

# CURSO e-ABOGACÍA

2

# CURSO e-ABOGACÍA

## Presentación del curso

El Consejo General de la Abogacía Española (en adelante, CGAE) le da la bienvenida al curso e-Abogacía.

Como órgano representativo, coordinador y ejecutivo superior de los Ilustres Colegios de Abogados de España, el CGAE representa a la Abogacía Española y es portavoz del conjunto de los Ilustres Colegios de Abogados de España.

Como parte de sus funciones, CGAE colabora con los colegios de abogados para facilitar el acceso a la vida profesional de los recién titulados, y organiza, como en este caso, cursos para la formación profesional de los abogados y de los colegiados no ejercientes.

El objetivo fundamental del curso e-Abogacía es dar a conocer las ventajas que la práctica profesional electrónica aporta a los abogados en términos de tiempo, costes y facilidad de comunicación con sus clientes, colegas de profesión, colegios de abogados y Administraciones Públicas.

El éxito de la implantación de este curso pasa por que el alumno pueda familiarizarse y conocer por sí mismo la capacidad, utilidad y mejoras que el nuevo entorno tecnológico supone, eliminando desde la base los posibles temores o desconfianza que surgen siempre a lo desconocido y aparentemente complejo. Con este fin, se revela como necesario abarcar conceptos progresivamente complejos, por lo que el curso se ha estructurado en tres módulos de dificultad creciente, como veremos más adelante.

Durante las nueve sesiones de que consta el curso, el abogado conocerá los aspectos tecnológicos que rodean a los servicios electrónicos desarrollados por parte de la abogacía institucional y las Administraciones Públicas para el ejercicio de su profesión, capaces de agilizar su actividad y reducir los costes derivados de los trámites habituales.

La formación a impartir en el curso e-Abogacía incorpora los aspectos recogidos en la normativa europea que regula la firma electrónica y el comercio electrónico.

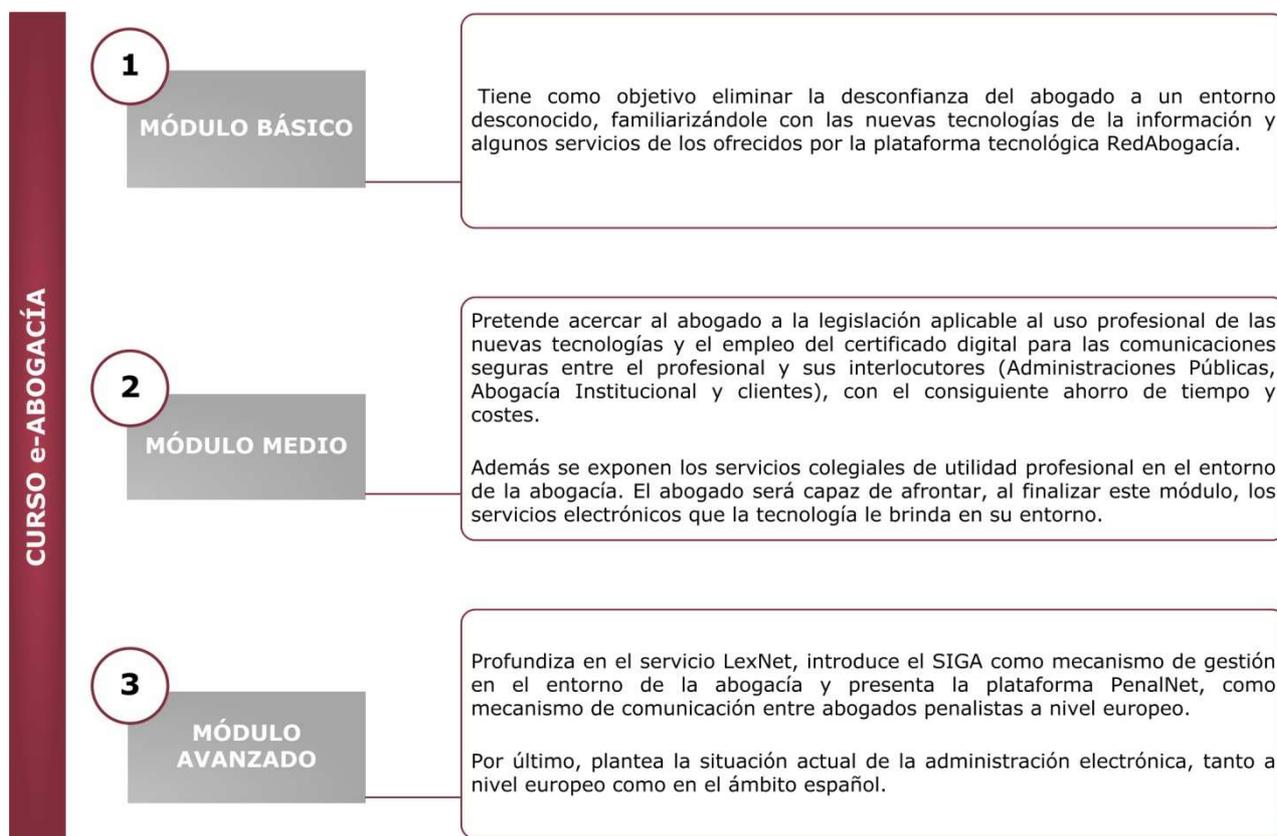
*(Directivas 99/93/CE y 2000/31/CE, y Leyes 59/2003 y 34/2002 de Firma Electrónica y de Servicios de la Sociedad de la Información, respectivamente)*

