo que permite una mayor calidad de vida y una elección más caprichosa del lugar de residencia y ocio... ello repercute en una mayor integración en su grupo familiar o social, con lo que se apoya y potencia la relación humana”. (Davara, 1997, p. 58).

También, se puede dar la modalidad del teletrabajo por otras razones como para padres con hijos pequeños, personas con capacidades diferentes, o que tenga algún tipo de incapacidad motriz para desplazarse a su centro de labores. Según expertos, un teletrabajador deberá contar con, “grandes dosis de autodisciplina... autoorganización...” (Armas, 2002, p. 68); para poder mantener su capacidad de producción para la empresa debido a los cambios del entorno.

Por otro lado, esto conllevaría en beneficios económicos para la empresa debido a una considerable reducción de costos, puesto que se reduciría el mobiliario, el uso de espacio físico, materiales de oficina, servicios eléctricos, telefónicos, de internet, etc.; costos que son necesarios con un trabajador de régimen normal. A esto se le suma la posibilidad de seleccionar al personal que se desee tener trabajando desde casa y por este motivo, tener una reorganización de la empresa con una visión de futuro.

3. Requisitos del teletrabajo

El Decreto Supremo N° 009-2015-TR, reglamento de la Ley N° 30036 se estipula que el contrato, designación y acuerdos del teletrabajo deben darse por escrito y contemplando los requisitos mínimos del teletrabajo y con copia al trabajador considerando y especificando lo siguiente:

- El tipo de tecnología de la información y as comunicaciones y los equipos que se utilizarán como parte del trabajo y quien los proveerá.
- Si se diera el caso de que sea el empleador quien brinde estos euipos, se debe estipular claramente el uso adecuado del mismo, las limitaciones y responsabilidades inherentes y la forma de devolución cuando terminen las relaciones laborales.
- Si los equipos fueran provistos por parte de trabajador, debe considerarse la cantidad económica que el empleador debe pagar por el uso del mismo.
- El empleador debe especificar la forma en la cual se respetará la política de seguridad de la empresa al utilizar las TICs como parte de su trabajo.
- El tipo de jornada laboral que establezca el empleador y los objetivos que debe alcanzar el teletrabajador según ley.
- La forma en cómo se pueda supervisar al teletrabajador y como este debe dar reportes de su avance en el trabajo según la actividad de que realice.

Si se gestiona un cambio de la modalidad presencial del trabajo a un teletrabajo, se deberá especificar en el documento la razón por la cual se realiza el cambio y que es lo que se desea alcanzar por medio de este cambio. Asi mismo, cualquier otra modificación debe constar por escrito y en consideración de la normativa actual vigente, siempre respetando en todo momento la información esencial que establece la ley.

4. Ventajas y desventajas del teletrabajo

El tema de teletrabajo es una situación reciente en el mundo y aún más en Sudamérica. Por lo tanto la experiencia ha dado luz sobre sus principales ventajas y desventajas:

4.1. Ventajas:

4.1.1. Ventajas para el trabajador

Por medio del teletrabajo se alcanza un nivel de flexibilidad laboral en relación a las actividades que se realizan y los horarios en que estas se realizan. Esto le permite al teletrabajador organizar su tiempo de la forma que él disponga, generar una actitud más responsable sobre su propio trabajo, por ende aumentar su productividad. Esto conlleva a armonizar mejor la relación entre el trabajo y el ámbito familiar del teletrabajador. El teletrabajo permite que los empleados puedan pasar más tiempo con su familia y también desempeñar actividades como el cuidado de los hijos, y otras personas dependientes de ellos como personas con cierta discapacidad o ancianos según sea el caso.

4.1.2. Ventajas para las empresas

Muy aparte del ahorro económico y financiero que representa para la empresa el tener la modalidad del teletrabajo, puesto que, según estudio, esto representa entre un 50 a un 70% de ahorros para las empresas, también se cuenta con un incremento en la flexibilidad para estas empresas cambiando los modelos tradicionales de empresas donde los niveles jerárquicos desaparecen y dan lugar a una estructura horizontal que se basa en los objetivos para medir la productividad puesto que el tiempo que debe dedicar depende ahora del trabajador para cumplir con sus metas. Algunas ventajas que esto conlleva son:

- Aumento de la productividad de los empleados.
- Internacionalización de las empresas.
- Posicionamiento en el mercado más estable.
- Ahorro significativo de costos fijos y variables para las empresas.
- Trabajo de mejor calidad.
- Ahorro en costos relacionados con a la atención al cliente.
- Condiciones de trabajo y calidad de vida más aceptables.
- Mayor capacidad de contratación de personal.

4.1.3. Ventajas para la sociedad.

Entre las ventajas más significativas del teletrabajo se tienen una importante reducción de tráfico y contaminación ambiental y sonora en horas punta Por este motivo, en Europa y los Estados Unidos se busca promover políticas que incentiven el cambio al teletrabajo por estas ventajas para el ambiente. Asimismo, se tiene un considerable incremento de personas que no podían trabajar en el pasado a la fuerza laboral del país; esto habla muy bien de la inclusión e igualdad de las personas. Este grupo incluye personas con habilidades diferentes, personas con niños pequeños, mujeres embarazadas, entre otros.

4.2.Desventajas del teletrabajo

4.2.1. Desventajas para las personas

Entre las desventajas que se tienen en el teletrabajo se evidencia la soledad que puede experimentar un teletrabajador debido a la falta de comunicación e interacción directa con otros trabajadores que puede representar un aumento de emociones como las soledad y aislamiento. También, se da el caso de que un teletrabajador sienta que por no estar a la vista de sus jefes, no podrá tener un ascenso en comparación de sus colegas que si están en la oficina central. Además, se tiene que no todos los trabajadores pueden hacer distinción entre su familia y su lugar de trabajo, lo que conllevaría a tener una productividad menor o que la influencia de uno sobre el otro sea contraproducente. También, podría generar una carencia de respeto a las figuras de autoridad de la empresa al no tenerlos presentes en su nuevo lugar de trabajo.

4.2.2. Desventajas para las empresas

Una de las más grandes desventajas para las empresas es el costo relacionado con el equipo e infraestructura que pueda requerir para que se implemente un lugar de trabajo completamente funcional desde el hogar; además, que no todas las empresas y compañías podrían ser capaces de implementar el teletrabajo debido a la naturaleza de su empresa, salvo por los trabajos informáticos y muchos de oficina. Se deben considerar 3 aspectos para la implementación del teletrabajo:

- Acceso y utilización adecuada de las TICs.
- Un sistema administración y control debidamente adecuado para el caso.
- Formas de trabajo basadas en objetivos y metas o que conlleven proyectos

4.2.3. Desventajas para la sociedad

En el ámbito de la sociedad, la principal desventaja del teletrabajo se refleja en las diferencias jurídicas y legislativas que existen en los diferentes países.

