Tema 4. Conceptos básicos y marco legal de la actividad del profesional informático

Una cosa no es justa por el hecho de ser ley.
Debe ser ley porque es justa. (Montesquieu)

La revolución informática origina un gran problema de regulación jurídica. El aparato legislativo, la mayoría de las veces, no consigue ir a la misma velocidad que las tecnologías de la información. A pesar de ello, el profesional informático, como cualquier otro profesional, realiza su labor en el marco de las normativas legales que le puedan afectar en el ejercicio de su profesión. En este capítulo se introduce los aspectos básicos de dicho marco legal y las principales leyes relacionadas con su ámbito de actuación. También se revisa la responsabilidad civil que puede recaer sobre los informáticos por los daños causados a terceros. Finalmente, se tratan los delitos informáticos desde el punto de vista legislativo.

1. Introducción

El derecho informático no existe como tal; se refiere al conjunto de normas que regulaban otros aspectos y que pueden aplicarse también a la informática. Pero existe además un conjunto de normas cada vez mayor que sí tratan aspectos informáticos exclusivamente.

Para el informático de hoy en día, es imprescindible tener unos conocimientos mínimos del Derecho que va a regular los aspectos relacionados con su profesión. La regulación fragmentaria no ayuda en absoluto. Y a otro nivel, también se le va a plantear al informático muchos problemas éticos a los que tendrá que encontrar solución.

Antes de adentrarnos en el marco legal del profesional informático, vamos a tratar algunos conceptos básicos sobre el derecho.

1.1. Conceptos básicos

Según la concepción del Estado que se acepte, variará sustancialmente la visión del derecho: si el Estado es el organismo establecido por una clase dominante para mantener su dominio, el derecho será el aparato normativo destinado a organizarlo y a protegerlo; si, por el contrario, se acepta un Estado armonizador e integrador de unos grupos sociales no incompatibles, el derecho será sustancialmente idéntico en toda la sociedad, siendo este el aparato normativo destinado a evitar las luchas internas y a establecer la sociedad "armónica". En ambas visiones queda claro su carácter normativo, en este sentido en el RAE queda definido como "conjunto de principios y normas, expresivos de una idea de justicia y de orden, que regulan las relaciones humanas en toda sociedad y cuya observancia puede ser impuesta de manera coactiva".

Y ¿quién será el encargado de definir dicho conjunto de principios y normas? Pues quien o quienes ostenten el poder legislativo. El legislador elige y decide por medio de la ley qué conducta va a exigir, qué derechos va a conceder a personas, grupos o asociaciones, cómo organizará la sociedad y sus componentes en el terreno económico, social y político.

En España, la constitución de 1978 establece la división de poderes: Poder ejecutivo, poder legislativo y poder judicial. El gobierno ejerce el poder ejecutivo (aplicación de las leyes), las cortes generales ejercen la potestad legislativa (elaboración de las leyes), y los jueces y tribunales el poder judicial (administran justicia aplicando las normas jurídicas). Se trata por tanto de las cortes generales las encargadas del poder legislativo, las cuales están formadas por el congreso de diputados y el senado.

La jerarquía en el conjunto de leyes es:

1. Ley fundamental: En España es la Constitución, que regula el régimen básico de derechos y libertades de los individuos y organiza a los poderes e instituciones políticas. Está por encima de cualquier ley.

2. Leyes orgánicas y ordinarias: Las leyes orgánicas se diferencian de las ordinarias ya que las primeras son las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución. La aprobación, modificación o derogación de las Leyes orgánicas exigirá mayoría absoluta del Congreso, en una votación final sobre el conjunto del proyecto.

3. Decreto-ley: En caso de extraordinaria y urgente necesidad, el Gobierno podrá dictar disposiciones legislativas provisionales que tomarán la forma de Decretos-leyes y que no podrán afectar al ordenamiento de las instituciones básicas del Estado, a los derechos, deberes y libertades de los ciudadanos regulados en la Constitución, al régimen de las Comunidades Autónomas, ni al derecho electoral general. Los Decretos-leyes deberán ser inmediatamente sometidos a debate y votación de totalidad al Congreso de los Diputados, convocado al efecto si no estuviere reunido, en el plazo de los treinta días siguientes a su promulgación. El Congreso habrá de pronunciarse expresamente dentro de dicho plazo sobre su convalidación o derogación, para lo cual el Reglamento establecerá un procedimiento especial y sumario. Durante el plazo establecido en el apartado anterior las Cortes podrán tramitarlos como proyectos de Ley por el procedimiento de urgencia.

4. Disposiciones reglamentarias: Los reglamentos (reales decretos y órdenes ministeriales) emanan del poder ejecutivo (el real decreto del consejo de ministros, y las órdenes ministeriales de los diferentes ministerios), y no pueden contradecir lo dispuesto en las leyes.

Es necesario destacar que existe legislación supranacional producto de la cesión de soberanía nacional para llevar a cabo acciones comunes (o una acción unificada) entre un conjunto de países. En el caso de la Unión Europea surge un traspaso de poderes al consejo, la comisión y el parlamento europeo que tienen iniciativa legislativa. Se distingue entre reglamento, directiva y decisión. Los reglamentos son normas jurídicas emanadas de las instituciones europeas que poseen efecto directo en los países miembros, y que prevalecen sobre el Derecho nacional. Las directivas contienen unos objetivos que los países deben cumplir en un determinado periodo de tiempo, y cada país transcribe la directiva a su propia legislación según sus propios criterios. Por último, la decisión también posee un efecto directo, pero en este caso tienen un carácter más administrativo y van dirigidas a destinatarios precisos.

La constitución prevé y regula la cesión de ciertos aspectos del ejercicio de la soberanía a organismos internacionales. Y en este sentido, los tratados internacionales válidamente celebrados, una vez publicados oficialmente en España, forman parte del ordenamiento interno.

