IES POETA PACO MOLLÁ
PETRER
Departamento de Informática

Seguridad Informática

CFGM Sistemas Microinformáticos y Redes
2.º curso

TEMA 8
Legislación

GENERALITAT VALENCIANA
Conselleria d'Educació, Investigació, Cultura i Esport

Sumario

I Introducción....4
II LOPD-GDD....5
1 Aspectos destacables....6
1.1 Figuras legales en la LOPD-GDD....6
1.2 Consentimiento....7
1.3 Régimen sancionador....7
2 RGPD....8
2.1 Definiciones....8
2.2 Puesta a disposición de información personal....9
2.3 Medidas de protección de datos....10
3 Garantía de los derechos digitales....11
3.1 Derechos de los ciudadanos en Internet....11
3.2 Derechos de los menores y la educación....11
3.3 Derechos relacionados con el ámbito laboral....12
3.4 Derechos de la era digital y las comunicaciones....13
4 La Agencia Española de Protección de Datos....14
III LSSI....16
1 Aspectos destacables....17
1.1 Información al cliente....17
1.2 Páginas de enlaces y similares....17
1.3 Comunicaciones comerciales....18
1.4 Régimen sancionador....18
2 El portal de la LSSI....19
IV LPI....20
1 Derechos de autor....21
2 La copia privada....21
2.1 Puntos básicos con respecto a la copia privada....22
2.2 El ámbito de la copia privada....23
3 Programas informáticos....23
3.1 El software *pirata* en el Código Penal....24
4 Alternativas a las obras protegidas....24
V Legislación internacional....25
1 Unión Europea....25
2 Consejo de Europa....26
3 Naciones Unidas....27
VI Normas ISO: seguridad de la información....28
VII La Administración electrónica....30
1 El sistema Cl@ve....30
2 El Punto de Acceso General....31
2.1 La Carpeta Ciudadana....32
VIII Anexo I: Notificaciones en el correo electrónico....33
IX Bibliografía....34

v1.00

Julio Garay
IES Poeta Paco Mollá
Petrer (Alicante), 2022

I Introducción

De todos los temas relacionados con la seguridad informática, con toda probabilidad el relativo a la legislación es el menos atractivo para los futuros técnicos informáticos. Sin embargo es **uno de los temas más importantes**, dado que dichos técnicos serán los encargados (y responsables) de que se cumplan muchos aspectos legales en las infraestructuras que gestionen.

Dada la extensión y el alcance que la omnipresente Internet ha ido alcanzando en nuestras vidas, era de esperar que la legislación se adaptase para cubrir ámbitos que, en el pasado, se había dejado de lado. Las principales leyes españolas que cubren la actividad de los profesionales informáticos son:

- LOPD-GDD: Ley Orgánica de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales
- LSSI: Ley de Servicios de la Sociedad de la Información y Comercio Electrónico
- LPI: Ley de Propiedad Intelectual

Si el aspecto menos atractivo de la legislación es su aridez, al menos en la actualidad contamos con la notable ventaja de que **cualquiera puede consultar las leyes** a través de Internet en caso de duda. **Acudir a la propia ley** sobre la que se tienen dudas, en lugar de buscar la información en algún blog o canal de Youtube es una manera muy recomendable de asegurarse de estar haciendo lo correcto. Por otra parte, la legislación no es inmutable: con el tiempo se va adaptando a las nuevas realidades del país, y por ello es imprescindible mantenerse al tanto de sus cambios, ya que pueden tener un impacto directo en nuestro trabajo y en cómo lo desempeñamos.

Tengamos siempre presente el famoso principio

La ignorancia de la Ley no excusa de su cumplimiento

Además de estas leyes, en este tema revisaremos algunos aspectos adicionales de legislación internacional y nos detendremos en conceptos menos directamente relacionados pero también de importancia práctica.

II LOPD-GDD

Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales	
Título oficial	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
Objetivo	Adaptar la legislación española al **Reglamento General de Protección de Datos** de la UE, y garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.
Fecha de entrada en vigor	7 de diciembre de 2018 (día siguiente a su publicación en el BOE)
Texto completo	**BOE-A-2018-16673** (disponible en varios formatos, incluido PDF y ePub)
Predecesoras	LORTAD (Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal), 1992-1999 LOPD (Ley Orgánica de Protección de Datos Personales), 1999-2018
Estructura y extensión	97 artículos, organizados en diez títulos (más varias disposiciones adicionales, transitorias, etcétera). En total, unas 67 páginas.

La LOPD-GDD establece una serie de obligaciones destinadas a la protección de los datos personales contenidos en ficheros, automatizados (informatizados) o no (en papel u otro soporte), que poseen empresas y administraciones públicas, y que son tratadas por éstas con diferentes finalidades: gestión de personal, proveedores, clientes, campañas de *marketing*, etc. Por tanto, **cualquier fichero que contenga datos de personas** (una base de datos, una hoja de cálculo —y, teóricamente, incluso un modesto archivo *txt* o una lista de nombres y teléfonos en un folio—) **cae dentro del ámbito de esta ley.** Incumplir esta ley expone a la empresa u organización responsable a sanciones por parte de la Agencia Española de Protección de Datos (AGPD).

La LOPD-GDD equipara y **convierte el derecho a la protección de los datos personales en un derecho fundamental de las personas**. Dicho derecho fundamental tiene una relación directa con el derecho a la intimidad y al honor, descritos en el art. 18 de la Constitución. Este nuevo derecho fundamental protege el «control que a cada una de las personas le corresponde sobre la información que les concierne personalmente, sea íntima o no, para preservar el libre desarrollo de la personalidad».

Debemos consultar la LOPD-GDD, entre otros casos, **siempre que vayamos a**:

- Crear o gestionar ficheros de datos, informatizados o no;
- Instalar o gestionar sistemas de videovigilancia (art. 22);
- Gestionar sistemas de distribución de publicidad (art. 23);

- Mantener ficheros o manejar datos más allá de nuestras fronteras —debe considerarse que esto afecta particularmente al uso de servicios «en la nube», ya sean de almacenamiento, computación, etc.— (título IV).

1 Aspectos destacables

Vamos a ver, en este punto, algunos aspectos importantes de la LOPD-GDD:

- Figuras legales
- Puesta a disposición de información personal
- Consentimiento
- Régimen sancionador

1.1 Figuras legales en la LOPD-GDD

La LOPD-GDD define una serie de figuras de importancia, para cada una de las cuales establece derechos y/o responsabilidades:

- **Responsable del fichero o tratamiento** («tratamiento», «fichero» y «archivo» son sinónimos en este contexto). Persona u organización que decide sobre la finalidad, contenido y uso del tratamiento. Típicamente, «el dueño» de la empresa.
- **Encargado del tratamiento**. Persona u organización que, sola o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento. Normalmente «el informático» de la empresa, en organizaciones pequeñas. O los administradores de bases de datos, en organizaciones más grandes.
- **Afectado** o **interesado**. Persona física (o sea, un ser humano, no una organización ni similar) cuyos datos son objeto del tratamiento.
- **Delegado de protección de datos** (***Data Protection Officer***, en el RGPD[1]). Interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y, en su caso, las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias. **El artículo 34 de la ley explicita en qué casos es obligatoria la existencia de esta figura.**

El Reglamento de desarrollo de la LOPD[2] (Real Decreto 1720/2007, de 21 de diciembre) añade dos figuras más:

1 Reglamento General de Protección de Datos de la Unión Europea; véase la pág. 8.

2 Dada la relativamente reciente aprobación de la nueva LOPD-GDD, en el momento de elaborar estos apuntes aún no se ha publicado el reglamento de desarrollo de dicha Ley. Es previsible que ocurra en un futuro más o menos próximo. Hasta que esto ocurra, el reglamento citado es el vigente.