5. Modalidades del teletrabajo

Teniendo en cuenta el lugar de donde se desarrolla el teletrabajo, podemos identificar diversas modalidades:

5.1. Teletrabajo en casa

- **Empleados:** Utilizan sus hogares como centro de trabajo a través de un contrato con la empresa.
- **Empresarios:** Personas que deciden inicar su empresa desde la comodidad de su hogar.
- **Freelance o autoempleado:** son las personas que ofrece servicios profesionales en particulares proyectos desde su hogar.

5.2. Teletrabajo en oficinas remotas

- **Centros de recursos compartidos:** En un solo lugar, se llevan a cabo diversas actividades que guardan relación con el teletrabajo y se disponen de equipos relacionados a las TICs adecuados para este fin. En otras palabras es posible realizar teletrabajo desde un lugar que no sea precisamente la casa de alguien, pero al mismo tiempo le brinde la libertad de proveer servicios profesionales a otros en diversas partes del mundo

- **Telecentros u oficinas satélites:** Estos lugares están acondicionados para un tipo de teletrabajo donde se realizan actividades relacionadas entre sí con el fin de cumplir un solo propósito. Esto significa que una empresa tienen oficinas distribuidas geográficamente en diversos lugares, pero trabajan conjuntamente.

- **Telecottages:** Este tipo de teletrabajo se implementa en zonas rurales con la finalidad de llevar progreso a zonas de difícil acceso mediante servicios o productos que ellos puedan brindar desde esos puntos.

5.3. Teletrabajo móvil

Este tipo de teletrabajo contempla un constante movimiento de los trabajadores en lugar de tener un domicilio de teletrabajo estable. Esto lo hace a través de dispositivos móviles y del uso del internet; usual-

mente se utilizan servicios VPN (red privada virtual) para tener acceso a recursos de sus compañías o en el caos de freelancers, lo hacen a través de cuentas en internet

6. La legislación Peruana y el teletrabajo

A continuación se hará referencia completa de la (Ley N° 30036, 2013) que fue aprobada el 15 de mayo del 2013 y contempla los siguientes lineamientos.

Ley que regula el teletrabajo

Artículo 1. Objeto de la Ley
La presente Ley tiene por objeto regular el teletrabajo, como una modalidad especial de prestación de servicios caracterizada por la utilización de tecnologías de la información y las telecomunicaciones (TIC), en las instituciones públicas y privadas, y promover políticas públicas para garantizar su desarrollo.

Artículo 2. Definición de teletrabajo
El teletrabajo se caracteriza por el desempeño subordinado de labores sin la presencia física del trabajador, denominado "teletrabajador", en la empresa con la que mantiene vínculo laboral, a través de medios informáticos, de telecomunicaciones y análogos, mediante los cuales se ejercen a su vez el control y la supervisión de las labores. Son elementos que coadyuvan a tipificar el carácter subordinado de esta modalidad de trabajo la provisión por el empleador de los medios físicos y métodos informáticos, la dependencia tecnológica y la propiedad de los resultados, entre otros.

Artículo 3. Reglas sobre el uso y cuidado de los equipos
Cuando los equipos sean proporcionados por el empleador, el teletrabajador es responsable de su correcto uso y conservación, para lo cual evita que los bienes sean utilizados por terceros ajenos a la relación laboral.

Cuando el teletrabajador aporte sus propios equipos o elementos de trabajo, el empleador debe compensar la totalidad de los gastos, incluidos los gastos de comunicación, sin perjuicio de los mayores beneficios que pudieran pactarse por acuerdo individual o convenio colectivo. Si el teletrabajador realiza sus labores en una cabina de Internet o en un equipo proporcionado por terceras personas, el empleador asume los gastos que esto conlleva. El reglamento establece la forma como se efectuará esta compensación de condiciones de trabajo.

Artículo 4. Carácter voluntario y reversible del teletrabajo
Por razones debidamente sustentadas, el empleador puede variar la modalidad de prestación de servicios a la de teletrabajo, previo consentimiento del trabajador.

El cambio de modalidad de prestación de servicios no afecta la naturaleza del vínculo laboral, la categoría, la remuneración y demás condiciones laborales, salvo aquellas vinculadas a la asistencia al centro de trabajo. Sin perjuicio de lo dispuesto en el primer párrafo, el teletrabajador puede solicitar al empleador

la reversión de la prestación de sus servicios bajo esta modalidad. El empleador puede denegar dicha solicitud en uso de su facultad directriz.

El empleador puede reponer al teletrabajador a la modalidad convencional de prestación de servicios que ejecutaba con anterioridad si se acredita que no se alcanzan los objetivos de la actividad bajo la modalidad de teletrabajo.

Artículo 5. Derechos y obligaciones laborales
El teletrabajador tiene los mismos derechos y obligaciones establecidos para los trabajadores del régimen laboral de la actividad privada. Pueden utilizarse todas las modalidades de contratación establecidas para dicho régimen. En todos los casos, el contrato de trabajo debe constar por escrito.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Teletrabajo en el régimen laboral público
Las entidades públicas sujetas al régimen laboral del Decreto Legislativo 276, Ley de bases de la carrera administrativa y de remuneraciones del sector público, y a regímenes especiales, se encuentran facultadas para aplicar la presente norma cuando así lo requieran sus necesidades. El reglamento establece las cuotas mínimas de personal sujeto a esta modalidad, de acuerdo a las necesidades de cada entidad.

SEGUNDA. Plazo para establecer políticas públicas de teletrabajo
Dentro de los noventa (90) días hábiles de entrada en vigencia de la presente Ley, el Ministerio de Trabajo y Promoción del Empleo formula las políticas públicas referidas al teletrabajo para garantizar su desarrollo y su preferente utilización a favor de las poblaciones vulnerables, para lo cual coordina con la Autoridad Nacional del Servicio Civil (SERVIR), con la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), con el Consejo Nacional para la Integración de la Persona con Discapacidad (CONADIS) y con la Comisión Multisectorial para el Seguimiento y Evaluación del Plan de Desarrollo de la Sociedad de la Información en el Perú (CODESI).

TERCERA. Financiamiento en las entidades del Estado
Las acciones a cargo de las entidades del Estado de los diferentes niveles de gobierno, que se deban implementar para el cumplimiento de lo dispuesto en la presente norma, se financian con cargo a sus respectivos presupuestos institucionales, sin demandar recursos adicionales al Tesoro Público.

CUARTA. Reglamentación
El Ministerio de Trabajo y Promoción del Empleo, mediante decreto supremo, reglamenta la presente Ley en un plazo máximo de noventa (90) días hábiles desde el inicio de su vigencia.

Nota: Tomado de la Ley que regula el teletrabajo. Disponible en: http://www.trabajo.gob.pe/normaCompletaSNIL.php?id=2940

TEMA N° 3: Sistemas de apreciación probatoria

Con el avance innegable de la tecnología en los diferentes aspectos de la vida ha mudado el concepto de prueba documental que ha sufrido modificaciones necesarias en su concepción y aceptación. En estos días, los administradores de justicia y las legislaciones se ven superadas por la tecnología. La tecnología avanza día tras día, mientras que el derecho tiene un paso más lento, por lo que se hace necesario contar con medidas legales que permitan resolver problemas relacionados con la tecnología. Por esta razón los administradores de justicia deben estar preparados en temas de valoración documentaria electrónica para dar solución a conflictos donde se quiere recudir y poco a poco eliminar el uso de papel para los procesos.