## Estructura del curso

El curso e-Abogacía se pone en marcha como complemento necesario al proyecto tecnológico emprendido desde el año 2004 por la abogacía institucional, y que se materializa en el uso de firma electrónica y desarrollo de servicios en RedAbogacía.

Este curso es una iniciativa del CGAE para formar a colegiados de todo el territorio nacional en nuevas tecnologías y servicios electrónicos orientados al ejercicio de la abogacía.

El curso e-Abogacía consta de nueve sesiones formativas estructuradas en tres módulos (básico, medio y avanzado) que abordan, como veremos a continuación, los siguientes niveles de conocimiento:



Para la obtención de la titulación correspondiente al curso e-Abogacía, el alumno deberá completar los test evaluativos correspondientes a cada uno de los módulos

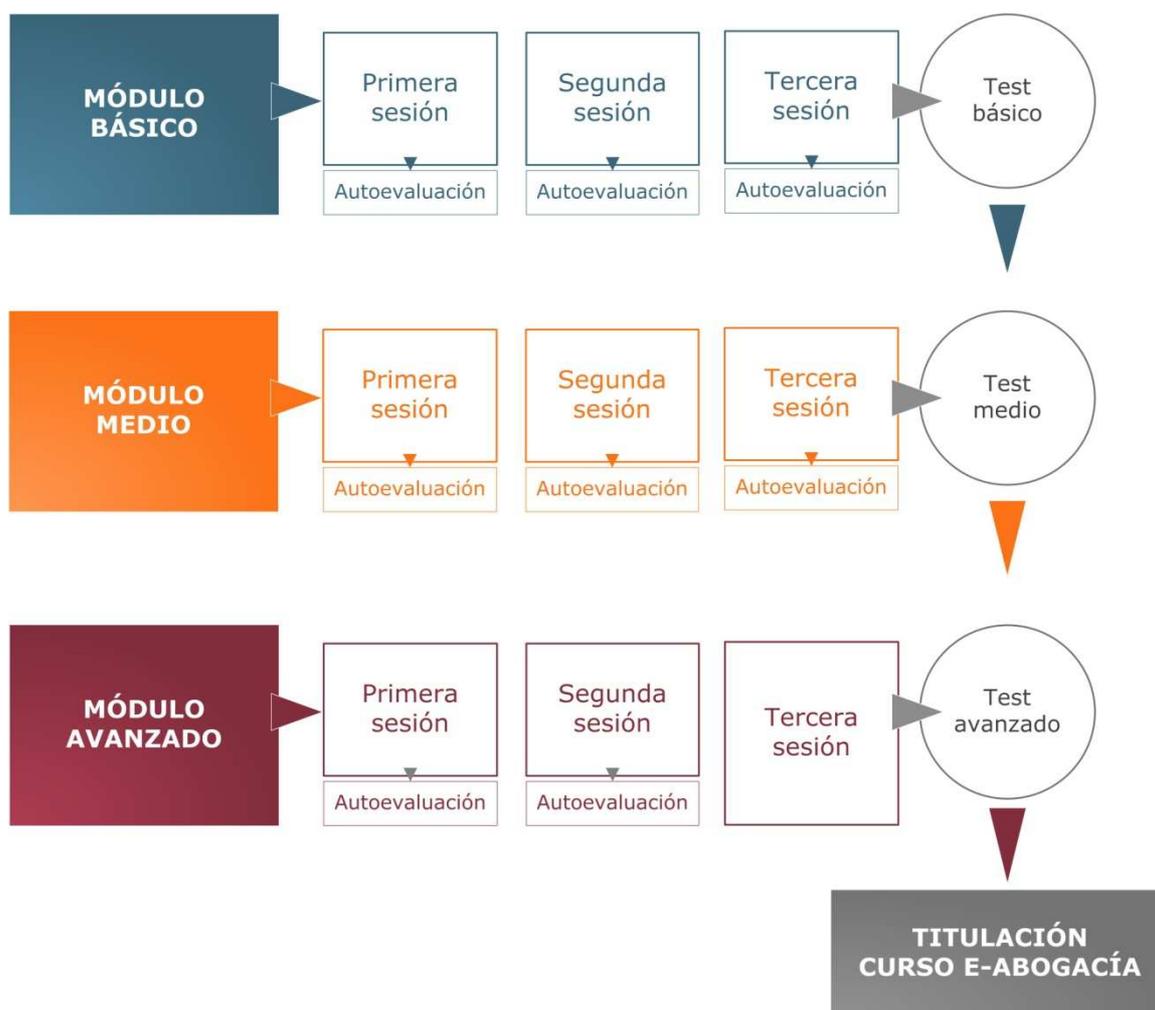
La asistencia al módulo básico es de carácter opcional para los alumnos introducidos en el manejo de ordenador e Internet. Igualmente, quienes estén familiarizados con los conceptos relativos a la certificación digital y los servicios electrónicos sencillos podrán prescindir de la asistencia al módulo intermedio.