1.2. Marco legal del profesional informático

En el conjunto de leyes existentes en nuestro ordenamiento jurídico que puedan afectar de manera destacada a la actividad del profesional informático, destacan las siguientes:

- Ley de protección de datos
- Ley de propiedad intelectual
- Ley de servicios de la sociedad de información
- Ley de acceso electrónico de los ciudadanos a los servicios públicos

Por la importancia de las dos primeras leyes, se dedican los siguientes dos capítulos a abordarlas con más profundidad. Los dos siguientes apartados nos introducen la Ley de servicios de la sociedad de la información y la Ley de acceso electrónico de los ciudadanos a los servicios públicos.

2. Ley de servicios de la sociedad de la información

La Ley de servicios de la sociedad de la información[1] surge para incluir en nuestra legislación una directiva europea relativa a determinados aspectos de los servicios de la sociedad de la información[2].

En esta ley se entiende por servicios de la sociedad de la información o servicios: todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros, y siempre que representen una actividad económica, los siguientes:

- La contratación de bienes o servicios por vía electrónica
- La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales
- La gestión de compras en la red por grupos de personas
- El envío de comunicaciones comerciales
- El suministro de información por vía telemática

[1] Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y el Comercio Electrónico.
[2] Directiva 2000/31/CE.

El prestador de servicios estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

- Nombre o denominación social
- Domicilio
- Dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva
- Datos de su inscripción en el Registro Mercantil u otro registro público en el que se encuentren inscritos para la adquisición de personalidad jurídica o a los solos efectos de publicidad
- En el caso de actividad regulada, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión
- El número de identificación fiscal
- Al referirse a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío o en su caso aquello que dispongan las normas de las Comunidades Autónomas con competencias en la materia
- Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente

2.1. Responsabilidades

Respecto a las responsabilidades, los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley.

Los operadores de redes de telecomunicaciones y proveedores de acceso a una red de telecomunicaciones que presten un servicio de intermediación que consista en transmitir por una red de telecomunicaciones datos facilitados por el destinatario del servicio o en facilitar acceso a esta no serán responsables por la información transmitida, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos.

Los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios no serán responsables por el contenido de esos datos ni por la reproducción temporal de los mismos, si:

- No modifican la información
- Permiten el acceso a ella solo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita
- Respetan las normas generalmente aceptadas y aplicadas por el sector para la actualización de la información

- No interfieren en la utilización lícita de tecnología generalmente aceptada y empleada por el sector, con el fin de obtener datos sobre la utilización de la información, y

- Retiran la información que hayan almacenado o hacen imposible el acceso a ella, en cuanto tengan conocimiento efectivo de lo siguiente: que ha sido retirada del lugar de la red en que se encontraba inicialmente; que se ha imposibilitado el acceso a ella, o que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella.

Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que:

- No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

- Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

La responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:

- No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

- Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

2.1.1. Comunicaciones comerciales y contratación vía electrónica

Las comunicaciones comerciales vía electrónica deben ser claramente identificables como tales (indicando publicidad o publi). Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

Un elemento fundamental en esta Ley es el contrato electrónico, entendido como: todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones. Los contratos realizados por vía electrónica se equiparan con los contratos tradicionales. Tras la recepción de la aceptación del contrato, se debe enviar una confirmación de dicha recepción.

2.1.2. Infracciones y sanciones

Las infracciones se clasifican como muy graves, graves y leves.

Se trata de una infracción muy grave el incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, cuando un órgano administrativo competente lo ordene.

Son infracciones graves entre otras:

- No facilitar información sobre su denominación, domicilio o modo de comunicación directa y efectiva
- El envío masivo de comunicaciones comerciales por correo electrónico cuando en dichos envíos no se cumplan los requisitos establecidos
- La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados

Entre las infracciones leves se encuentra principalmente el incumplimiento de la obligación de informar de los diferentes aspectos que establece la ley.

Las sanciones son de 150.001 hasta 600.000 euros para infracciones muy graves, de 30.001 hasta 150.000 euros para infracciones graves y de hasta 30.000 euros para infracciones leves.

3. Acceso electrónico de los ciudadanos a los servicios públicos

Los términos "administración electrónica" y "acceso electrónico" tienen a confundirse. De hecho, ha sido derogada la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos ante la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público) que integra en su contenido a la misma. No se pretende hacer un estudio exhaustivo de ambas leyes, sino tan solo reseñar lo más significativo para el ejercicio profesional en el campo de las TIC.

Conviene pues empezar a definir qué es eso de "Administración electrónica". Tomando la definición de la Comisión Europea diremos que "La Administración electrónica es el uso de las TIC en las AAPP, combinado con cambios organizativos y nuevas aptitudes, con el fin de mejorar los servicios públicos y los procesos democráticos y reforzar el apoyo a las políticas públicas".

Hubo un tiempo en que para dar idea de "novedoso", se añadía un prefijo ("E-") a todo lo que queríamos definir como electrónico: del correo al comercio, pasando por la administración, e incluso democracia o gobierno. Hoy, buena parte de nuestra sociedad ha asimilado como algo habitual el uso de las tecnologías de la información y la comunicación. Los accesos a Internet, los mensajes por correo electrónico, mensajería, las redes sociales… provocan que lo que era excepcional pase a ser no solo usual sino prácticamente el único camino a recorrer.

Nuevos tiempos, nuevos conceptos y nuevas formas de trabajar, para conseguir ese prefijo "e" que anticipa modernidad y que ahora vemos acompañado de palabras como administración, gobierno, democracia o comercio. (Almonacid & Moreno, 2015). Así, la Ley no se llama "del procedimiento electrónico", por resultar redundante, es algo que va implícito, como en una supuesta "Ley para la defensa de la infancia de los niños y niñas". Precisamente, una de las razones principales que llevan a la derogación de las leyes 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento administrativo Común y la 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos con su consecuente sustitución por las leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público es precisamente el impulso definitivo a la Administración electrónica.