1. Conceptos Preliminares

1.1. Prueba

Capitant, define a la prueba como la, “demostración de la existencia de un hecho material, o de un acto jurídico en las formas admitidas por la ley; o medio empleado para hacer la prueba”. Se entiende como la razón, instrumento, argumento u otro medio que se usa para mostrar y hacer patente la verdad o falsedad de algo y más concretamente, la justificación de la verdad de los hechos controvertidos en un juicio. (Enciclopedia Omeba, 1995, p. 729).

1.2. Teoría General de la Prueba

La Teoría General de la Prueba se ha definido, al igual que la Teoría General del Proceso, como como una vertiente derivada de la unidad fundamental del proceso que requiere de una prueba específica para cualquier forma de proceso, "siempre que en ella se distingan aquellos puntos que por política legislativa, ya que no por razones de naturaleza o función, pueden estar regulados de diferente manera en uno u otro proceso" (Devis Echeandia, 2000. P. 16).

1.3. Concepto Procesal de Prueba

La prueba, en su sentido más genérico, es entendida como "un hecho supuestamente verdadero que se presume debe servir de motivo de credibilidad sobre la existencia o inexistencia de otro hecho" (Bentahm, 1971, p. 21). Ahora bien, si se toma la perspectiva del ámbito jurídico procesal se podrá definir la prueba, "como el conjunto de motivos o razones, que de los medios aportados se deducen y que nos suministran el conocimiento de los hechos, para los fines del proceso" (Devis Echeandia, 2000. P. 20-21). También se podrá decir que es, "El conjunto de las normas jurídicas que regulan el proceso de fijación de los hechos controvertidos, constituye, pues, la institución jurídica de la prueba” (Carnelutti, 200, p. 44).

1.4. Medios Probatorios

Hinostroza A. da una definición al respecto como, "los instrumentos que emplean las partes u ordena el magistrado de los que se derivan o generan...las razones que conducen al Juez a adquirir certeza sobre los hechos" (Hinostroza, 1999, p. 16). Así también Paredes P. refiere que, "Técnicamente, el medio probatorio es la manifestación formal del hecho a probar; es la descripción, designación o representación mental de un hecho" (Paredes, 1997, p. 153).

1.5. Objeto de Prueba

Un objeto de prueba lleva la idea del hecho que sucede en un tiempo y lugar específicos, que hacen referencia a la hipótesis normativa que se

esbozó; por este motivo, Paredes P. afirma que, "Concluyentemente el hecho ocurrido es tanto objeto de la hipótesis de incidencia, como objeto de la prueba, o mejor dicho de los medios de prueba" (Paredes, 1997, p. 160).

1.6. Fuente de prueba

Una fuente de prueba se describe como aquel hecho es utilizado por un administrador de justicia con la finalidad de poder confirmar veracidad de lo que se quiere demostrar. Hinostroza menciona que "Se entiende por fuente de la prueba a la información obtenida gracias a los medios probatorios, teniendo una existencia autónoma en relación al proceso" (Hinostroza, 1999, p. 17). También, Carnelutti hace una distinción entre fuente de prueba y medios de prueba de esta manera: "...llamo por mi cuenta medio de prueba a la actividad del juez mediante la cual busca la verdad del hecho a probar, y fuente de prueba al hecho del cual se sirve para deducir la propia verdad" (Carnelutti, 200, p. 70-71).

1.7. Finalidad de la Prueba

La finalidad de la prueba es sin duda tener por cierto si existen o no los hechos que las partes vinculadas afirman, por este motivo se debe hacer uso de las presunciones y los medios probatorios. El Artículo 188 del Código Procesal Civil indica claramente que cada uno de los medios de prueba debe poder confirmar lo que las partes afirman y ayudar a los administradores de justicia a poder tomar decisiones correctas basadas en estas. Cabe aclarar que se tienen en cuenta los medios de prueba, mas no la prueba, lo que resulta absurdo en razón que los medios de prueba tan solo son instrumentos del derecho, mientras que la prueba en sí, es capaz de dar la seguridad al administrador de justicia. Al respecto, Verger Grau afirma que la finalidad de la prueba, "es la de obtener afirmaciones instrumentales depuradas para poder compararlas con las afirmaciones fácticas de las partes" (Verger Grau, 2003, p. 502).

1.8. Etapas Probatorias

1.8.1. Ofrecimiento

Es labor de las partes el proveer los medios probatorios para poder defender su posición con respecto al caso; de esta forma, es estará cumpliendo por lo estipulado por el Artículo 196 del Código Procesal Civil, que menciona que es responsabilidad de las partes proveer las pruebas necesarias que acrediten o contraigan lo que la otra parte afirma.

1.8.2. Admisión y Procedencia

La labor de declarar si un medio probatorio se considera procedente o admisible o en su defecto improcedente e inadmisible, le corresponde al juez, quien considera los principios de idoneidad, pertinencia y utilidad de estos medios. Esto quiere decir que si los medios probatorios son adecuados, relevantes para el caso en particular y si ayudarán al juez a tomar decisiones especificas al considerarlas.

1.8.3. Actuación

Para la actuación se consideran ciertos criterios establecidos por ley como el modo, el tiempo y lugar específicos y la presencia del juez. También se tiene personas que interactúan con los

medios probatorios como los abogados, los testigos, las partes, peritos especialistas e incluso el juez.

1.8.4. Valoración

La valoración de medios probatorios es tarea del Juez, quien sopesa dichos medios de forma vinculante. Se explicará el tema de forma más profunda en la siguiente sección.

1.8.5. La Valoración de la Prueba

Devis Echeandía H. menciona que, "por valoración o apreciación de la prueba judicial se entiende la operación mental que tiene por fin conocer el mérito o valor de convicción que pueda deducirse de su contenido" (Devis Echeandia, 2000. P. 141). Paredes P. nos dice que, "la apreciación o valoración es acto del juez consistente en medir la eficacia probatoria de cada medio de prueba, o de su conjunto, según el precio o valor que le asigna la ley o le otorgue el juez, en relación al grado de convicción que permita generar certeza en el juez de la ocurrencia del hecho a probar" (Paredes, 1997, p. 305). Asimismo, Carrión Lugo menciona que, "Podemos sostener válidamente que la apreciación y valoración de los medios probatorios constituye la fase culminante de la actividad probatoria. Es el momento también en que el Juez puede calificar con mayor certeza si tal o cual medio probatorio actuado tiene eficacia para convencerlo sobre los hechos alegados y si ha sido pertinente o no su actuación en el proceso" (Carrión Lugo, 2000, p. 52).