- **Usuario**. Sujeto o proceso autorizado para acceder a datos o recursos.
- **Responsable de seguridad**. Persona o personas de la organización a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables. Cabría interpretar que esta figura ha sido remplazada por el delegado de protección de datos, visto más arriba.

1.2 Consentimiento

El trato automatizado de los datos de los interesados requiere de su **consentimiento**: una manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta el tratamiento de datos personales que le conciernen.

Si el tratamiento automatizado tiene varios fines, el interesado debe ser informado de todos ellos, y debe dar permiso específica e inequívocamente para todos ellos.

Al interesado **sólo se le puede exigir el consentimiento para los tratamientos que guarden relación con el mantenimiento, desarrollo o control del contrato**. El resto de los consentimientos serán optativos para el interesado.

1.3 Régimen sancionador

El título IX, «Régimen sancionador», establece todos los tipos de infracciones, diferenciando entre infracciones leves, graves y muy graves:

Sanciones por incumplimiento de la LOPD-GDD		
Infracciones	**Cuantía**	**Prescripción**
Leves	Hasta 40 000 €	1 año
Graves	De 40 001 a 300 000 €	2 años
Muy graves	De 300 001 a 20 000 000 € (0 de 2% a 4% de la facturación **bruta** anual)	3 años

2 RGPD

Dado que el objetivo principal de la LOPD-GDD es integrar el Reglamento General de Protección de datos en nuestro ordenamiento jurídico, y dado que, en muchas ocasiones, la ley hace referencias al contenido del reglamento sin desarrollarlo, vamos a dedicarle un apartado al RGPD.

Reglamento General de Protección de Datos de la Unión Europea	
Título oficial	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
Objetivo	Establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos en la Unión Europea. Proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.
Fecha de entrada en vigor	25 de mayo de 2018 (aprox. 2 años desde su publicación, el 4/5/2016)
Texto completo	**Documento 32016R0679** (disponible en formatos HTML y PDF)
Predecesores	Directiva de protección de datos (Directiva 95/46/CE), 1995-2018
Estructura y extensión	99 artículos, organizados en once capítulos. En total, unas 88 páginas.

El Reglamento General de Protección de Datos de la Unión Europea **otorga un amplio control y seguridad a los ciudadanos sobre su información personal en el mundo digital**. El RGPD amplía sus derechos a decidir cómo desean que sus datos sean tratados y cómo quieren recibir información de las empresas.

El cumplimiento del RGPD es obligatorio para todas las empresas y organizaciones de la UE desde el 25 de mayo de 2018. Aunque muchas empresas, particularmente PYMES, no son conscientes de la importancia de cumplir con el RGPD, y de las sanciones que puede acarrear no hacerlo, este reglamento **endurece el control sobre los datos personales** y **otorga a cada individuo el derecho a que sean utilizados o no por cualquier entidad**, pública o privada, así como la manera en la que se accede a ellos y a retirar el acceso.

En España, el cumplimiento del RGPD se enmarca en la LGPD-GDD (pág. 5), y es vigilado por la AEPD (pág. 14).

2.1 Definiciones

El **artículo 4** establece todas las **definiciones** necesarias para entender el reglamento: «datos personales», «tratamiento», «elaboración de perfiles», «seudonimización», «fichero», «responsable del tratamiento», etc.

2.2 Puesta a disposición de información personal

El *responsable del tratamiento* está obligado (arts. 12, 13 y 14) a facilitar al *interesado* «en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo» toda la información relativa a la identidad y datos de contacto del responsable, del delegado de protección de datos (DPD), etc.

Por otra parte, el *interesado* tendrá derecho (art. 15) a obtener del *responsable del tratamiento* confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y —entre otra— a la siguiente información:

- Los **fines** del tratamiento;
- Las **categorías de datos** personales de que se trate;
- Los **destinatarios o las categorías de destinatarios** a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
- La **existencia del derecho a solicitar del responsable la rectificación o supresión** de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
- Cuando los datos personales no se hayan obtenido del interesado, cualquier **información disponible sobre su origen.**

En las páginas web que recojan información con formularios, conviene poner una notificación incluyendo toda la información necesaria para cumplir con el RGPD. Debemos incluir:

- **Información sobre la privacidad de los datos recogidos**: los usuarios deben conocer en todo momento que estamos recogiendo sus datos, tanto en el formulario como en la política de privacidad.
- **Información sobre tiempo de conservación de datos**: es importante garantizar que los datos de los usuarios serán limitados a un mínimo de plazo, no deben conservarse más de lo necesario. Es decir, hemos de establecer plazos para su revisión periódica.
- **Derecho al olvido**: los datos personales pueden dejar de ser tratados si los usuarios retiran su consentimiento o se oponen al tratamiento de sus datos.

El **texto legal de una página web** debe ser completo y ceñirse a la legislación vigente; en Internet es relativamente fácil encontrar múltiples ejemplos de textos legales que puedan cumplir todos los requisitos de nuestro sitio web. Teniendo en cuenta la LPI, debemos tomar esos textos como orientación para crear los nuestros, pero **no copiarlos literalmente**.

2.2.1 El correo electrónico y el RGPD

El simple uso del correo electrónico supone un sistema de recogida y almacenamiento de datos personales en un fichero y, por tanto, está sujeto a las normas del RGPD, por lo que, como para cualquier otro medio de comunicación, conviene incluir en el contenido un añadido similar a este:

> **PROTECCIÓN DE DATOS:** de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 de 27 de abril de 2016 (RGPD), le informamos que los datos personales y dirección de correo electrónico, recabados del propio interesado o de fuentes públicas, serán tratados bajo la responsabilidad de NOMBRE_DEL_RESPONSABLE_DEL_TRATAMIENTO para el envío de comunicaciones sobre nuestros productos y servicios y se conservarán mientras exista un interés mutuo para ello. Los datos no serán comunicados a terceros, salvo obligación legal. Le informamos que puede ejercer los derechos de acceso, rectificación, portabilidad y supresión de sus datos y los de limitación y oposición a su tratamiento dirigiéndose a DIRECCIÓN_POSTAL o enviando un mensaje al correo electrónico: DIRECCIÓN_DE_CORREO_ELECTRÓNICO. Si considera que el tratamiento no se ajusta a la normativa vigente, podrá presentar una reclamación ante la autoridad de control en www.agpd.es.