Abundemos: el procedimiento no solo debe ser electrónico, sino que además se debe procurar que sea lo más simple y menos burocrático posible. Recurramos de nuevo al texto de la ley 39/2015 (art. 1.2) donde se apunta la simplificación de trámites:

"Solo mediante ley, cuando resulte eficaz, proporcionado y necesario para la consecución de los fines propios del procedimiento, y de manera motivada, podrán incluirse trámites adicionales o distintos a los contemplados en esta Ley. Reglamentariamente podrán establecerse especialidades del procedimiento referidas a los órganos competentes, plazos propios del concreto procedimiento por razón de la materia, formas de iniciación y terminación, publicación e informes a recabar" (BOE, 2015)

En ese orden de cosas, basculan elementos tan significativos como que ya no será obligatoria la comparecencia de las personas ante las oficinas públicas, salvo cuando esté previsto en una norma con rango de ley (art. 19). Si queremos afilar más, podemos entrever elementos tan afines a nosotros como la reingeniería de procesos.

¿Qué se busca? No se trata de pasar sin más del papel al mundo digital, sino de conseguir *"mayores garantías de control e integridad documental"* y facilitar *"el cumplimiento de las debidas obligaciones de transparencia, pues permite ofrecer información puntual, ágil y actualizada a los interesados".*

Para muestra, un botón: podemos leer en la Exposición de Motivos de la Ley 39/2015 se afirma que

en el entorno actual, la tramitación electrónica no puede ser todavía una forma especial de gestión de los procedimientos sino que debe constituir la actuación habitual de las Administraciones. Porque una Administración sin papel basada en un funcionamiento íntegramente electrónico no sólo sirve mejor a los principios de eficacia y eficiencia, al ahorrar costes a ciudadanos y empresas, sino que también refuerza las garantías de los interesados

(BOE, 2015)

De los elementos de la derogada ley 11/2007 de la que actual hereda su espíritu, destacamos que se busca:

- Facilitar el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos
- Facilitar el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, con especial atención a la eliminación de las barreras que limiten dicho acceso
- Crear las condiciones de confianza en el uso de los medios electrónicos (protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas)
- Promover la proximidad con el ciudadano y la transparencia administrativa, así como la mejora continuada en la consecución del interés general

Para todo ello las Administraciones Públicas deberán habilitar diferentes canales o medios para la prestación de los servicios electrónicos, garantizando en todo caso el acceso a los

mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos. Las Administraciones Públicas deberán hacer pública y mantener actualizada una relación de las oficinas en las que se prestará asistencia para la presentación electrónica de documentos (art. 16.7).

La accesibilidad no deja de ser un elemento importante. En concreto en el artículo 38.5 de la ley 40, podemos leer

"La publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará los principios de accesibilidad y uso de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos"

(BOE, 2015)

La accesibilidad es un elemento que nos preocupa particularmente como informáticos, dado que es una barrera de entrada a determinados ciudadanos que está en nuestra mano eliminar.

Otro elemento de interés es el estudio de las implicaciones técnicas en aspectos como la conservación en formato electrónico por las Administraciones Públicas de los documentos de un expediente, la obtención de copias electrónicas de documentos electrónicos que formen parte de procedimientos, la seguridad, uso de aplicaciones con estándares abiertos (o de uso generalizado), la ventanilla única o la firma electrónica. Vamos a profundizar en algunos de ellos.

3.1. La firma electrónica

Este elemento destaca por la necesaria identificación y autentificación. En este sentido, las Administraciones Públicas utilizarán sistemas para su propia identificación electrónica y para la autenticación de los documentos electrónicos que produzcan. Las Administraciones Públicas están obligadas a verificar la identidad de los interesados, los sistemas admitidos serían:

> a) Sistemas basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».
>
> b) Sistemas basados en certificados electrónicos reconocidos o cualificados de sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».
>
> c) Sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan.

La sede electrónica es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública. Las sedes electrónicas utilizarán para su identificación y autentificación la firma electrónica o medio equivalente.

También el personal al servicio de la Administración Pública debe estar identificado y autentificado, y para ello cada Administración Pública podrá proveer a su personal de sistemas de firma electrónica.

Por último, los ciudadanos también pueden hacer uso de los sistemas de firma electrónica para su identificación y autentificación. Volveremos brevemente a la firma electrónica al hablar de la interoperabilidad.

Hay que reseñar que se distingue por primera vez en una norma entre identificación y firma. Esta división se basa en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. (Consejo Europeo, 2014)

3.2. Los registros electrónicos y las comunicaciones

Cada Administración dispondrá de un Registro Electrónico General, para la recepción y remisión de solicitudes, escritos y comunicaciones. Se podrán anotar en el mismo, así mismo, documentos oficiales salientes, dirigidos a otros órganos o particulares.

Hay que considerar así mismo que los organismos públicos vinculados o dependientes de cada Administración podrán disponer a su vez de su propio registro electrónico plenamente interoperable e interconectado con el Registro Electrónico General de la Administración de la que depende. De esta forma, el Registro Electrónico General de cada Administración funcionará como un portal que facilitará el acceso a los registros electrónicos de cada organismo[3].

Los registros electrónicos se regirán a efectos de cómputo de los plazos imputables tanto a los interesados como a las Administraciones Públicas por la fecha y hora oficial de la sede electrónica de acceso. Ésta deberá contar con las medidas de seguridad necesarias para garantizar su integridad y figurar de modo accesible y visible.

Además, los registros electrónicos permitirán la presentación de solicitudes, escritos y comunicaciones todos los días del año durante las veinticuatro horas. La presentación en un día inhábil se entenderá realizada en la primera hora del primer día hábil siguiente. El registro electrónico garantizará la constancia de un número, epígrafe expresivo de su naturaleza, fecha y hora de su presentación, identificación del interesado, órgano administrativo remitente, si procede, y persona u órgano administrativo al que se envía, y, en su caso, referencia al contenido del documento que se registra.

Los ciudadanos podrán elegir en todo momento la manera de comunicarse con las Administraciones Públicas, sea o no por medios electrónicos.

[3] En todo caso, los registros electrónicos deben cumplir con las garantías y medidas de seguridad previstas en la legislación en materia de protección de datos de carácter personal.