2. La prueba y sus formalidades

Si bien es cierto, los documentos actuales han hecho un cambio radical en el estilo de pruebas que se tienen; sin embargo, no se puede dejar de lado la raíz de la prueba del derecho tradicional para poder entender los documentos probatorios electrónicos Además, se deben conocer los distintos sistemas de apreciación probatoria que se irán adaptando a los modelos electrónicos puesto que tienen una base en los documentos de papel que reconoce el derecho.

3. Evolución de los Medios de Prueba

Los medios de prueba como tales tienen tres etapas muy marcadas:

3.1. La expositiva, polémica o postulatoria

En esta etapa se expresan las demandas por parte de las partes, en estas demandas se considera la descripción de los hechos en su contexto y se hace alusión a las leyes y normas que amparan su caso ante el administrador de justicia.

3.2. Probatoria o demostrativa

En esta etapa, se realiza un esfuerzo conjunto por poder probar los hechos presentados anteriormente por parte del juez y las partes. Es en esta etapa donde se proveen los medios probatorios para poder apoyar la posición de cada uno; luego se decide su admisión o inadmisión según ley.

3.3. Conclusiva

Para dar conclusión al proceso, ambas partes presentan su conclusiones y alegatos finales en relación a todos los medios probatorios presentados; posteriormente, es el juez quien, a través de la sentencia,

expresa su decisión basado en la veracidad de los medios probatorios presentados. Así se concluye la primera instancia del proceso.

4. Diferentes Medios de Prueba

A continuación veremos cómo (Tellez, 2008) distribuye los principales medios de prueba:

4.1. Confesional

"Es una declaración que contiene el reconocimiento de un hecho de consecuencias jurídicas desfavorables para el confesante." (Tellez, 2008, p. 286).

4.2. Documental

"También llamada literal, es la que se hace por medio de documentos en la forma establecida en las leyes procesales." (Tellez, 2008, p. 286).

4.3. Pericial

"Se deriva de la apreciación de un hecho por un observador con preparación especial obtenida mediante el estudio de la materia a que se refiere o simplemente por la experiencia personal." (Tellez, 2008, p. 286).

4.4. Testimonial

"Dada por los testigos como aquellas personas que comunican al juez el conocimiento que posee acerca de determinado hecho (o hechos) cuyo esclarecimiento interesa para la decisión de un proceso." (Tellez, 2008, p. 286).

4.5. Inspección judicial

"Consiste en un examen directo por el juez de la cosa mueble o inmueble sobre la que recae para formar su convicción concerniente al estado o situación en que se encuentra al realizarla (ésta se puede llevar a cabo fuera o dentro del juzgado)." (Tellez, 2008, p. 286).

4.6. Fama pública

"Estado de opinión acerca de un hecho que se prueba mediante el testimonio de personas que la ley considera hábiles para este efecto." (Tellez, 2008, p. 286).

4.7. Presuncionales

"Operaciones lógicas mediante las cuales, a partir de un hecho conocido, se llega a la aceptación como existente de otro desconocido o incierto." (Tellez, 2008, p. 286).

5. Sistemas de apreciación probatoria

5.1. Sistema de libre apreciación o convicción

Conocido también bajo los nombres de prueba racional, libre convicción y apreciación razonada. Carrión Lugo menciona que en estos casos, "el juzgador tiene libertad para apreciar las pruebas actuadas de acuerdo a las reglas de la lógica, a las reglas de la experiencia, a su propio criterio racional de apreciación, a su observación crítica, a sus propios conocimientos psicológicos y alejado, naturalmente, de la arbitrariedad" (Carrión Lugo, 2000, p. 53).

5.2. Sistema de la prueba legal o tasada

En este tipo de sistema, el juez tiene la facultad y responsabilidad de medir cuan eficaz es un medio probatorio según las normas. Por lo tanto, este sistema obliga "al juez a reglas abstractas preestablecidas, que le señalan la conclusión que forzosamente debe aceptar en presencia o por la ausencia de determinados medios de prueba" (Devis Echeandia, 2000. P. 64).

5.3. Sistema de la sana crítica

Es entendido sistema de sana crítica a las "pautas racionales fundadas en la lógica y la experiencia que hacen de la valoración judicial la emisión de un juicio formalmente válido (en tanto respeta la leyes lógicas del pensamiento) y argumentativamente sólido (en tanto apoyado en la experiencia apuntala la convicción judicial) que demuestra o repite, en los autos, la convicción formada en base a aquéllas" (Paredes, 1997, p. 312).

5.4. Sistema mixto

Según dicho sistema, el legislador contempla y regula ciertos aspectos mientas que otros se dan facultad al juzgador. En este tipo de sistema se da cierta libertad de apreciación, sin embargo, siempre habrá predominancia del legislador.

TEMA N° 4: Valor probatorio de los documentos electrónicos

El cambio del uso de papel al uso de documentos electrónicos ha generado un nuevo desafío para el derecho por temas como la firma de dichos documentos y la veracidad de los mismos. Es por eso, ante un innegable cambio progresivo en la documentación virtual y su efecto en el derecho y legalidad de los mismos, se hace necesario una nueva perspectiva de los documentos electrónicos y su valor probatorio considerado las implicancias que esto pueda tener para el derecho y sus ramas afines. Por lo tanto, un nuevo campo en el derecho y nuevas regulaciones son necesarias ante este nuevo fenómeno.

1. El concepto del documento electrónico en el derecho informático

Para entender que es un documento electrónico, es necesario definir que es un documento puesto que si se considera su origen etimológico latino, documentum unido al vocablo docere, se entiende como un escrito que se enseña.

El diccionario de la lengua de la Real Academia Española nos dice sobre documento, “un diploma, carta relación u otro escrito que ilustra acerca de un hecho, principalmente de los históricos. Cualquier cosa que sirve para ilustrar o comprobar algo (RAE, 2016).

Para el curso, debemos definir a la palabra documento desde la perspectiva legal, si comenzamos a partir del derecho tradicional consideraremos que es una escritura o papel que contiene aseveraciones de voluntad.

Coture E. describe al documento de la siguiente forma: “un objeto por su contenido, en cuyo texto se consigna o representa alguna cosa apta para establecer un hecho o se deja constancia de una manifestación de voluntad que produce efectos jurídicos, no siendo necesaria la utilización del lápiz y papel, sino basta que se haya fijado en un soporte posible de ser comunicado a terceros.” (Coture, 1955 p. 34).

Así también, Núñez J. dice que el documento es un instrumento o medio que puede ayudar a probar los hechos dentro de un proceso; así también, un do-

cumento “es un acto humano perceptible que puede servir de prueba de los hechos de un proceso. Estas definiciones nos permiten establecer las principales características del documento” (Nuñez, 1996, p. 22).

En concepto de documento electrónico varía con respecto al concepto tradicional puesto que ya no se utiliza papel en él; en todo caso, e remplaza por la codificación de bits que pueden ser percibidos, para los humanos, a través periféricos de un ordenador como una impresora, monitor, parlantes, etc.