2.3 Medidas de protección de datos

El RGPD establece la obligación por parte del *responsable del tratamiento*, así como del *encargado del tratamiento*, de llevar un **registro de las actividades del tratamiento**. El **artículo 30** detalla toda la información que dicho registro debe incluir.

Además, el **artículo 32** especifica los **requerimientos de seguridad:** teniendo en cuenta las posibilidades técnicas, las necesidades, y los riesgos, el responsable y el encargado del tratamiento aplicarán medidas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la ***seudonimización*** y el **cifrado** de datos personales;

b) la capacidad de **garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes** de los sistemas y servicios de tratamiento;

c) la **capacidad de restaurar la disponibilidad** y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un **proceso de verificación, evaluación y valoración** regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

En el caso de que se registre una violación de la seguridad de los datos personales, los artículos 33 y 34 imponen la **obligatoriedad de informar a la autoridad competente** (normalmente la AEPD) **y al interesado**, respectivamente. «La notificación incompleta, tardía o

defectuosa» a la autoridad de protección de datos es una infracción leve de la LOPD-GDD (véase el punto 1.3, *Régimen sancionador*, en la pág. 7)

3 Garantía de los derechos digitales

El título X de la LOPD-GDD desarrolla la mayor novedad de esta ley con respecto a su predecesora: la *garantía de los derechos digitales*.

Dichos derechos se pueden agrupar en cuatro bloques:

1. Derechos de los ciudadanos en Internet;
2. Derechos de los menores y la educación;
3. Derechos relacionados con el ámbito laboral;
4. Derechos de la era digital y las comunicaciones.

3.1 Derechos de los ciudadanos en Internet

Agrupa los artículos 79 a 82, 85 y 86 de esta ley:

- **Derecho de acceso y neutralidad de Internet**. El derecho a Internet es un derecho humano desde 2011 para la ONU y ahora esta nueva ley reconoce que debe ser «universal, asequible, de calidad y no discriminatorio».
- **Derecho a la seguridad digital**, en las comunicaciones que los usuarios transmitan y reciban a través de Internet (una extensión del artículo 18 de la Constitución, que recoge el derecho de privacidad de las comunicaciones, al mundo digital).
- **Derecho de rectificación en Internet**: incluye la libertad de expresión en Internet, prohibiendo que se niegue el servicio o se bloquee la participación de los usuarios por sus opiniones. Además, reconoce el derecho a la rectificación de información publicada en redes sociales u otros servicios equivalentes.
- **Derecho a la actualización de información en los medios de comunicación digitales**: reconoce el derecho a que una noticia u opinión publicada en un medio de comunicación sea corregida si su información no se corresponde con la situación actual.

3.2 Derechos de los menores y la educación

Este bloque está formado por los artículos 83, 84 y 92:

- **Derecho a la educación digital** desde la etapa escolar a la universitaria, abogando por la formación de alumnos y profesores en los conocimientos digitales.

- **La protección de los menores en Internet** también está recogida en la ley, quedando encomendada a los padres y tutores, el ministerio fiscal y los centros educativos u otras entidades que desarrollen actividades en las que participen menores de edad. La publicación de datos personales a través de redes sociales o similares deberá contar con el consentimiento del menor o sus representantes legales.

3.3 Derechos relacionados con el ámbito laboral

Los artículos 87 a 91 recogen una serie de derechos novedosos en el ámbito del trabajo. Los desarrollamos en mayor detalle porque serán doblemente importantes para los futuros técnicos superiores, en su doble vertiente de administradores de sistemas informáticos (como «encargados del tratamiento») y de empleados (como «interesados»):

- **Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral**.
  - **Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad** en el uso de los dispositivos digitales puestos a su disposición por su empleador.
  - **El empleador podrá acceder a los contenidos de medios digitales** facilitados a los trabajadores **sólo para controlar el cumplimiento de las obligaciones** laborales y para garantizar la integridad de dichos dispositivos.
  - **Los empleadores deberán establecer criterios de utilización de los dispositivos digitales** respetando su intimidad según los usos sociales y derechos reconocidos. En su elaboración deberán participar los representantes de los trabajadores.
  - **El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados** requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los periodos en que los dispositivos podrán utilizarse para fines privados.
    Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.
- **Derecho a la desconexión digital en el ámbito laboral.**
  - **Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital** a fin de garantizar, fuera del tiempo de trabajo, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.
  - **El empleador debe elaborar una política interna** en la que definirá las modalidades de ejercicio del derecho a la desconexión.
  - En particular, **se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia.**

- **Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.**
  - **Los empleadores podrán usar cámaras para el control de las funciones laborales de los trabajadores**, que habrán de ser informados previamente.
  - **En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento** de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.
  - **La utilización de sistemas de grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad** de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo.
- **Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.**
  - **Los empleadores podrán usar sistemas de geolocalización** para el control de los trabajadores o los empleados públicos en el ejercicio de sus funciones.
  - **Los empleadores habrán de informar previamente de forma expresa, clara e inequívoca** a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente **deberán informarles acerca del posible ejercicio de los derechos** de acceso, rectificación, limitación del tratamiento y supresión.
- **Derechos digitales en la negociación colectiva.**
  - **Los convenios colectivos podrán establecer garantías adicionales** de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

3.4 Derechos de la era digital y las comunicaciones

Los artículos 93 a 96 recogen una serie de derechos adicionales, que podemos resumir:

- **Derecho al olvido digital**, tanto en buscadores como en redes sociales (no afecta a los medios de comunicación, sino a los buscadores que indexan las noticias y a las redes sociales o servicios similares, que deberán eliminar la información personal a solicitud de la persona afectada).
- **Derecho de portabilidad en servicios de redes sociales** y servicios equivalentes, según el cual los usuarios de redes sociales y similares tendrán derecho a trasladar sus contenidos a otros servicios (si es técnicamente posible).

- **Posibilidad del testamento digital**: regula la eliminación, rescate o conservación del legado digital de una persona después de su fallecimiento. Este legado digital incluye: blogs, perfiles en redes sociales, cuentas de correo electrónico, documentos gráficos y fotográficos digitales, etc.

4 La Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos (AEPD), establecida por el título VII de la LOPD-GDD, es la autoridad administrativa independiente que se encarga de la correcta aplicación de esta ley, así como del Reglamento General de Protección de Datos, en España.