3.3. Los documentos

Las Administraciones Públicas emitirán los documentos administrativos por escrito, a través de medios electrónicos, a menos que su naturaleza exija otra forma más adecuada de expresión y constancia. Para que estos documentos sean considerados válidos, deben (Artículo 26.2 de la ley 39/2015)

a) Contener información de cualquier naturaleza archivada en un soporte electrónico según un formato determinado susceptible de identificación y tratamiento diferenciado.
b) Disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.
c) Incorporar una referencia temporal del momento en que han sido emitidos.
d) Incorporar los metadatos mínimos exigidos.
e) Incorporar las firmas electrónicas que correspondan de acuerdo con lo previsto en la normativa aplicable.

Además, se considerarán válidos los documentos electrónicos, que cumpliendo estos requisitos, sean trasladados a un tercero a través de medios electrónicos. (BOE, 2015)

Aparece un concepto interesante: la "copia auténtica". De forma tradicional, se ha usado la compulsa[4]. Hay que recordar que, históricamente, hacer copias de documentos era, al principio, imposible y luego, muy costoso, pudiendo en el proceso de copia perderse calidad llegando incluso a establecer dudas sobre la identidad entre original y copia. Con los medios digitales es mucho más fácil obtener copias pero, no lo olvidemos, también modificarlas con intención de alterar el sentido original del documento primitivo. Así, consideraremos "copia auténtica de un documento público administrativo o privado" las realizadas, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido. Las copias auténticas tendrán la misma validez y eficacia que los documentos originales. (art 27 de la ley 39/2015). Las copias electrónicas deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento. Se requiere que el documento haya sido digitalizado[5] y deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento. Cuando se trate de copias en soporte papel de documentos electrónicos se requerirá que en las mismas figure la condición de copia y contendrán un código generado electrónicamente u otro sistema de verificación, que permitirá contrastar la autenticidad de la copia mediante el acceso a los archivos electrónicos del órgano u Organismo público emisor. Por último, las copias en soporte papel de documentos originales emitidos en dicho soporte se proporcionarán mediante una copia auténtica en papel del documento electrónico que se encuentre en poder de la Administración o bien mediante una puesta de manifiesto electrónica conteniendo copia auténtica del documento original.

[4] Según la RAE, en su segunda acepción: Copia de un documento cotejada con su original.

[5] Se entiende por digitalización, el proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en un fichero electrónico que contiene la imagen codificada, fiel e íntegra del documento (art. 27 Ley 39/2015)

Sobre la presentación presencial de documentos ante las Administraciones Públicas, se introduce una novedad: éstos deberán ser digitalizados por la oficina de asistencia en materia de registros en la que hayan sido presentados para su incorporación al expediente administrativo electrónico, devolviéndose los originales al interesado, sin perjuicio de aquellos supuestos en que la norma determine la custodia por la Administración de los documentos presentados o resulte obligatoria la presentación de objetos o de documentos en un soporte específico no susceptibles de digitalización. (art. 16.5 ley 39/2015).

Es de especial importancia remarcar que este proceso, necesario para llevar a buen puerto la normativa sobre transparencia, seguridad[6] e interoperabilidad, necesita que cada Administración Pública mantenga un archivo electrónico único de los documentos electrónicos que correspondan a procedimientos finalizados. Documentos electrónicos que deberán conservarse en un formato que permita garantizar la autenticidad, integridad y conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión. La eliminación de dichos documentos deberá ser autorizada de acuerdo a lo dispuesto en la normativa aplicable.

3.4. Interoperabilidad de sistemas y aplicaciones

Las Administraciones Públicas utilizarán las tecnologías de la información en sus relaciones con las demás administraciones [7] y con los ciudadanos, aplicando medidas informáticas, tecnológicas, organizativas, y de seguridad, que garanticen un adecuado nivel de interoperabilidad técnica, semántica y organizativa y eviten discriminación a los ciudadanos por razón de su elección tecnológica.

El Esquema Nacional de Interoperabilidad comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad (art. 156.1 Ley 40/2015).

El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los

[6] Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos. (art. 17 Ley 39/2015)

[7] La Administración General del Estado, las Administraciones Autonómicas y las Entidades Locales, adoptarán las medidas necesarias e incorporarán en sus respectivos ámbitos las tecnologías precisas para posibilitar la interconexión de sus redes con el fin de crear una red de comunicaciones que interconecte los sistemas de información de las Administraciones Públicas y permita el intercambio de información y servicios entre las mismas, así como la interconexión con las redes de las instituciones de la Unión Europea y de otros Estados Miembros (art. 155.3 Ley 40/2015).

principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada (Ley 40/2015).

Muy relacionado con la interoperabilidad, por cuestiones obvias, está la reutilización de sistemas y aplicaciones de propiedad de la Administración. Al respecto, la Ley 40/2015, en su artículo 157.1 y 157.2, dice:

1. Las Administraciones pondrán a disposición de cualquiera de ellas que lo solicite las aplicaciones, desarrolladas por sus servicios o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares, salvo que la información a la que estén asociadas sea objeto de especial protección por una norma. Las Administraciones cedentes y cesionarias podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas.
2. Las aplicaciones a las que se refiere el apartado anterior podrán ser declaradas como de fuentes abiertas, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración Pública o se fomente con ello la incorporación de los ciudadanos a la Sociedad de la información.

Al respecto de la interoperabilidad de la firma electrónica, la ley 40/2015, en su artículo 45.2 dice que con el fin de favorecer la interoperabilidad y posibilitar la verificación automática de la firma electrónica de los documentos electrónicos, cuando una Administración utilice sistemas de firma electrónica distintos de aquellos basados en certificado electrónico reconocido o cualificado, para remitir o poner a disposición de otros órganos, organismos públicos, entidades de Derecho Público o Administraciones la documentación firmada electrónicamente, podrá superponer un sello electrónico[8] basado en un certificado electrónico reconocido o cualificado.

3.5. Derechos y obligaciones

Aparecen en algún caso y se reafirma en otro, algunos derechos del ciudadano. Así, según el artículo 13 de la Ley 39/2015, aparece una enumeración, de los que destacamos por su interés los siguientes:

- Comunicación digital: Comunicarse con las Administraciones Públicas a través de un Punto de Acceso General electrónico de la Administración.