Considerando este cambio, se podrá definir el documento informático como el que abarca todo o cualquier elemento que haya sido elaborado a través o con el uso del computador, pudiendo muchos de ellos conocerse en su contenido en forma directa, sin necesidad de recurrir a equipo o máquina especial por estar contenidos en soportes tradicionales o de acceso directo al hombre, que se pueda leer y en cuya memoria se mantiene el original con caracteres totalmente distintos al que el periférico o soporte que lo contiene.

En la opinión de algunos entendidos en la materia, no existe alguna diferencia entre documentos electrónicos o en papel, puesto que la única diferencia que hay entre los 2 es la presentación y el estado físico del mismo, mientras que en uno se util9iza papel, en el otro se hace uso de medios metálicos y plásticos.

Por lo tanto, el documento electrónico tiene es un como documento que almacena un lenguaje lingüístico en forma de bits. Esta información en forma de bits puede ser codificada, registrada, almacenada, procesada, y transmitida y cuya característica más primordial es su duración. Obviamente, estos criterios están siendo recientemente aceptados por el ámbito legal para que pueda regularse su uso.

Ahora bien, entendiendo la naturaleza del documento electrónico, se afirmará que este documento es simplemente una nueva manera de existir del documento escrito debido a que de la misma forma que un documento tradicional, el electrónico contiene un mensaje cualesquiera almacenado en lo que se denomina, sistema analógico, microformas o sistema binario, dentro de cintas, películas y discos magnéticos, unidades extraíbles que pueden ser transmitidos y comunicados a otras personas y al mismo tiempo pueden permanecer con el paso del tiempo.

Además, según el Decreto Legislativo 681, se hace válida la utilización tecnologías que ayudan a la generación, almacenamiento y distribución de documentos electrónicos tales como la micrograbación, que abarca procesos como la creación de microformas de tipos como la microforma imagen que es una versión compacta del original, el microduplicado el cual es una copia fiel del original y el microarchivo que es el archivo de todos los elementos en forma de microforma. Habiéndose aceptado su uso, su valor legal y probatorio es también innegable.

Del mencionado Decreto Legislativo 681, en su capítulo V, artículo 14, se dice que las empresas de derecho privado pueden organizar sus archivos ellas mismas mediante las tecnologías de las microformas que trata esta ley, teniendo en cuenta los requisitos de ser supervisadas por la Superintendencia de Banca o por la Comisión Nacional Supervisora de Empresas y Valores CONASEV, pudiendo ser empresas dedicadas al comercio electrónico.

Ahora bien, se debe aclarar la diferencia entre un documento electrónico y un documento digital. Un documento electrónico podría estar almacenado o ser reproducido utilizando un tipo de tecnología similar como fotocopiadora, scanner, fax, etc. Mientras que un documento digital solo es posible producirlo o copiado por un ordenador.

2. Características

Dentro del ámbito jurídico se deben tener en cuenta ciertas características que le dan al documento electrónico la validez apropiada:

2.1. Inalterabilidad.

Uno de las dificultades para dar un valor correcto en términos de eficacia a los documentos probatorios es el nivel de permanencia para dichos documentos; esto debido a existir el riesgo de que dichos documentos puedan ser modificados de alguna manera utilizando medios informáticos y por lo tanto la importancia de las firmas electrónicas.

2.2. Autenticidad.

EL concepto de autenticidad cobra sentido solo si el documento no tiene ninguna modificación en su contenido con respecto del original; por supuesto, si no se ha alterado, entonces es auténtico. El nivel de seguridad de un documento dependerá en cuán difícil sea de cambiarlo o alterarlo y al mismo tiempo, debería ser fácil de identificar si se ha realizado una modificación.

2.3. Durabilidad.

Se dice que un documento es durable si permanece sin cambio con respecto del original y que no solamente tienen permanencia en el tiempo sino también que no puede ser modificado en el tiempo. Como es sabido, el papel es un material en el cual se podría tener un documento que es difícil de alterar; sin embargo, el papel puede sufrir algún otro daño y perder su propiedad de durabilidad; por lo se busca de los documentos electrónicos que sean capaces de durar en el tiempo.

2.4. Seguridad

El tema de la seguridad de los documentos electrónicos tiene que ver con su autenticidad y la dificultad que pueda existir con respecto a generar copias. Considerando los avances en el uso de criptografía para el cifrado de los documentos, se ha logrado tener un equivalente al documento tradicional firmado en papel.

En el caso de documentos, se necesitan las firmas de las partes en el ámbito jurídico, donde la firma es una representación gráfica de la identidad de la persona, su conformidad ante un actuado, su declaración de voluntad o su autoría según fuera el caso.

En el caso de una firma digital, la idea es en cierto modo la misma, aunque esta no tiene el mismo valor legal en sí misma. Por lo cual se utilizan otras técnicas como la criptografía y la biometría para suplir estas carencias; indudablemente, estas nuevas tecnologías le dan a la firma digital el valor de una firma manuscrita al aparecer al finalizar un documento electrónico porque acepta el mismo y le da un sentido de conformidad.

3. Clasificación

Si consideramos que el documento electrónico está representado por ceros y unos, es decir en lenguaje de ordenador y que necesita de periféricos de computadora para poder mostrarse entendibles la ser humano, han de distinguirse ciertas clases de documentos electrónicos de acuerdo con (Giannantonio, 1987) los documentos electrónicos pueden ser clasificados así:

3.1. Documento formado por la computadora

En este tipo de documentos se utilizan diversos instrumentos tecnológicos para poder determinar el contenido de la voluntad de una persona. Es decir, no solo es un documento redactado en computadora, sino que por medios electrónicos como la firma electrónica, expresa la voluntad en el mismo documento de forma electrónica y que tiene validez en el ámbito electrónico de los ordenadores.

3.2. Documento formado por medio de la computadora

En este tipo de documento electrónico, no es creado como en el caso anterior sino que se encarga de hacer la comprobación de los documentos contenidos en dispositivos de almacenamiento. Estos documentos, están contenidos en dispositivos de almacenamiento extraíbles y que solo pueden ser leídos por un ordenador.

Desde el punto de vista de como se conserva los documentos electrónicos tenemos:

3.2.1. De carácter volátil

Son los documentos que se encuentran termporalmente almacenados en memoria RAM, que como sabemos, solo almacenan información mientras se le suministre energía eléctrica.

3.2.2. Permanentes

Son los documentos que se encuentran almacenados en algún tipo de dispositivo que no es volátil como discos duros, cintas magnéticas, etc. Donde la única manera de que desaparezcan es si se les borra del dispositivo.

3.2.3. Inalterables

Son los documentos que una vez creados no pueden ser cambiados y solo se pueden leer. En esta clasificación tenemos las memorias ROM que son de solo lectura, CDs y DVDs que no sean regrabables.