Entre las funciones que tiene atribuidas están las de:

- **Emitir autorizaciones;**
- **Atender peticiones y reclamaciones** formuladas por las personas afectadas;
- **Requerir a los responsables y los encargados de los tratamientos la adopción de medidas** necesarias para la adecuación del tratamiento de datos a las disposiciones;
- En su caso, **ordenar la cesación de los tratamientos e incluso la suspensión de transferencias internacionales de datos;**
- **Imponer sanciones** en virtud de las siguientes leyes:
  - LOPD-GDD, obviamente;
  - Ley 34/2002, de 11 de julio, de **servicios de la sociedad de la información y de comercio electrónico** (conocida como **LSSI**, véase la pág. 16);
  - Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

La AEPD ofrece diversos servicios para ayudar a las organizaciones y empresas a asegurar el cumplimiento de dichos elementos legislativos:

- **La Sede electrónica** permite realizar diversos trámites a través de Internet, como por ejemplo consultar quién es el/la DPD (Delegado/a de Protección de Datos) de alguna organización, **comunicar quién es el/la DPD de nuestra organización/empresa**, presentar reclamaciones, etc.
- **La sección de Guías y publicaciones**, orientadas tanto a personas como a responsables de tratamientos de datos.
- **La sección Derechos,** que nos informa sobre qué derechos tenemos en relación con el tratamiento de nuestros datos, como *interesados*.

- **La sección Deberes,** que nos facilita información sobre qué deberes tenemos a la hora de crear o gestionar tratamientos (como *responsables* o *encargados* de los mismos).
- **La herramienta Facilita RGPD,** que permite a quien la utiliza valorar su situación respecto del tratamiento de datos personales que lleva a cabo: si se adapta a los requisitos exigidos para utilizar *Facilita RGPD* (empresas que tratan datos personales de escaso riesgo, como por ejemplo, datos personales de clientes, proveedores o recursos humanos) o si debe realizar un análisis de riesgos. Además, una vez finalizada su ejecución, los datos aportados durante el desarrollo de la misma se eliminan, por lo que la AEPD no puede conocer la información que haya sido aportada.

III LSSI

Ley de servicios de la sociedad de la información y de comercio electrónico	
Título oficial	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
Objetivo	Incorporar al ordenamiento jurídico español la Directiva europea sobre el comercio electrónico y, en parte, la Directiva europea 98/27/CE (esta última, derogada posteriormente por la Directiva 2009/22/CE).
Fecha de entrada en vigor	12 de octubre de 2002
Texto completo	**BOE-A-2002-13758** (disponible en varios formatos, incluido PDF y ePub)
Predecesoras	–
Estructura y extensión	45 artículos, organizados en siete títulos (más varias disposiciones adicionales, transitorias, etcétera). Aproximadamente 38 páginas.

La LSSI (o LSSICE) determina el régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica. Entiende por «servicio de la sociedad de la información» toda actividad que cumpla los siguientes requisitos:

- Recibe una contraprestación económica;
- La actividad se realiza a distancia por medios electrónicos o telemáticos;
- Se efectúa a petición individual del destinatario del servicio.

En la práctica, la Administración considera que, **siempre que se pueda percibir un ingreso económico** (independientemente de su cuantía) **a través de un medio telemático** (por ejemplo un sitio web), **estamos hablando de una actividad sujeta a esta ley.**

Debemos consultar la LSSI, entre otros casos, **siempre que vayamos a**:

- Prestar algún tipo de servicio a través de Internet (u otros medios telemáticos);
- Hacer uso de algún servicio a través de Internet (u otros medios telemáticos), y:
  - Tengamos algún problema con el proveedor;
  - O necesitemos saber qué obligaciones tendrá el proveedor hacia nosotros;
- Gestionar comunicaciones comerciales, ofertas promocionales, etc. (título III).

1 Aspectos destacables

Vamos a ver, en este punto, algunos aspectos importantes de la LSSICE:

- Información al cliente
- Páginas de enlaces y similares
- Comunicaciones comerciales
- Régimen sancionador

1.1 Información al cliente

De acuerdo con el artículo 10.1 de la ley, el prestador de servicios de la sociedad de la información (por ejemplo, el dueño de una tienda *online)* está 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:

1. Su **nombre o denominación social**; su **residencia o domicilio** o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su **dirección de correo electrónico** y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.
2. Los datos de su **inscripción en el Registro Mercantil**.
3. El **número de identificación fiscal** (NIF) que le corresponda.
4. **Precio(s)** del servicio.

1.2 Páginas de enlaces y similares

Según el art. 17, un sitio web que proporcione enlaces a otros contenidos (o motores de búsqueda de contenidos) no será responsable de la información a la que dirijan dichos enlaces o búsquedas a condición de que:

- No sepa que la información a la que envían los enlaces es ilícita;
- O, si sabe (o se le informa de) que la información referenciada es ilícita, actúa con diligencia para suprimir o anular el enlace.

Es decir, podemos tener una página con enlaces a sitios de descargas, pero si sabemos (o se nos notifica) que un determinado enlace conduce a una descarga ilegal, deberemos eliminarlo.

1.3 Comunicaciones comerciales

Uno de los aspecto que regula la LSSI (artículos 19 a 22) es el envío de comunicaciones comerciales por vía electrónica. Veamos los supuestos de aplicación más comunes en este sentido: el envío de correos electrónicos y SMS-MMS.

El objetivo de la LSSI en este sentido es restringir los mensajes publicitarios no deseados *(spam)*, para lo que exige varios requisitos para el envío de comunicaciones comerciales electrónicas, además de la existencia de consentimiento expreso por parte del destinatario.

El artículo 21.1 **prohíbe el envío de comunicaciones comerciales electrónicas no solicitadas o autorizadas** expresamente por su destinatario (ya sea una persona, organización o empresa). **Si se cuenta con el consentimiento previo y expreso** para el envío de la comunicación comercial, el mensaje enviado deberá cumplir con los siguientes requisitos informativos:

- Identificar claramente el nombre de la persona física o jurídica en nombre de la que se envía el mensaje publicitario;
- **Incluir en el comienzo del mensaje la palabra «Publicidad»** (en los correos electrónicos) **o «Publi»** (especialmente en los SMS).
- **Facilitar al receptor** del mensaje **la posibilidad de revocar el consentimiento** de una forma sencilla y gratuita.

Eso sí, **no será necesario el consentimiento previo** del receptor del mensaje cuando los datos hubieran sido obtenidos a partir de un contrato preexistente, si las comunicaciones tratan de productos o servicios similares a los del contrato.

El envío de comunicaciones comerciales sin el cumplimiento de los requisitos previstos es una **infracción leve** (véase el punto siguiente, *Régimen sancionador)*. Pero **el envío de tres o más comunicaciones comerciales** a un mismo destinatario **en el plazo de un año**, sin cumplir con los requisitos establecidos, constituye una **infracción grave** (ídem).

Dependiendo del uso que demos al correo electrónico, puede ser interesante incluir un texto estándar en nuestros mensajes del estilo del siguiente:

> **PUBLICIDAD:** en cumplimiento de lo previsto en el artículo 21 de la Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE), si usted no desea recibir más información sobre nuestros productos y/o servicios, puede darse de baja enviando un correo electrónico a DIRECCIÓN_DE_CORREO_ELECTRÓNICO, indicando en el Asunto «BAJA» o «NO ENVIAR».