- Derecho de asistencia: ser asistidos en el uso de medios electrónicos en sus relaciones con las Administraciones Públicas.

- Transparencia: acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico.

[8] Un certificado de Sello Electrónico vincula unos Datos de Verificación de Firma a los datos identificativos y de autenticación de determinada Administración, organismo o entidad y la persona física representante de la Administración, organismo o entidad Titular del certificado y, en su caso, el personal en quien se delegue a efectos de la actuación administrativa automatizada. (Ministerio de Justicia, 2016)

- Identificación electrónica: obtención y utilización de los medios de identificación y firma electrónica contemplados en esta Ley.

- Protección de datos: protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Sobre la obligatoriedad de la comunicación, la respuesta a la pregunta ¿Quién está obligado a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo? nos la aclara el artículo 14 de la Ley 39/2015, que nos dice que para las personas físicas existe cierta optatividad (Las personas físicas podrán elegir en todo momento si se comunican con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos o no, salvo que estén obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas. El medio elegido por la persona para comunicarse con las Administraciones Públicas podrá ser modificado por aquella en cualquier momento) y nos indica quien debe, de forma obligatoria, usar éste canal para la realización de cualquier trámite de un procedimiento administrativo:

a) Las personas jurídicas.

b) Las entidades sin personalidad jurídica.

c) Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones Públicas en ejercicio de dicha actividad profesional. En todo caso, dentro de este colectivo se entenderán incluidos los notarios y registradores de la propiedad y mercantiles.

d) Quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración.

e) Los empleados de las Administraciones Públicas para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado público,

Vemos que básicamente, hablamos de empresas cuando nos centramos en la obligatoriedad. Obviamente, no solo por los principios de interoperabilidad, sino por la búsqueda de ese sueño de la Administración Única, dejando por sentado que toda relación interadministrativas debe ser obligatoriamente electrónica. Si nos planteamos la pregunta ¿debe un empleado público tramitar obligatoriamente por medios electrónicos los procedimientos?, la respuesta es un “SI” tajante.

3.6. Problemas principales en su aplicación

Con el paso dado, el legislador parece querer poner al alcance del ciudadano la administración que éste desea: transparente, participativa, digital, sostenible… se le da vueltas a la correcta prestación de los servicios públicos, lo que, ligado a lo anterior nos apunta una relación evidente con lo que damos en llamar gobierno abierto, e incluso con las “Smart City”. Esto es muy ambicioso, pensemos desde donde se parte y hasta donde se quiere llegar. El cambio

lleva implícito un buen conjunto de problemas que posiblemente el profesional se encuentre, de entre los que destacamos:

- No respetar la neutralidad tecnológica. Nos encontramos con sedes electrónicas que sólo son accesibles desde determinados sistemas, incluso desde versiones concretas de Windows o navegadores (destacando que en algún caso solo es posible el acceso desde explorer, con los consiguientes problemas para personas con determinados tipos de discapacidad).
- Confusión en las administraciones: se ha tendido a asimilar la Administración electrónica con la eliminación de los documentos en papel o el uso masivo de la informática, cuando estos factores no son más que consecuencias, pero no causas ni mucho menos definiciones de este tipo de Administración.
- Inexistencia de procedimientos (incluso protocolos internos) adaptados a este modo de funcionar. Estos procedimientos o se han de crear de cero, o hay que hacer una labor ardua de reingeniería con los muchas veces obsoletos procedimientos anteriores.
- Falta de canales para la colaboración entre administraciones públicas para la integración e interconexión electrónica. Esto es algo que puede ser leído dentro del ámbito de la interoperabilidad, adoptando criterios técnicos comunes

4. La responsabilidad civil

La **responsabilidad civil** debe entenderse como la obligación que tiene toda persona de reparar los daños y perjuicios producidos a un tercero a consecuencia de una acción u omisión, propia o de otro por el que se deba responder, en la que haya habido algún tipo de culpa o conducta dolosa (por ejemplo, daños a terceros en accidentes de coches, de caza, por escapes contaminantes en una empresa, por errores profesionales, etc.).

Desde el punto de vista de intencionalidad podemos distinguir dos tipos de conductas:

- **Conducta culposa o negligente**. Actos lícitos que causan daños por no haberse tomado las precauciones debidas, es decir, por haber actuado negligentemente.

- **Conducta dolosa**. Actos en los que el sujeto es consciente de que va a ocasionar un daño.

La Responsabilidad Civil es la institución jurídica cuya finalidad es regular el sistema de compensaciones económicas reparadoras de daños producidos a terceras personas como consecuencias de **relaciones contractuales o extracontractuales**. En este último caso, la **responsabilidad por hechos extracontractuales**, conlleva que una persona debe indemnizar a otra, con quien no le une ningún vínculo jurídico específico, porque le ha causado un daño. En la **responsabilidad contractual**, alguien promete a otro proporcionar una cosa o servicio y luego, en el momento de ejecución de esas obligaciones, quien debe cumplirlas no lo hace o lo hace de modo defectuoso ocasionando un daño a su contraparte, quien al contratar había adquirido un derecho a recibir algo que luego no recibe o recibe de modo incompleto o inadecuado.

La **indemnización** consiste en cuantificar los daños y perjuicios sufridos por la persona física o jurídica, debido a la actividad desarrollada por aquel sujeto que tiene responsabilidad y en

resarcir los perjuicios ocasionados. El derecho a la indemnización podría comprender no sólo el valor de la pérdida que haya sufrido (**daño emergente**), sino también el de la ganancia que haya dejado de obtener el acreedor (**lucro cesante**). El importe así obtenido se denomina **reparación integra** de forma que la persona que sufre el perjuicio debe ser restituida a la situación anterior de haberse producido el acto que da lugar a la indemnización.