4. Valor probatorio del documento electrónico

En el Perú, a partir del año 1991, se ha empezado a dar valor a los documentos electrónicos creados y almacenados en medios electrónicos. Según la Ley 25323 y su Reglamento Decreto Supremo D.S. 008-92-JUS, artículo 2 se contemplan las funciones del Sistema Nacional de Archivos y en su inciso d) menciona lo siguiente: “fomenta la investigación científica y tecnológica a través de los fondos documentales, con el objeto de poder preservar el patrimonio documental a través del archivo de los documentos mediante el uso de tecnologías como la micrograbación.” Esto hace referencia a que en nuestro país ya se tenían aspiración de utilizar la tecnología para los medios probatorios desde ese tiempo. También vemos que el Decreto Legislativo 681, da validez a la utilización de diversos tipos de tecnologías para poder almacenar documentos a través del uso de microformas que fueron usadas en sus inicios por los bancos y empresas privadas. (Castellares, 1992, p. 187).

Con la legislación actual se puede afirmar que el uso de los documentos electrónicos en nuestro país se encuentran reconocidos y que además, se ha puesto en marcha un proyecto de disminución de documentos impresos en papel por un tema medio ambiental y de ahorro de recursos. Del mismo modo, la implementación del DNI electrónico que contempla la firma digital, permitirá también el uso de los documentos electrónicos en otras esferas como la comercial, contractual, documentaria y legal.

Con respecto al valor probatorio de estos documentos, es la entidad certificadora la encarga de dar fe a las firmas electrónicas que se es da a las personas a través del certificado digital y que también tiene valor legal en nuestro país. En el caso legal, son los administradores de justicia los encargados de poder dar la validez de los medios probatorios documentarios electrónicos tan igual como se realizó por muchos años con los documentos en papel.

4.1. La Firma Digital

La firma digital es un conjunto de caracteres que se añaden a un documento electrónico para dar conformidad y aceptación al documento o expresar autoría por el mismo. Si se desea firmar un documento electrónicamente y que esto evite modificaciones posteriores, se debe utilizar la llave publica (tecnología basada en criptografía asimétrica de llave privada y pública) de la persona que firma el documento para que luego no se pueda negar que fue la persona quien firmó el documento. Entre las peculiaridades que se deben considerar en la firma digital tenemos:

- La firma digital se debe generar cifrando el código de verificación del mensaje o documento que se desee firmar haciendo uso de la llave privada de la persona que posea el certificado digital.
- A cada titular le corresponde una única firma digital y por lo tanto, cada documento electrónico puede ser verificable al utilizar la clave pública de la persona.
- El firmado digital está bajo responsabilidad de la persona titular del certificado digital.
- Se adhiere al documento electrónico de tal manera que cualquier alteración al documento o a la firma puedan detectarse de forma rápida.

Por otro lado, aquel que es titular del certificado electrónico y por ende de la firma digital, tiene las siguientes obligaciones:

- Brindar, bajo su propia responsabilidad, brindar información clara y veraz.
- Crear su propia clave privada y firmar de forma digital todos los requisitos que establece la autoridad certificadora.
- Guardar en completo privado y bajo su responsabilidad su clave privada.
- Tener en consideración las disposiciones de la autoridad certificadora con respecto al uso de su certificado y firma digital.

En nuestro país, el uso de firmas y certificados digitales se encuentra normado y regulado por la Ley 27269 y su reglamento que nos brindan la información necesaria con respecto al uso de los mismos; por lo tanto, se recomienda su lectura.

4.2. Las Entidades Certificadoras

Considerando el crecimiento de la sociedad de la información y por ende del comercio electrónico, se ha previsto también un incremento en la utilización de firmas digitales; por lo tanto, la existencia de una entidad encargada de salvaguardar la información relacionada a las personas que poseen las firmas electrónicas a través de un certificado digital emitido por estas es inevitable y necesario; estas entidades llevan el nombre de autoridades certificadoras.

Paez Pereira M. nos dice que las autoridades certificadoras son, "aquellas empresas nacionales o extranjeras que otorgan firmas digitales o certificados digitales, generados por medios electrónicos seguros descritos en la reglamentación de la ley, a quienes se les faculta para suspender o revocar dichos documentos digitales cuando no cumplan los requisitos de ley." (Pereira, 2000, p. 94).

Por lo tanto, son estas autoridades, las encargadas de conservar un registro de la información concerniente a claves públicas de forma pública a través del internet para que una empresa pueda emitir certificados a sus trabajadores y un gobierno lo haga con sus ciudadanos, etc.

Como ya se mencionó, la Ley 27269, Ley de firmas y certificados digitales, menciona lo referente a los certificados y firmas digitales y en su artículo 12, se menciona que las autoridades certificadoras son las encargadas de emitir o derogar los certificados digitales, y de velar por el correcto funcionamiento del sistema de certificados y firmas digitales.

Según el reglamento de firmas y certificados digitales, en su artículo 4, se nos da información con respecto a la entidad certificadora de nuestro país y nos dice que es una persona de tipo jurídico que brinda servicios de generación, administración, cancelación y verificación de certificados digitales, así como otros servicios relacionados. Por supuesto, entre sus obligaciones están la de velar por la confidencialidad de toda la información que mantiene con la excepción de una orden judicial, dar facilidades para realizar certificaciones cruzadas cuando una autoridad extranjera necesita hacer algún trámite o viceversa entre otros relacionados a esta actividad.

4.3. El Certificado Digital Vigencia y Supervisión

El D.S. N-019-2002 –JUS en su artículo 4 nos brinda una definición acera de los certificados digitales; según este artículo se entiende como certificado digital al documento electrónico emitido y firmado por una autoridad certificadora relaciona una llave publica con una persona natural o jurídica atribuyéndole identidad tal cual lo haría una partida de nacimiento o un documento de identidad físico. Para el uso en el exterior de los certificados digitales, se establecen certificaciones cruzadas que permiten que un certificado se reconozca en otros países. Si se requiere un certificado digital en nuestro país, se deberá considerar lo siguiente:

- Si se trata de una persona natural, se debe tener completa capacidad de los derechos civiles
- Si se trata de una persona jurídica, se debe acreditar que dicha persona exista y que tenga vigencia actual según lo contemplan los reglamentos relacionados.

La vigencia de los certificados digitales de suma importancia debido a su valor y alcance debido a que existe responsabilidad atribuida con respecto al uso del mismo solo a partir del a fecha de emisión y hasta la fecha de caducidad. En el Perú, la Ley N° 27269, no expresa cual es el tiempo de vigencia de los certificados digitales, pero si menciona que los certificados digitales deben tener una fecha de emisión y de caducidad contenidos en este mismo.

4.4. Revocación, Cancelación y Limites del Certificado Digital

Si se da el caso que un certificado electrónico no cumple con lsu funciones inherentes, o pone en riesgo algún procedimiento o transacción comercial, este certificado debe ser revocado; lo que significa que debe perder su validez desde la fecha de su revocación.

"De acuerdo a la ley de Utha, la División del Departamento Comercial del Estado de Utha cumple las funciones de Entidad Certificadora por excelencia, de conformidad al artículo 104 de la referida ley, donde dentro de sus funciones específicas conferidas puede revocar los certificados, según lo legislado para las autoridades certificadoras acreditadas." (Ruiz Barriouso, 1998, p. 126)

En el Perú, la Ley N° 27269, en su artículo 9, menciona que se puede solicitar la cancelación del certificado digital si es solicitado por el titular de la firma electrónica, si se la autoridad certificadora lo revoca, si caduca el certificado o si la entidad certificadora deja de operar.