1.4 Régimen sancionador

El título VII, «Infracciones y sanciones», enumera todos los tipos de infracciones penados por la ley, diferenciando entre infracciones leves, graves y muy graves:

Sanciones por incumplimiento de la LSSICE		
Infracciones	**Cuantía**	**Prescripción**
Leves	Hasta 30 000 €	6 meses
Graves	De 30 001 a 150 000 €	2 años
Muy graves	De 150 001 a 600 000 €	3 años

2 El portal de la LSSI

El Gobierno de España pone a disposición del público un portal con información muy completa y actualizada sobre la LSSI. En dicho portal es posible consultar todo tipo de información y dudas. Tanto desde el punto de vista de proveedores de servicios, como desde el de organizaciones, empresas y ciudadanos, merece la pena consultarlo cuando se nos plantee alguna duda con respecto a la ley. Su dirección es la siguiente:

www.lssi.gob.es

IV LPI

Ley de Propiedad Intelectual	
Título oficial	Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
Objetivo	Refundir las disposiciones legales vigentes en materia de propiedad intelectual, regularizando, aclarando y armonizando los textos que hubieran de ser refundidos, e incorporar al ordenamiento jurídico español la Directiva europea 93/98/CEE.
Fecha de entrada en vigor	23 de abril de 1996 (día siguiente a su publicación en el BOE)
Texto completo	**BOE-A-1996-8930** (disponible en varios formatos, incluido PDF y ePub)
Predecesoras	LPI (Ley de Propiedad Intelectual), 1987-1996.[3]
Estructura y extensión	203 artículos, organizados en cuatro libros de varios títulos (más varias disposiciones adicionales, transitorias, etcétera). Aproximadamente 97 páginas.

La LPI establece la gestión legal de los derechos de autor de obras literarias, artísticas y científicas, así como de los programas informáticos. Las obras protegidas incluyen, entre otras:

- **Libros** (incluyendo novelas gráficas o comics)
- **Composiciones musicales**
- **Obras cinematográficas** y similares
- **Fotografías** y similares
- **Programas de ordenador**

Hay que tener en cuenta que **los derechos de autor surgen en el mismo momento en que se crea una obra**; no es necesario hacer ningún trámite para que un autor disfrute de los derechos correspondientes a su obra.

La LPI no afecta a los técnicos informáticos en mucha mayor medida que al resto de la ciudadanía. Los casos particulares que pueden requerir un poco más de atención son:

- El uso de programas informáticos;
- El uso, almacenamiento o transmisión de obras sujetas a derechos de autor.

3 Esta ley fue sufriendo, con el transcurso de los años, diversas adiciones y modificaciones. El RD vigente deroga dicha ley, para crear una nueva con todas las modificaciones añadidas, que sigue manteniendo el nombre de Ley de Propiedad Intelectual (LPI).

1 Derechos de autor

La LPI reconoce dos tipos de derechos: los derechos morales, y los derechos de explotación.

Los **derechos morales** son irrenunciables e inalienables (el autor[4] no puede renunciar a ellos, y no se los puede traspasar a nadie más). Son, entre otros, los siguientes:

- Derecho a **decidir si publicar** su obra y cómo hacerlo
- Derecho a **ser reconocido** como autor
- Derecho a la **integridad de la obra** y a impedir cualquier modificación o atentado contra ella que suponga perjuicio a sus legítimos intereses o a su reputación

Los **derechos de explotación** son los correspondientes a la obtención de una retribución por la obra creada. Son los siguientes:

- **Explotación**: el autor puede explotar su obra libremente conforme a la ley.
- **Reproducción**: el autor puede efectuar la fijación directa o indirecta, provisional o permanente, por cualquier medio y en cualquier forma, de toda la obra o de parte de ella, que permita su comunicación o la obtención de copias.
- **Distribución**: el autor puede poner a disposición del público el original o copias de la obra, en un soporte tangible, mediante su venta, alquiler, préstamo, etc.
- **Comunicación pública**: el autor puede otorgar acceso a la obra a una pluralidad de personas a la obra sin previa distribución de ejemplares a cada una de ellas (no se considerará pública la comunicación en el ámbito doméstico si no está integrada o conectada a una red de difusión de cualquier tipo).

Los derechos de explotación caducan 70 años después del fallecimiento del autor. Durante ese tiempo (tras el fallecimiento del autor) pueden ser ejercidos por sus herederos.

Como curiosidad cabe señalar que esta desmesurada duración de los derechos de autor tiene su origen en las labores de presión política desarrolladas por la Corporación Disney en EE.UU. a lo largo del siglo XX.

2 La copia privada

La copia privada es una limitación a la explotación de los derechos de autor: en pocas palabras, la LPI autoriza a ciudadanos particulares a realizar y disfrutar de copias privadas de obras de todo tipo (excepto programas de ordenador), bajo ciertas condiciones y con ciertas restricciones importantes.

4 Siguiendo la redacción de la ley, usaremos el término «autor» para referirnos igualmente a autores y autoras.

La copia privada constituye uno de los campos de batalla más reñidos de nuestra legislación, ya que se aúnan en él los siguientes aspectos:

- La existencia de (muy) poderosos *lobbies* que ejercen toda la influencia política que pueden para modificar la legislación a su gusto;
- Unos usos y costumbres de la ciudadanía muy arraigados, que la ley defiende en mayor o menor medida;
- Una legislación poco clara, con múltiples elementos involucrados en este asunto.

La escasa claridad de la legislación ha determinado que muchos conflictos acaben en los tribunales que, poco a poco, van sentando jurisprudencia. En este punto vamos a analizar los aspectos de la copia privada que están claros.

2.1 Puntos básicos con respecto a la copia privada

1. **La copia privada no es legal para uso profesional.** Sobre esto no cabe duda: la copia privada sólo se permite a las personas físicas (es decir, no organizaciones ni empresas) para uso privado.
2. **La copia privada no puede hacerse con fines de lucro.** No se puede hacer copias de obras para venderlas, alquilarlas, ni obtener beneficios económicos de ninguna otra manera.
3. **La copia privada no está permitida para programas informáticos ni bases de datos.** Sólo está permitida para libros, películas, imágenes, etc.
4. **La copia privada, recogida en el art. 31 de la LPI, cambia cada pocos años** (hasta ahora en 1998, 2006, 2015 y 2017), en función de las presiones de las partes interesadas. Por ello puede ser necesario examinar de vez en cuando el contenido de la ley.
5. **La copia privada se compensa a los autores con un canon.** El famoso *canon por copia privada* tasa todos los artículos susceptibles de ser usados para copias privadas con un impuesto que se destina a compensar a los autores. Esto afecta, por ejemplo, a fotocopiadoras, unidades de memoria USB, lectoras y grabadoras de discos ópticos, impresoras, etc.
6. **Los usuarios profesionales pueden reclamar la devolución del canon.** Este derecho no es tan fácil de llevar a la práctica pero, dado que el uso profesional de copias privadas es ilegal, los dispositivos adquiridos para uso profesional no pueden ser gravados con el canon descrito en el punto anterior, y se puede solicitar su devolución.