En cualquier caso, si el alumno prefiere no asistir a alguno de los dos primeros módulos, deberá superar los test evaluativos correspondientes a cada módulo con el fin de acreditar que posee efectivamente los conocimientos objeto de la formación.

Estos test evaluativos, de tipo test, se deberán realizar obligatoriamente desde la plataforma de e-learning dispuesta en la zona privada que tiene el colegio en RedAbogacía, a la que los alumnos deben acceder con su certificado digital de abogado ACA.

Este tipo de test evaluativo, que supone una experiencia pionera en nuestro país, garantiza la identidad del examinando, su aprovechamiento y la seguridad en las comunicaciones, además de proveerle con su nuevo carné colegial con certificado digital de la Autoridad de Certificación de la Abogacía.

A continuación reflejamos de forma esquemática la estructura de los módulos y exámenes:



## Recomendaciones al Usuario para la realización del Curso e-Abogacía

A continuación daremos unas recomendaciones al usuario con el objetivo de que éste obtenga el máximo aprovechamiento del curso.

El **servicio Campus virtual** permite a los abogados acceder a la plataforma de **cursos online**, con la posibilidad de examinarse para posteriormente obtener un certificado de aprovechamiento en el **“Curso e-Abogacía para el uso de servicios con certificado digital”** expedido por el CGAE.

### RECOMENDACIONES

---

- 1.** Para abordar el estudio de cada uno de los módulos (básico, medio y avanzado) haga uso de los materiales didácticos que se ponen a disposición en la plataforma de cursos online. El contenido de estos se encuentra desarrollado en **tres manuales** correspondientes a cada uno de los módulos, cuya estructura se ha explicado en el apartado anterior.
- 2.** Tras finalizar cada capítulo es aconsejable que realice los correspondientes **ejercicios** para afianzar en la práctica los conceptos que haya adquirido en la lectura y análisis de los contenidos.
- 3.** El usuario dispone de **3 locuciones con presentaciones gráficas** que podrán servir de **material de apoyo** a los contenidos de estos módulos. El objetivo de estas presentaciones es mostrar al usuario de manera más esquemática todos los aspectos ampliamente desarrollados en las distintas sesiones. Por lo que **se recomienda que el usuario tras finalizar cada uno de los módulos acceda a la zona virtual correspondiente y visualice la locución correspondiente con el fin de refrescar y afianzar los conceptos más importantes.**
- 4.** Tras finalizar cada sesión es aconsejable que realice la **autoevaluación**, que consiste en un conjunto de preguntas tipo test que abarcan aspectos teóricos de los contenidos expuestos en cada uno de los módulos.
- 5.** Además el usuario tiene a su disposición un conjunto amplio de **información en forma de manuales** (sobre servicios de Buromail, Oficina Postal, LexNet...), artículos relacionados con los temas expuestos, legislación vigente de interés, etc.