LECTURA SELECCIONADA N° 1: POLÍTICA ANTI-SPAM, UN CASO PRÁCTICO

Publiperu. (2015). Política anti-SPAM, un caso práctico. Disponible en: http://publiperu.pe/spam.html

LECTURA SELECCIONADA N° 2: La regulación del Teletrabajo

Ugaz, M. (2013). La regulación del teletrabajo. Disponible en: http://www.ius360.com/privado/laboral/la-regulacion-del-teletrabajo/

LECTURA SELECCIONADA N° 3: Comentario a la Ley de firm@s y certific@dos digit@les, Ley Nº 27269

Guzmán Cobeñas, M. P. (2006). Comentario a la Ley de firm@s y certific@dos digit@les. Disponible en:
http://www.derechoycambiosocial.com/RJC/Revista8/comercio.htm

ACTIVIDAD N° 1

Instrucciones

1. Ingrese al foro y participe con comentarios críticos y analíticos del tema Regulación Jurídica del SPAM; debe incluir su opinión clara y precisa sobre como el SPAM es involucrada de su vida y situación particular. Debe sustentar su opinión con ejemplos claros de su vida cotidiana. Además debe incluir que acciones debería tomar ante esto

Para esto Lea y analice el tema N° 1 y la Lectura 1

2. Responda en el foro a las siguientes preguntas acerca de la Regulación Jurídica del SPAM:

   ¿Cuál es el objetivo del SPAM?

   ¿Cuál es la finalidad de la ley N° 28493?

   ¿Por qué piensa que no se escuchan muchas denuncias sobre el tema de SPAM en el país?

ACTIVIDAD N° 2

Instrucciones

1. Ingrese al foro y participe con comentarios críticos y analíticos acerca del tema implicancias del teletrabajo; debe incluir su opinión clara y precisa sobre su perspectiva del teletrabajo como oportunidad y como problema para nuestro país. Debe sustentar su opinión con ejemplos claros. Para esto lea y analice el tema N° 2 y la Lectura 2
2. Responda en el foro a las preguntas acerca del Protección de datos personales:

   ¿Cuáles son las implicancias del teletrabajo para el profesional de sistemas?

   ¿Para qué profesiones o empleos se implementaría el teletrabajo de forma eficaz en el Perú? Dé 3 ejemplos y explique.

ACTIVIDAD N° 3

Instrucciones

1. Ingrese al foro y participe con comentarios críticos y analíticos acerca del tema valoración probatoria de documentos electrónicos; debe incluir su opinión clara y precisa sobre la realidad actual de nuestro país sobre el tema de firmas digitales y documentos electrónicos; que es lo que está haciendo el gobierno para poder trabajar con esta nueva tecnología. Debe sustentar su opinión. Para esto lea y analice los temas N° 3 y 4 y las lectura 3 y 4 y se le recomienda investigar acerca del tema.

GLOSARIO DE LA UNIDAD IV

1. Junk mail

Junk mail significa Correo basura. Junk mail es cualquier tipo de mensaje de e-mail considerado basura, como pueden ser los spams u otros correo basura. (Olamendi, 2015, p. 19)

2. Bot

Un bot, también conocido como sistema experto, es un programa de computadora diseñado para emular ciertas actitudes humanas; este puede estar diseñado para cumplir tareas muy básicas como recordar alguna tarea o automatizar algún proceso, también existen bots con programación más compleja que buscan realizar actividades que conllevan toma de decisiones, estas decisiones son tomadas a partir de filtros o parámetros que el programador incluye en el código de programación. (Olamendi, 2015, p. 7)

3. Compensación pecuniaria

Es un tipo de compensación que involucra dinero o relacionado al dinero. (Diccionariojuridico, 2016, en línea)

4. INDECOPI

INDECOPI (Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual) es una entidad de servicios con marcada preocupación por fomentar una cultura de calidad para lograr la plena satisfacción de sus clientes: la ciudadanía, el empresariado y el Estado. (INDECOPI, 2016)

5. Teleinformática

Este vocablo se refiere a la rama de la ciencia que estudia la transmisión y comunicación de información mediante vía de equipos informáticos. (Diccionariojuridico, 2016, en línea)

6. Multilocalización

Es un concepto que lleva consigo la idea de estar en varios lugares a la vez. En el tema de teletrabajo, se considera la labor que realizan personas desde diferentes puntos. (Diccionariojuridico, 2016, en línea)

7. Cifrado

es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) transforma un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo. Las claves de cifrado y de descifrado pueden ser iguales (criptografía simétrica), (criptografía asimétrica) o (Criptografía híbrida). (Olamendi, 2015, p. 9)

8. Encriptación informática

Es la codificación la información de archivos o de un correo electrónico para que no pueda ser descifrado en caso de ser interceptado por alguien mientras esta información viaja por la red. (Olamendi, 2015, p. 13)

9. Microformas digitales

Son una figura jurídica con un alto componente informático, creada en el Perú para que las imágenes de los documentos digitalizados tengan el mismo valor probatorio que un documento en papel. (Diccionariojuridico, 2016, en línea)

10. Sistema binario

Llamado también sistema diádico en ciencias de la computación, es un sistema de numeración en el que los números se representan utilizando solamente dos cifras: cero y uno (0 y 1). Es uno de los que se utilizan en las computadoras, debido a que estas trabajan internamente con dos niveles de voltaje, por lo cual su sistema de numeración natural es el sistema binario (encendido 1, apagado 0). (Olamendi, 2015, p. 39)