Hasta aquí las certezas. Hay otra serie de puntos que parecen ir afianzándose en la jurisprudencia, pero que no están completamente claros, y pueden depender del criterio de un juez o la interpretación que haga un fiscal de la ley.

2.2 El ámbito de la copia privada

Como hemos dicho, la copia privada se circunscribe a la vida privada de las personas, a su intimidad. Por tanto, se aleja del alcance y objetivos de estos apuntes.

Ejercer el derecho de copia privada es, desde el punto de vista legal, una tarea llena de áreas grises en las que no está clara la legalidad o ilegalidad de muchas prácticas permitidas por la tecnología. Además, la legislación cambiante hace que determinadas prácticas hayan podido pasar de ser legales a ilegales —o viceversa— a lo largo de los años. Y, por si fuera poco, día a día sigue habiendo un enfrentamiento furibundo entre defensores y detractores del derecho a la copia privada.

Para quien esté interesado en el tema, recomendamos seguir las noticias y comentarios de David Bravo (abogado especializado en derecho informático, notoriamente en propiedad intelectual; merece particularmente la pena seguir su actividad en Twitter), así como de Carlos Sánchez Almeida (abogado especialista en delitos informáticos y Derecho en Internet).

3 Programas informáticos

El título VII de la ley se refiere exclusivamente a los programas informáticos. Entre otros puntos de interés, cabe resaltar que:

- Los programas desarrollados en el ejercicio de las funciones de un trabajo asalariado generan derechos de explotación a favor de la empresa; es decir, si creas un programa en tu trabajo, los derechos de explotación no son tuyos, son de la empresa (art. 97.4).
- La reproducción (copia) de un programa informático, incluso para uso personal, debe contar con el permiso del titular del derecho (art. 99 a).
- Pueden efectuarse copias sin permiso cuando sean simples copias de seguridad para uso de la misma persona u organización que ha adquirido el software (art. 100.2)

Existen algunas limitaciones y derechos adicionales que pueden ser útiles en determinadas circunstancias, cuando haya necesidad de modificar un programa adquirido. En tal caso es útil consultar el título VII de la LPI.

Según el artículo 102 **es ilegal:**

- **Poner en circulación copias ilegítimas** de programas;
- **Poseer con fines comerciales copias ilegítimas** de programas;
- Poner en circulación o poseer con fines comerciales cualquier instrumento cuyo único uso sea anular la protección de un programa de ordenador. En otras palabras, **poner en circulación o poseer «cracks», «keygens» o similares** para poder utilizar progra-

mas protegidos (con pena de prisión de entre seis meses y tres años, según el art. 270.6 del Código Penal).

3.1 El software *pirata* en el Código Penal

El uso de software ilegal es un delito castigado con dureza en el código penal. **Las organizaciones o empresas que no hayan adoptado medidas para evitar que sus equipos tengan software ilegal son penalmente responsables** de su uso pudiendo aplicarse las penas previstas, además de las correspondientes indemnizaciones: multas de hasta 280 000 euros, suspensión de actividades, clausura de locales, inhabilitación para obtener contratos, subvenciones y ayudas de las administraciones públicas e intervención judicial o incluso la disolución de la persona jurídica.

Además, los administradores de algún software ilegal podrían encarar **hasta cuatro años de prisión**, **además de multas similares a las previstas** para las personas jurídicas.

4 Alternativas a las obras protegidas

En muchos casos las organizaciones pueden preferir no asumir los costes necesarios para poder hacer uso de obras protegidas. En tal caso existe la posibilidad de emplear obras que se ofrezcan libremente para uso, o con restricciones que no impidan su utilización a nuestra organización.

Para ello podemos buscar en Internet obras (¡y software!) que cumplan alguna de estas condiciones:

- Estar en el dominio público, o haberse publicado renunciando a los derechos de autor (en realidad a los derechos de explotación);
- Que haya prescrito su plazo de protección;
- Que se hayan publicado con licencias menos restrictivas, como ***Creative Commons***, y que la licencia empleada permita su uso en nuestro caso.

Muchas organizaciones han venido descubriendo en los últimos años que hay gran cantidad de trabajos de calidad publicados renunciando a los derechos de autor, o bajo las normas *Creative Commons*, y que no necesitan acudir a obras protegidas ni pagar a las entidades gestoras de sus derechos.

Observa, por ejemplo, que estos apuntes están creados y publicados con una licencia CC-BY-NC-SA. Tienes toda la información en la página 3: el tipo de licencia que es, qué significa, y los derechos que tienes con respecto al documento.

V Legislación internacional

Existe un buen número de leyes y tratados internacionales relativos a la seguridad informática. Aquí proporcionamos los datos de varios de ellos, para facilitar su consulta.

1 Unión Europea

Obviando el RGPD, ya estudiado por su trascendencia, otras normas importantes son:

Directiva de medidas para la seguridad en redes y sistemas de información	
Título oficial	Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión
Objetivo	Establecer medidas con el objeto de lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior. Entre otros puntos: • establece obligaciones para todos los Estados miembros de **adoptar una estrategia nacional de seguridad** de las redes y sistemas de información; • **crea una red de equipos de respuesta a incidentes de seguridad informática** («red de CSIRT»); • establece **requisitos de seguridad y notificación** para los **operadores de servicios esenciales** y para los **proveedores de servicios digitales**; • obliga a los Estados miembros a designar **autoridades nacionales competentes, puntos de contacto únicos** y **CSIRT** con funciones relacionadas con la seguridad de las redes y sistemas de información.
Fecha de entrada en vigor	10 de mayo de 2018 (fecha de publicación: 19/7/2016)
Texto completo	**Documento 32016L1148** (disponible en formatos HTML y PDF)
Estructura y extensión	26 artículos, organizados en siete capítulos, más un anexo dedicado a los CSIRT. En total, unas 30 páginas.

Reglamento relativo a ENISA y a la certificación de la ciberseguridad	
Título oficial	Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las TIC
Objetivo	Establecer los objetivos, tareas y aspectos organizativos relativos a ENISA (Agencia de la Unión Europea para la Ciberseguridad). Facilitar la creación de esquemas europeos de certificación de la ciberseguridad.
Fecha de entrada en vigor	27 de junio de 2019 (fecha de publicación: 7/6/2019)
Texto completo	**Documento 32019R0881** (disponible en formatos HTML y PDF)
Predecesores	Reglamento de creación de la Agencia Europea de Seguridad de las Redes y de la Información (Reglamento (CE) n.º 460/2004), 2004-2013 Reglamento sobre la Ciberseguridad (Reglamento (UE) n.º 526/2013), 2013-2018
Estructura y extensión	69 artículos, organizados en cuatro títulos, más un anexo. En total, unas 55 páginas.

2 Consejo de Europa

El Consejo de Europa es una institución internacional fundada después de la SGM para defender los Derechos Humanos, la democracia y el dominio de la Ley. No tiene nada que ver con la Unión Europea, aunque es fácil de confundir, porque usan la misma bandera e himno. Cuenta con 47 estados miembros, que representan una población de unos 820 millones de habitantes.