También es necesario distinguir entre daños patrimoniales y los extra patrimoniales (llamados **daños morales**). Estos últimos están constituidos por los perjuicios que, sin afectar a las cosas materiales, se refieren al patrimonio espiritual, a los bienes inmateriales de la salud, el honor, la libertad y otros análogos.

La **responsabilidad civil** se diferencia de la **responsabilidad penal**, en que esta última tiene por finalidad designar a la persona que deberá responder por los daños o perjuicios causados a la sociedad en su totalidad, no a un individuo en particular. Por tanto, en la responsabilidad penal los daños o perjuicios tienen un carácter social, pues son considerados como atentados contra el orden público lo suficientemente graves como para ser fuertemente reprobados y ser erigidos en infracciones. La responsabilidad civil intenta asegurar a las víctimas la reparación de los daños privados que le han sido causados, por tanto, la sanción de la responsabilidad civil es, en principio, indemnizatoria, y no represiva. Ambas responsabilidades pueden coexistir en un mismo hecho.

4.1. La responsabilidad civil en el ámbito de la ingeniería

Barcelo (2003) trata la responsabilidad civil en lo que respecta a la profesión de ingeniero, donde se pueden exigir responsabilidades en función de sus competencias siempre que su actuación haya tenido relación de causa-efecto sobre el daño producido.

En las relaciones contractuales se distinguen entre obligaciones de medios o actividad y obligaciones de resultado. En la **obligación de resultado** el acreedor (cliente) busca exclusivamente un fin y no le interesa examinar los medios de los que se valga el deudor (técnico). Así, si el deudor debe un resultado, responde por éste, por lo que a toda obligación de resultado corresponderá una responsabilidad de resultado. En este tipo de obligaciones el cliente espera un resultado, produciéndose el incumplimiento de la obligación si este resultado no se obtiene, con independencia de la diligencia empleada por aquel a quien se contrató. Cuando la **obligación** es **de medios o actividad**, el técnico se compromete solamente a hacer lo posible para procurar al cliente la prestación que éste espera: no se compromete a procurarle un resultado, sino a actuar diligentemente. Son obligaciones en las que precisamente esta diligencia del técnico constituye el objeto de las mismas. Y esto es así porque el resultado perseguido es demasiado aleatorio y depende poco de la sola diligencia del deudor. De forma que si el resultado perseguido no se obtiene y el técnico ha prestado la adecuada diligencia en sus actuaciones, no será suficiente para generar responsabilidad civil del profesional.

La **responsabilidad civil profesional** se define como aquella que incumbe a una determinada persona por los daños causados a un tercero como consecuencia de una acción u omisión negligente en el ejercicio de su actividad profesional.

Tradicionalmente, se ha reducido o circunscrito el ámbito profesional a aquellas actividades liberales que se entendían como elitistas (arquitectos, ingenieros, abogados, médicos, etc.) caracterizadas en líneas generales como: el empleo de las facultades intelectuales, la ausencia de

todo vínculo de dependencia con respecto a la empresa pública o privada, y una autonomía y amplias facultades en orden a la toma de decisiones y asunción de la propia responsabilidad.

Hoy en día, dichas profesiones no pueden considerarse ya elitistas, y tampoco los trabajos son absolutamente liberales, por cuanto muchos de estos profesionales pueden estar vinculados profesionalmente a empresas de asesoría o consultoría.

En el caso de los ingenieros en informática, uno de los supuestos típicos donde puede incurrir en responsabilidad es en la protección de datos personales. De hecho la Ley de Protección de Datos declara que el interesado que sufra daño o una lesión tiene derecho a ser indemnizado. Para que pueda reclamarse la indemnización, la persona interesada que reclama debe haber sufrido un daño cierto, probado, efectivo y real; no basta con que se haya incumplido algún deber en relación al tratamiento de sus datos.

4.2. El seguro de responsabilidad civil

Hoy en día, el ejercicio de las actividades industriales, profesionales e incluso las particulares no es concebible sin el apoyo de la contratación de seguros de responsabilidad civil, que permiten desplazar el riesgo del pago de indemnizaciones hacia empresas especializadas en ello.

Una clasificación de los distintos seguros de responsabilidad civil puede ser la siguiente:

a) Seguros Particulares: El más frecuente es el de responsabilidad civil como cabeza de familia. Cubre los riesgos derivados de la vida particular, así como la propiedad de viviendas, animales, etc. Excluyendo los riesgos profesionales y los derivados de la circulación, esta cobertura suele estar incluida en los seguros multi riesgo de hogar.

b) Seguros Industriales: La cobertura de los riesgos de responsabilidad civil de las empresas suele hacerse en un único contrato en el que se incluyen diferentes garantías según las necesidades de la empresa.

c) Seguros Profesionales: Cubren los daños que puedan ocasionar los errores profesionales cometidos por personas que ejercen las actividades propias de la titulación que poseen.

d) Seguros obligatorios: Vienen exigidos por la ley y la administración como requisito para ejercer una actividad (Ej. De automóviles, de caza, de embarcaciones de recreo, …)

e) Seguros de responsabilidad civil de los administradores: Las pólizas de las aseguradoras garantizan a los consejeros y directivos asegurados el pago de las posibles indemnizaciones que le puedan ser requeridas por su gestión, al frente de la empresa en su condición de administradores de la misma, realizadas sin la debida diligencia.

Cada póliza determinará, mediante condiciones especiales, la responsabilidad civil que cubre en concreto, es decir, las actividades que quedan cubiertas con sus limitaciones especificas.

Las compañías aseguradoras condicionan su responsabilidad y el precio del seguro a determinados requisitos, estableciendo una serie de limitaciones y exclusiones en las obligaciones del asegurador:

a) Limites referentes a los riesgos cubiertos: Estos límites vendrán dados por la definición y descripción de la actividad realizada que realmente esté amparada por las condiciones de la póliza, como origen de las responsabilidades cubiertas por el seguro.

b) Límites cuantitativos: Las obligaciones del Asegurador quedarán limitadas respecto a las cuantías de las indemnizaciones por dichos límites.

c) Límite mínimo: Pueden estar condicionados por una franquicia, entendida ésta como cantidad que no queda cubierta por el contrato de seguro (queda a cargo del asegurado).

d) Delimitación temporal: La póliza puede diferenciarse en función de criterios temporales de cobertura.

e) Delimitación geográfica: El ámbito de cobertura se extiende generalmente a los daños ocasionados dentro del territorio español y reclamados ante la autoridad judicial española.

f) Exclusiones: Las compañías aseguradores tienden a establecer exclusiones generales en otras situaciones posibles.