#### PRIMERA SESIÓN

REGULACIÓN DE LAS TIC

#### SEGUNDA SESIÓN

SEGURIDAD DE LA  
INFORMACIÓN

#### TERCERA SESIÓN

SERVICIOS ELECTRÓNICOS  
PARA EL EJERCICIO DE LA  
ABOGACÍA

# Módulo medio



En el módulo medio podrá aprender, entre otras cuestiones, las siguientes:

- Exposición del régimen jurídico de las TIC: firma electrónica, servicios de la sociedad de la información, protección de datos personales, propiedad intelectual, y telecomunicaciones.
- La firma electrónica en sus relaciones jurídico-públicas.
- Los problemas de seguridad informática y las herramientas para solventarlos de manera rápida y eficaz.
- La seguridad en el correo electrónico: cómo cifrar y firmar digitalmente un correo electrónico.
- Los servicios colegiales de utilidad profesional a través de RedAbogacía: Buromail, Campus virtual, Iuris et Legis, Libros, e-Mensajes, Oficina Postal y Oficina de catastro.
- Los servicios disponibles a través de RedAbogacía con las Administraciones Públicas.

Al final del módulo el alumno deberá superar un test de evaluación para la obtención del título propio "Curso e-Abogacía para el uso de servicios con certificado digital". El test se realizará online y el alumno se identificará utilizando su certificado digital ACA.

PRIMERA SESIÓN	SEGUNDA SESIÓN	TERCERA SESIÓN
<b>REGULACIÓN DE LAS TIC.....08</b>	<b>SEGURIDAD DE LA INFORMACIÓN.....82</b>	<b>SERVICIOS ELECTRÓNICOS PARA EL EJERCICIO DE LA ABOGACÍA.....106</b>
<p><b>CAP.1_Régimen jurídico de las TIC.....09</b></p> <p>1.1 Firma electrónica 1.2 Servicios de la Sociedad de la Información 1.3 Protección de datos personales 1.4 Propiedad intelectual 1.5 Telecomunicaciones Ejercicios Prácticos</p> <p><b>CAP.2_La firma electrónica en las relaciones jurídico-públicas.....66</b></p> <p>2.1 Introducción 2.2 Eficacia y necesidad de la firma electrónica en las relaciones jurídico-públicas 2.3 Problemas procesales de la firma electrónica Puntos Clave</p> <p><b>CAP.3_Interoperabilidad.....72</b></p> <p>3.1 Introducción 3.2 Marco de Interoperabilidad de las AA.PP. europeas y españolas Puntos Clave</p>	<p><b>CAP.1_Seguridad informática.....83</b></p> <p>1.1 Importancia de la Información 1.2 Problemas de Seguridad Puntos Clave</p> <p><b>CAP.2_Solventar problemas de seguridad .....89</b></p> <p>2.1 Clasificación de herramientas 2.2 Solución a problemas de tecnología 2.3 Solución a problemas de procesos 2.4 Solución a problemas de personal Puntos Clave</p> <p><b>CAP.3_Seguridad en el correo electrónico .....93</b></p> <p>3.1 El papel del certificado digital en el correo electrónico 3.2 Cómo puedo firmar digitalmente un correo electrónico 3.3 Cómo puedo firmar digitalmente un documento 3.4 Cifrado del correo electrónico Puntos Clave</p>	<p><b>CAP.1_Servicios colegiales de utilidad profesional.....107</b></p> <p>1.1 Buomail 1.2 Campus virtual 1.3 Iuris et Legis 1.4 RedAbogacía Libros 1.5 e-Mensajes 1.6 Oficina postal 1.7 Oficina de catastro Puntos Clave</p> <p><b>CAP.2_Servicios de las Administraciones Públicas.....147</b></p> <p>2.1 Servicios de las AA.PP. estatales 2.2 Servicios de las AA.PP. autonómicas 2.3 Servicios de las AA.PP. locales Puntos Clave</p> <p><b>SÍNTESIS TERCERA SESIÓN.....153</b></p> <p><b>AUTOEVALUACIÓN.....154</b></p>
<b>SÍNTESIS PRIMERA SESIÓN.....78</b>	<b>SÍNTESIS SEGUNDA SESIÓN.....103</b>	
<b>AUTOEVALUACIÓN.....79</b>	<b>AUTOEVALUACIÓN.....104</b>	
		<b>ANEXOS..... .157</b>

# Primera Sesión

## Regulación de las TIC

**Al finalizar esta sesión habrá adquirido los siguientes conocimientos...**

- ❑ Profundo análisis del marco jurídico de las TIC (Tecnologías de la Información y la Comunicación) en materia de: firma electrónica, servicios de la sociedad de la información, protección de datos personales, propiedad intelectual y telecomunicaciones.
- ❑ Una introducción a la interoperabilidad entre órganos y Administraciones tanto a nivel europeo como a nivel español.
- ❑ La eficacia y la necesidad de la firma electrónica en las relaciones jurídico-públicas, así como los problema procesales que pueden darse en el uso de la firma electrónica.