Convenio de Budapest sobre ciberdelincuencia	
Título oficial	*Treaty No. 185: Convention on Cybercrime*
Objetivo	• Armonizar el derecho penal y disposiciones relacionadas de los países signatarios con respecto a los delitos informáticos. • Proporcionar el derecho procesal necesario para la investigación y el enjuiciamiento de esos delitos, así como otros delitos cometidos por medio de un sistema informático o con evidencias en formato digital. • Establecer un régimen rápido y eficaz de cooperación internacional.
Fecha de entrada en vigor	1 de octubre de 2010 (para España)
Texto completo	**BOE-A-2010-14221** (disponible, entre otros formatos, en HTML y PDF)
Estructura y extensión	48 artículos, organizados en cuatro capítulos, más un anexo sobre la ratificación. En total, 21 páginas (sin contar el anexo).

Aunque este convenio es propio del Consejo de Europa, muchos otros países del mundo se han adherido a él. El Convenio de Budapest tiene su propia página web.

Existe un protocolo adicional al Convenio de Budapest: el **Protocolo adicional a la Convención en Cibercrimen, respecto de la criminalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos**. Este protocolo adicional, creado el 2003 (y ratificado por España en diciembre de 2014), tiene como objetivo que los estados participantes penalicen la difusión de material, amenazas y ofensas racistas y xenófobos por medio de sistemas informáticos.

3 Naciones Unidas

La Organización de Naciones Unidas también tiene un amplio surtido de reglas, acuerdos, directrices (y un largo etcétera), centrados en la seguridad informática.

Estos son algunos de los más relevantes:

Principios rectores aplicables a los ficheros informatizados de datos personales	
Título oficial	Resolución 45/95: Principios rectores para la reglamentación de los ficheros computadorizados de datos personales
Objetivo	Establecer orientaciones para las legislaciones nacionales referentes a la gestión de ficheros de datos personales, incluyendo una serie de garantías mínimas
Fecha de aprobación	14 de diciembre de 1990
Texto completo	es/A/RES/45/95 (disponible en HTML)
Estructura y extensión	10 principios más una sección relativa a los ficheros de organizaciones internacionales gubernamentales. Aproximadamente 3 páginas.

Derecho a la privacidad en la era digital	
Título oficial	Resolución 73/179: El derecho a la privacidad en la era digital
Objetivo	Defender el derecho a la privacidad digital, y particularmente en Internet
Fecha de aprobación	17 de diciembre de 2018
Texto completo	es/A/RES/73/179 (disponible en PDF)
Estructura y extensión	Un largo preámbulo y 11 puntos. Siete páginas.

VI Normas ISO: seguridad de la información

Las normas ISO son disposiciones o estándares establecidos por la ISO[5] y la IEC,[6] relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacional o mundial, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.

En concreto, **ISO/IEC 27000** es una familia (en crecimiento) de estándares sobre ***sistemas de gestión de la seguridad de la información*** **(SGSI)**. Contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para SGSI, utilizables por cualquier tipo de organización.

Dentro de la familia ISO/IEC 27000, distinguimos, entre otros:

Norma	Descripción
ISO/IEC 27000	Vocabulario estándar para el SGSI para todas las normas de la familia.
ISO/IEC 27001	**Es la norma más importante de la familia.** Especifica los **requisitos necesarios para implantar un SGSI certificable** conforme a las normas 27000. • Define el SGSI, cómo se gestiona y las responsabilidades de los participantes. • Sigue un modelo PDCA *(Plan-Do-Check-Act)* • Los puntos claves son: (1) Gestión de riesgos y (2) la Mejora continua.
ISO/IEC 27002	Es un **código de buenas prácticas para la gestión de la seguridad**. Consiste en: • Recomendaciones para asegurar los sistemas de información de una organización. • Objetivos de control (aspectos que analizar para garantizar la seguridad de la información) y especifica los controles recomendados que hay que implantar.
ISO/IEC 27003	**Directrices para la implementación de un SGSI**. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010. No está certificada actualmente.
ISO/IEC 27004	**Métricas para la gestión de seguridad de la información**. Proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.
ISO/IEC 27005	Normativa dedicada a la **gestión de riesgos en seguridad de la información**. Suministra directrices para gestionar los riesgos que puede sufrir la información de una empresa.
ISO/IEC 27007	Guía para certificadores y auditores (internos o externos) en su trabajo **para certificar la implementación del estándar ISO/IEC 27001** por parte de las empresas.
ISO/IEC 27014	Guía de ideas y principios para el **gobierno corporativo** de la seguridad de la información.
ISO/IEC 27017	Pautas y directrices sobre los controles de seguridad de la información relacionadas con **servicios en la nube**.
ISO/IEC 27032	líneas generales de orientación para fortalecer el estado de la **ciberseguridad en una empresa**, centrándose en diferentes aspectos técnicos y otros relacionados: • Seguridad en las **Redes y en Internet**. • Seguridad de la **Información**. • Protección de las **Infraestructuras Críticas para la Información**.

5 Organización Internacional para la Estandarización
6 Comisión Electrotécnica Internacional

ISO/IEC 27701	Extensión de privacidad para mejorar un SGSI existente con requisitos adicionales para crear, mantener y mejorar un Sistema de Gestión de Información de Privacidad (PIMS)

Las normas ISO no son de cumplimiento obligatorio, **pero ofrecen una garantía de calidad** a las personas y organizaciones con las que se relaciona nuestra propia organización o empresa.

Para mucha gente, **la obtención de una certificación ISO es una forma de promoción**, dando a entender «al mundo» que la organización se toma en serio los aspectos certificados. En empresas dedicadas a la seguridad informática, la obtención del certificado ISO 27001 es prácticamente indispensable; pero cualquier organización puede optar a obtener esta certificación.

Por otra parte, algunas empresas especializadas tienen como negocio ayudar a otras organizaciones a obtener esta certificación.

VII La Administración electrónica

La posibilidad de relacionarse con la administración a través de Internet constituye un fin tan práctico y deseable para los ciudadanos como para las diferentes administraciones públicas.

Desde el año 2004, se han puesto en marcha múltiples iniciativas para impulsar el desarrollo de la Administración electrónica en España y mejorar la atención a los ciudadanos.

Los principales elementos catalizadores actuales de la administración electrónica son:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público

Estas dos leyes establecen el **derecho universal de los ciudadanos a relacionarse con todas las administraciones públicas de manera electrónica**. El objetivo es promover una Administración más eficiente, eficaz, cercana y transparente.

El **Portal de Administración electrónica** **(PAe)** es un sitio web de la Secretaría General de Administración Digital, dependiente del Ministerio de Asuntos Económicos y Transformación Digital. En él se recoge toda la información con respecto a la implantación de la Administración digital, así como el catálogo de servicios que se ofrecen por vía electrónica desde la Administración Pública.