5. Delitos informáticos

Se entiende por código penal al conjunto de normas jurídicas punitivas de un Estado ordenadas de tal manera que permiten recoger en un solo compendio la legislación aplicable. El objetivo es proteger a la sociedad mediante la regulación de las conductas punibles, consideradas como delitos, con la aplicación de una pena. En cuanto al Derecho español, el Código Penal vigente fue aprobado por Ley Orgánica 10/1995, de 23 de Noviembre. Por supuesto, ha sido objeto de varias reformas posteriores.

Según la RAE, un delito es la acción u omisión voluntaria o imprudente penada por la ley. Es decir, para que exista responsabilidad criminal y por tanto delito, la persona debe haber actuado con dolo o culpa; o sea, con intención o con imprudencia, respectivamente.

5.1. Definición de delito informático

El Código Penal español no contempla los delitos informáticos como tal. El delito informático podría definirse como aquél que se comete a través de medios informáticos. Se estaría hablando pues de delitos de estafa, delitos contra la propiedad intelectual e industrial, etc., es decir hechos que están tipificados como delito en el Código Penal, y que se basan en técnicas o mecanismos informáticos. En este sentido, algunos consideran que no es necesario diferenciarlos de los delitos tradicionales.

Por otro lado, por delito informático se entiende también aquél que tiene como objetivo el dañar de alguna manera ordenadores, medios electrónicos o redes de Internet. Los sistemas informáticos se han convertido en un objetivo interesante de ataque. El perjuicio provocado es enorme puesto que va mucho más allá del valor material de los objetos dañados.

En resumen, los datos o sistemas informáticos pueden ser el objeto del ataque o el medio o instrumento para cometer otros delitos.

5.2. Características de los delitos informáticos

Según Julio Téllez Valdés (1991), los delitos informáticos presentan una serie de características comunes:

- En su mayoría son actos imprudentes, es decir que no necesariamente se cometen con intención.
- En ocasiones son actos que pueden realizarse de forma sencilla y rápida.
- Pueden provocar pérdidas económicas serias.
- Su comisión requiere ciertos conocimientos técnicos, pudiendo llegar a ser muy sofisticados.
- No requieren la presencia física para que puedan llegar a consumarse.
- Son delitos que presentan dificultades para su comprobación ya que, en muchos casos, es complicado encontrar las pruebas.
- La proliferación y evolución de estos delitos hace aún más complicada su identificación y consiguiente persecución.

5.3. Clasificación de los delitos informáticos

El Convenio de Ciberdelincuencia del Consejo de Europa[9] surge de la necesidad de aplicar una política penal común, encaminada a proteger a la sociedad frente a la ciber delincuencia. Se trata de un acuerdo internacional fruto de cuatro años de trabajo de los expertos de los 45 países miembros del Consejo de Europa y de no miembros como Estados Unidos, Canadá y Japón.

Como consecuencia del desarrollo y utilización cada vez mayor de las tecnologías de la información y la comunicación, se hace necesario adoptar una legislación adecuada (derecho penal, derecho procesal) y mantener una política de cooperación internacional para luchar contra la ciber delincuencia.

En este convenio se definen los delitos informáticos como: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos".

A partir de esta definición presenta la siguiente clasificación de los delitos informáticos en cuatro grupos:

- Delitos de intrusión contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, es decir acceso ilícito, interceptación ilícita, atentados contra la integridad de los datos, atentados contra la integridad del sistema, abuso de equipos e instrumentos técnicos. Ejemplos de este tipo de delitos son el robo de identidades, el uso de claves restringidas para obtener y divulgar información, la violación de sistemas de seguridad de sistemas informáticos, la conexión a redes no autorizadas, …

[9] Convenio firmado en Budapest el 23 de noviembre de 2001 y de entrada en vigor el 22 de marzo de 2004.

- Delitos patrimoniales como la falsedad informática o la estafa informática con repercusiones económicas. Entre otros podemos poner los siguientes ejemplos: el beneficiarse de pólizas inexistentes, la alteración de movimientos bancarios o saldos de cuentas, la alteración de asistencias y notas en el sistema universitario, la modificación de un programa para favorecer por ejemplo que ciertos productos no paguen los impuestos correspondientes, el fraude con tarjetas de crédito y débito, las defraudaciones bancarias comúnmente como el phishing y pharming, …

- Infracciones relativas al contenido en las que se incluye exclusivamente las infracciones relativas a la pornografía infantil

- Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines con las copias ilegales de software o la piratería informática como ejemplos.

Aunque posteriormente se añadiría un quinto grupo, cuando en el año 2003 se promulgó la firma del Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa con el fin de criminalizar actos de racismo y xenofobia.

Hay otras clasificaciones de los delitos informáticos, siguiendo distintos criterios. Por ejemplo, la Brigada de Investigación Tecnológica de la Policía Nacional Española propone otra clasificación[10] posible. La Brigada de Investigación Tecnológica es la unidad policial destinada a responder a los retos que plantean las nuevas formas de delincuencia como la pornografía infantil, estafas y fraudes por Internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería…

Por último es interesante referir los delitos informáticos reconocidos por Naciones Unidas:

- Fraudes cometidos mediante manipulación informática como manipulación de datos de entrada o salida, manipulación de programas, fraude efectuado por manipulación informática

- Falsificación informática, tanto como objeto como instrumento

- Daños o modificaciones de programas o datos como el sabotaje informático, el acceso no autorizado a servicios y sistemas informáticos, la reproducción no autorizada de programas informáticos de protección legal

6. Ejercicios propuestos

6.1. Test

1. Las cortes generales ejercen el poder:

a) Judicial.

b) Ejecutivo.

c) Legislativo.