REFERENCIAS DE LA UNIDAD IV

1. Agencia Española de Protección de Datos. (2009). Guía para la lucha contra el spam.
2. Tellez, J. (2007). Regulación del SPAM en México. Disponible en: http://www.razonypalabra.org.mx/anteriores/n49/bienal/Mesa%205/JulioTellez.pdf
3. Panda Software. (2006). SPAM, ¿Cómo proteger a los usuarios de su empresa? Panda Software, SL. Disponible en: http://www.psiquiatria.com/imgdb/archivo_doc44.pdf
4. Sanz de las Heras, J. (2009) Evaluación de alternativas para reducir el spam. Disponible en: https://www.rediris.es/mail/abuso/doc/MedidasAntiSPam.pdf
5. La ley N° 28493 (2005). Ley que regula el uso de correo electrónico comercial no solicitado (SPAM). Disponible en: http://www.inen.sld.pe/portal/documentos/pdf/normas_legales/NUEVA_leyes/2005/28042010_LEY_N_28493.pdf
6. No-Luis y Caballero. (1994). Volumen I. III Congreso Iberoamericano de Informática y Derecho. Mérida, España.
7. Barriuso Ruiz, C. (1996). Interacción del Derecho y la Informática. Madrid, Editorial DYKINSON.
8. Núñez Ponce, J. (1996). Derecho Informático. Marsol Perú Editores S. A.
9. Ley N° 30036. (2013). Ley que regula el teletrabajo. Disponible en: http://www.trabajo.gob.pe/normaCompletaSNIL.php?id=2940
10. Davara Rodríguez, M. (1997). Informática y derecho. Navarra, Editorial Aranzandi.
11. Armas Morales, C. (2002). Sistemas de Contratación por medios electrónicos. Trabajo de Investigación F. D. Unidad de Post Grado, UNMSM. Lima-Perú.
12. Enciclopedia Jurídica Omeba. (1995). Tomo XXIII, Pres-Razo, Argentina, p.729.
13. Devis Echeandia, H. (2000). Compendio de la Prueba Judicial. Tomo I. Rubinzal-Culzoni Editores. Buenos Aires.
14. Bentahm, J. (1971). Tratado de las Pruebas Judiciales. Volumen I. Ediciones Jurídicas Europa-América. Buenos Aires.
15. Carnelutti, F. (2000). La Prueba Civil. 2º Edición. Ediciones Depalma. Buenos Aires.
16. Hinostroza, A. (1999). La Prueba en el Proceso Civil. 2º Edición. Gaceta Jurídica Editores. Lima.
17. Paredes, P. (1997). Prueba y Presunciones en el Proceso Laboral. ARA Editores. 1º Edición. Lima.
18. Verger Grau, J. (2003). Disposiciones generales de la prueba, prueba de interrogatorio de partes y testigos, en Revista Peruana de Derecho Procesal VI.
19. Carrión Lugo, J. (2000). Tratado de Derecho Procesal Civil. Volumen II. Editora Jurídica GRIJLEY. 1º Edición. Lima.
20. Ovalle Favela, J. (2005). Teoría General del Proceso, 6ª. Ed., México, Oxford.
21. Tellez, J. Derecho Informático. (2008). 4ta edición McGRAW-HILL/ Interamericana Editores, S.A.
22. Couture, E. J. (1955). Vocabulario jurídico. Montevideo, Uruguay.
23. Nuñez Ponce, J. (1996).Derecho Informático. Lima. Editorial Marsol.
24. Del Piazzo, C. E. y otros. (1984). Introducción a la Informática Jurídica y Derecho Informático. Montevideo.
25. Giannantonio, E. (1987). "El valor jurídico del documento electrónico" en informática y Derecho (Aportes de doctrina internacional). Dcpalma.

26. Castellares Aguilar, R. (1992). Los Documentos y los Títulos Valores Electrónicos. Primera Edición ECOFRAF E.I.R.LTDA. Lima.
27. Paez Pereira, M. (2000). Revista Electrónica de Derecho Informático.
28. Ruiz Barriuso, C. (1998). La Contratación Electrónica. Editorial Dykinson, S.L. Madrid.
29. Publiperu. (2015). Política anti-SPAM, un caso práctico. Disponible en: http://publiperu.pe/spam.html
30. Ugaz, M. (2013). La regulación del teletrabajo. Disponible en: http://www.ius360.com/privado/laboral/la-regulacion-del-teletrabajo/
31. Guzmán Cobeñas, M. P. (2006). Comentario a la Ley de firm@s y certific@dos digit@les. Disponible en: http://www.derechoycambiosocial.com/RJC/Revista8/comercio.htm
32. Diccionario Jurídico. (2016). Diccionario Jurídico. Disponible en: http://www.diccionariojuridico.mx/
33. (Olamendi, G. (2015). Diccionario de informática e internet. Disponible en: http://www.internetglosario.com/

AUTOEVALUACIÓN Nº 4

1. ¿Qué es el SPAM?

e. Es un filtro de protección ante correo electrónico no deseado.
f. Es correo comercial no solicitado, generalmente enviado a las direcciones electrónicas de los consumidores sin su autorización y consentimiento
g. Es una nueva tecnología que utiliza correo electrónico para generar ataques de denegación de servicios.
h. Es una forma de utilizar solo los correos electrónicos para poder generar conciencia social con respecto a problemas actuales

2. Es una forma de obtención de direcciones de correo electrónico para SPAM

a. Un virus de computadora que infecta el sistema operativo
b. La manipulación ilegal de bases de datos dentro de una empresa por los propios usuarios.
c. La compra de bases de datos de obtenidas ilegalmente.
d. El uso de bots para rastrear los archivos de computadora sin acceso internet.

3. Este tipo de SPAM muestra informacion muestra anuncions de servicio personal y consejos matrimoniales.

a. Adultos
b. Salud
c. Ocio
d. Fraudes

4. Según nuestra legislación peruana cuales son las modalidades de teletrabajo:

a. Teletrabajo en casa, oficina y televillage.
b. Teletrabajo en forma completa y mixta.
c. Teletrabajo en casa, oficina y mixta.
d. Teletrabajo en casa, oficina, televillage, móvil y compleja.

5. ¿Cuáles son los principios que rigen el teletrabajo?

a. Voluntariedad, protección de datos e igualdad de trato.
b. Reversibilidad, legalidad, continuidad e irrenunciabilidad de derechos.
c. Igualdad de trato, continuidad y razonabilidad.

d. Voluntariedad, reversibilidad, igualdad de trato y conciliación entre la vida personal, familiar y laboral.

6. ¿Es verdadero con respecto a la prueba?

a. Se define como demostración de la existencia de un hecho real, o de un acto jurídico en las formas admitidas sin considerar la ley.
b. Se define como demostración de la existencia de un hecho ficticio, o de un acto jurídico en las formas admitidas sin considerar la ley.
c. Se define como demostración de la existencia de un hecho material, o de un acto jurídico en las formas admitidas por la ley.
d. Se define como demostración de la inexistencia de un hecho material, o de un acto jurídico en las formas admitidas por la ley.

7. ¿Cuáles son las caratectristicas esenciales del documento electrónico ?

i. Durabilidad, legal, eficaz y valido.
j. Inalterabilidad, autenticidad, durabilidad y seguridad.
k. Confiabilidad, sensibilidad, objetividad y validez.
l. Aplicabilidad, autenticidad y eficacia.

8. ¿Qué entidad supervisa los certificados digitales?

e. Sunarp.
f. Reniec.
g. Sunat.
h. Indecopi.

9. ¿Qué es una firma digital?

a. Un bloque de caracteres que acompaña a un documento, que acredita quién es su autor
b. Un bloque de trazos siempre ilegibles que acompaña a un documento.
c. Un bloque de caracteres que acompaña a un documento, que acepta la no legitimidad del documento
d. Un bloque de caracteres alfanuméricos en bits codificados que acompaña a un documento, que acepta la legitimidad del documento

10. ¿Cuál es la ley que ampara las firmas digitales en el Perú?

a. la Ley 127269
b. la Ley 2726
c. la Ley 27269
d. la Ley 27299

ANEXO Nº 1
Respuestas de la Autoevaluación de la Unidad 4

Número	Respuesta
1	b
2	c
3	a
4	b
5	d
6	c

7	b
8	d
9	a
10	c