Desde el punto de vista de los ciudadanos/usuarios, hay tres pilares fundamentales para gestionar el acceso a la Administración electrónica:

- El sistema Cl@ve
- El Punto de Acceso General (PAG)
  - La Carpeta Ciudadana

1 El sistema Cl@ve

Cl@ve es un sistema orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos. Su objetivo principal es que el ciudadano pueda identificarse ante la Administración mediante claves concertadas (usuario más contraseña), sin tener que recordar claves diferentes para acceder a los distintos servicios.

Cl@ve contempla la identificación en base a dos principios diferentes:

- Identificación basada en certificados electrónicos:
  - Certificados de AC reconocidas, como la FNMT o la ACCV. Las AC reconocidas figuran en la Lista de confianza de prestadores cualificados de servicios electrónicos de confianza (TSL) del Ministerio de Industria, Comercio y Turismo;
  - DNI electrónico;
- Claves concertadas (sistemas de usuario y contraseña). En lo que respecta a las claves concertadas, Cl@ve admite dos posibilidades de uso:
  - **Cl@ve ocasional** (**Cl@ve PIN**): sistema de contraseña de validez muy limitada en el tiempo, orientado a usuarios que acceden esporádicamente a los servicios, que se corresponde con el sistema PIN24H de la Agencia Tributaria;
  - **Cl@ve permanente**: sistema de contraseña de validez duradera en el tiempo (aunque no ilimitada) orientado a usuarios habituales. Se corresponde con el sistema de acceso mediante usuario y contraseña, reforzado con claves de un solo uso por SMS, a los servicios de Seguridad Social. Este sistema será además el que permitirá el acceso al ciudadano a la firma en la nube.

Para poder utilizar estas claves concertadas y los servicios de *firma en la nube*[7] es necesario registrarse previamente en el sistema, aportando los datos de carácter personal necesarios.

2 El Punto de Acceso General

El **Punto de Acceso General** **(PAG)** constituye un punto único de acceso para el ciudadano a información de interés de los diversos ministerios, organismos públicos vinculados o dependientes, así como a información sobre empleo público, ayudas, subvenciones, becas y normativa de interés de las Administraciones Públicas y de la Unión Europea (UE).

Da acceso a los sitios web oficiales de los Departamentos ministeriales, organismos autónomos, comunidades autónomas, entidades locales, así como a sus sedes electrónicas.

Además, ofrece —a ciudadanos y empresas— acceso a los procedimientos (trámites) y servicios electrónicos de las Administraciones Públicas agrupados por materias, así como a información sobre el funcionamiento y organización de las Administraciones Públicas y el Estado.

Este portal también ofrece atención personalizada a través de un buzón de atención y un servicio de *webchat* en línea. Otros canales de atención son el teléfono **060** y las redes sociales.

7 La **firma en la nube** es una firma electrónica mediante certificados electrónicos centralizados, es decir, certificados electrónicos almacenados y custodiados por la Administración Pública. Estos certificados centralizados, o «certificados en la nube» permiten al ciudadano firmar documentos electrónicos desde cualquier dispositivo que tenga conexión a Internet y sin ningún equipamiento adicional.

El PAG dispone de un área restringida para los usuarios, a la que se accede previa autentificación (identificación electrónica), llamada Carpeta Ciudadana, que veremos a continuación.

2.1 La Carpeta Ciudadana

La **Carpeta Ciudadana** es un portal web que pretende facilitar la relación con las Administraciones Públicas. Desde ella se puede acceder a:

- Al estado de los expedientes del ciudadano/usuario;
- A sus notificaciones;
- A sus datos personales registrados en la Administración;
- A sus registros.

El acceso a este portal requiere, como era de esperar, el uso de la identificación a través de **Cl@ve**.

Entre otros, es posible consultar los estudios cursados (Primaria, Secundaria, FP, Bachillerato, Universidad, Certificados de Idiomas, etc.), domicilio, antecedentes penales y similares (y solicitar certificados al respecto), carné de conducir, puntos disponibles del mismo, y un largo etcétera.

VIII Anexo I: Notificaciones en el correo electrónico

En base a lo visto en la legislación, fundamentalmente la LOPD-GDD y la LSSI, es habitual encontrar en las comunicaciones profesionales por correo electrónico cláusulas de notificación para el recipiente.

En la página 10 hemos visto un ejemplo de notificación en función de la LOPD-GDD, que podemos usar, a condición de que la adaptemos a nuestras condiciones (seguramente el texto necesitará ser modificado dependiendo de la gestión de datos que haga nuestra organización/empresa).

Y **en la página 18 hemos visto un ejemplo de notificación en función de la LSSICE**, que podemos usar, en particular, en el caso de mensajes de correo informativos (o publicitarios) para nuestros contactos o clientes.

Por otra parte, muchas organizaciones añaden una **cláusula de privacidad o confidencialidad** en sus mensajes de correo electrónico. Dependiendo de la redacción, los mensajes pueden resultar amenazantes, exigiendo a la persona receptora eliminar el mensaje (incluso sin leerlo) si no está destinado a ella. Estas cláusulas, que muchas veces advierten de «poder estar contraviniendo la ley» si no se procede como ordenan, intentan usar el miedo del receptor para que elimine el mensaje si no está destinado a él. Sin embargo **carecen de todo sustento legal**: cuando una persona recibe un mensaje de correo electrónico, puede hacer con él prácticamente lo que quiera, mientras no contravenga la ley (por ejemplo, no puede divulgar datos privados de otras personas que figuren en el correo electrónico). En lugar de recurrir al *FUD*,[8] es más elegante usar una redacción parecida a esta, donde se solicita al receptor que actúe de la forma más adecuada (para nosotros):

> **CLÁUSULA DE CONFIDENCIALIDAD:** este *e-mail* y cualquiera de sus ficheros anexos son confidenciales y pueden constituir información privilegiada. Si usted no es el destinatario adecuado, por favor, notifíquelo inmediatamente al emisor y no revele estos contenidos a ninguna otra persona, no los utilice para otra finalidad, ni almacene o copie esta información en medio alguno.

8 FUD es el acrónimo en inglés de las palabras ***Fear, Uncertainty and Doubt*** (es decir, «Miedo, Incertidumbre y Duda»). Se suele aplicar a todo tipo de comunicaciones en las que se usa información negativa, vaga o sesgada —en lugar de información simplemente honesta y veraz— con el objeto de convencer a alguien de algo que interese al emisor.

IX Bibliografía

DEL PESO NAVARRO, E. (2009) Los diferentes personajes de la LOPD. IEE.

LOECHES MÁRQUEZ, A. (2018) La nueva LOPD. Consejo General de la Abogacía Española.

DESC. (2020) ¿Qué es la LOPDGDD y cómo se aplica? Consecuencias del nuevo marco legal. Cybot A/S.

DCD. (2018) La garantía de los derechos digitales en la nueva LOPD. DCD, SA.

DESC. (20??) Agencia Española de Protección de Datos. Wolters Kluwer.

Aula MENTOR. Normas ISO sobre gestión de seguridad de la información. Ministerio de Educación, Cultura y Deporte.