[10] http://www.policia.es/org_central/judicial/udef/bit_actuaciones.html

d) General.

2. Las directivas de la Unión Europea:

a) Son directrices y por tanto no son de obligado cumplimiento.

b) Son reglamentos y por tanto se deben cumplir como indica.

c) Son objetivos a cumplir y por tanto cada país transcribe la directiva a su propia legislación según sus propios criterios.

d) Son leyes españolas extrapoladas a la unión europea y por tanto deben ser consideradas por el consejo europeo para su implantación.

3. Entre los servicios incluidos en la ley de la sociedad de la información NO se encuentra:

a) La gestión de compras en la red por grupos de personas.

b) El suministro de información por vía telemática.

c) La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.

d) Servicios de asistencia técnica informática a domicilio.

4. Los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios serán responsables por el contenido de esos datos ni por la reproducción temporal de los mismos, si:

a) Permiten el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita.

b) Respetan las normas generalmente aceptadas y aplicadas por el sector para la actualización de la información.

c) Interfieren en la utilización lícita de tecnología generalmente aceptada y empleada por el sector, con el fin de obtener datos sobre la utilización de la información.

d) No modifican la información.

5. La Ley de acceso electrónico de los ciudadanos a los servicios públicos:

a) Regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa para las relaciones de los ciudadanos con las administraciones públicas.

b) Regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa para las relaciones entre administraciones públicas.

c) Regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa tanto en las relaciones de los ciudadanos con las administraciones públicas, como en las relaciones entre las propias administraciones.

d) Ninguna de las anteriores.

6. Desde el punto de vista de intencionalidad podemos encontrar:

a) Conducta dolosa: Actos lícitos que causan daños por no haberse tomado las precauciones debidas, es decir, por haber actuado negligentemente.

b) Conducta negligente: Actos en los que el sujeto es consciente de que va a ocasionar un daño.

c) Las respuesta a y b son ciertas.

d) Las respuestas a y b son falsas.

7. En las relaciones contractuales se distinguen entre obligaciones de medios o actividad y obligaciones de resultado:

a) En la obligación de resultado el acreedor (cliente) busca exclusivamente un fin y no le interesa examinar los medios de los que se valga el deudor (técnico).

b) Cuando la obligación es de medios o actividad, el técnico se compromete solamente a hacer lo posible para procurar al cliente la prestación que este espera; no se compromete a procurarle un resultado, sino a actuar diligentemente.

c) Las respuesta a y b son ciertas.

d) Las respuestas a y b son falsas.

Soluciones: 1. c); 2. c); 3. d); 4. c); 5. c); 6. d); 7. c)

6.2. Ejercicios

1. Elabora un cuadro comparativo de las diferencias esenciales entre las normas jurídicas y las normas morales, dando varios ejemplos de cada tipo de norma e indicando las sanciones correspondientes en caso de incumplimiento.

2. Compara un contrato electrónico con un contrato tradicional estableciendo sus diferencias y similitudes.

3. ¿Qué es la carta de servicios electrónicos? ¿Dónde se estable su marco general? Busca algún ejemplo en Internet.

4. ¿Cómo funciona la firma digital? ¿Qué es un certificado digital?

5. Existe una amplia variedad de seguros que ofertan las empresas aseguradoras que cubren diferentes tipos de riesgos, con variados límites y exclusiones. La actividad consiste en realizar una comparativa analizando tres seguros de interés en el ámbito de la informática, clasificarlos según las clasificaciones tratadas, identificar sus límites y exclusiones, y aportar conclusiones propias.

6. ¿Qué clasificación de delitos informáticos propone la Brigada de Investigación Tecnológica de la Policía Nacional Española?

7. Después de recopilar recortes de prensa relacionados con delitos informáticos, propón una clasificación según el criterio que más convenga.

8. A partir del mapa conceptual sobre hacking de René Mérou, investiga un poco sobre el concepto y las distintas formas de entenderlo.

7. Índice

Bibliografía

Almonacid, V., & Moreno, V. (2015). *Manifiesto Administración Electrónica.* Madrid: INAP Instituto Nacional Administración Pública.

Barceló Rico-Avello, G. (2003). *DTIE 17.02 – Responsabilidad civil del ingeniero. .* Madrid: ATECYR.

BOE. (2 de Octubre de 2015). Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas . *BOE, 236*. Madrid, España: BOE.

BOE. (2 de Octubre de 2015). Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. *BOE, 236*. Madrid, España: BOE.

Calvo Hornero, A. (2007). *Organización de la Unión Europea. .* Madrid: Editorial Universitaria Ramón Areces.

Consejo Europeo. (28 de Agosto de 2014). REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones. *Diario Oficial de la Unión Europea*. Bruselas, Europa: Diario Oficial de la Unión Europea.

Gobierno de España. (2016). *Portal de Administración Electrónica*. Recuperado el 24 de =ctubre de 2016, de https://administracionelectronica.gob.es

Grimalt Servera, P. (1999). *La responsabilidad civil en el tratamiento automatizado de datos personales. .* Madrid: Comares.

Martínez Sospedra, M. (1994). *Estado y Constitución. .* Madrid: Fundación Universitaria San Pablo CEU.

Ministerio de Industria, T. y. (2016). *LSSI*. Recuperado el octubre de 2016, de http://www.lssi.gob.es/paginas/Index.aspx

Ministerio de Justicia. (2016). *sede electrónica*. Recuperado el 20 de octubre de 2016, de https://sede.mjusticia.gob.es/cs/Satellite/Sede/es/informacion-general/sellos-electronicos

Noticias jurídicas. (2016). *Noticias jurídicas, legislación y convenios colectivos.* Recuperado el octubre de 2016, de http://noticias.juridicas.com/base_datos/

Téllez Valdés, J. (1991). *Derecho informático. .* México: Universidad Nacional Autónoma de México.

Torres del Moral, A. (1991). *Estado de derecho y democracia de partidos.* Madrid: Facultad de Derecho Universidad Complutense.