## 1

## RÉGIMEN JURÍDICO DE LAS TIC

## 1.1

## Firma electrónica

## MARCO JURÍDICO

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica (publicación DOCE L 13 19/01/2000)
- Ley 59/2003, de 19 de diciembre, de firma electrónica (publicación BOE 20/12/2003)

A continuación se presenta el contenido básico, más relevante para el usuario de la firma electrónica, de la Ley 59/2003.

El Título I lleva por rúbrica *Disposiciones generales* y en él destacan dos preceptos: en el art. 3 se establece el concepto de firma electrónica y de documento electrónico y en el art. 5 se regula el régimen de prestación de los servicios de certificación.

**Artículo 3. Firma electrónica, y documentos firmados electrónicamente.**

1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

2. La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

5. Se considera documento electrónico el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente.

6. El documento electrónico será soporte de:

a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

c) Documentos privados.

7. Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

8. El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida, con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que por el prestador de servicios de certificación, que expide los certificados electrónicos, se cumplen todos los requisitos establecidos en la ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica, y en especial, las obligaciones de garantizar la confidencialidad del proceso así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes. Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.

9. No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.

10. A los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.

Existen, por tanto, **tres tipos de firma electrónica**:

- **Firma electrónica simple.** Es aquella que responde al concepto establecido en el apartado 1, pero que no cumple las condiciones de los apartados 2 y 3.
- **Firma electrónica avanzada.** Es la que cumple lo establecido en los apartados 1 y 2, pero que no cumple con los requisitos del apartado 3.
- **Firma electrónica reconocida.** Es aquella que cumple los requisitos de los apartados 1, 2, y 3. Para que nos encontremos ante ella es necesario que concurren las dos siguientes circunstancias:
  - Ha de estar basada en un certificado reconocido. Son reconocidos los certificados emitidos por un prestador de servicios de certificación acreditado ante el Ministerio de Industria, Comercio y Turismo. La Autoridad de Certificación de la Abogacía (ACA) se encuentra acreditada, como se puede apreciar en la siguiente página del Ministerio: <https://www11.mityc.es/prestadores/datosPrestador.jsp>.

The screenshot shows a web browser window displaying the 'PRESTADORES DE SERVICIOS DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA' page for 'AC ABOGACÍA'. The page includes a header with the Spanish coat of arms and the text 'MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO'. Below the header, there are buttons for 'IMPRIMIR' and 'SALIR'. The main content is organized into sections: 'Identificación', 'Información comercial', and 'Servicios'. The 'Identificación' section lists: 'Nombre o Razón Social: Consejo General de la Abogacía Española', 'CIF: Q28630061', 'Teléfono: 915232593', 'Domicilio Social: Paseo de Recoletos, 13, Madrid (Madrid) - 28004', and 'Orden de creación: Real Decreto 658/2001, por el que se aprueba el Estatuto General de la Abogacía'. The 'Información comercial' section lists: 'Nombre Comercial: AC ABOGACÍA', 'Dominio: [www.acabogacia.org](http://www.acabogacia.org)', 'Teléfono: 915240550', 'e-mail: [info@acabogacia.org](mailto:info@acabogacia.org)', and 'Domicilio: Paseo de Recoletos, 13, Madrid (Madrid) - 28004'. The 'Servicios' section has a checked box for 'Servicios de certificación basados en certificados reconocidos' and a table with the following entries: 'Certificados Corporativos Reconocidos de Colegiados', 'Certificados Corporativos Reconocidos de Personal Administrativo de los Colegios de Abogados.', and 'Certificados Corporativos Reconocidos de Persona Jurídica.'. At the bottom, it states: 'Fecha de alta en el servicio de publicación previsto en el artículo 30.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica: 25/11/2004'. The browser's status bar at the bottom shows 'Internet | Modo protegido: activado' and '100%' zoom.

- El segundo requisito consiste en la utilización de un dispositivo seguro de creación de firma. Los chips criptográficos empleados en las tarjetas de ACA son dispositivos seguros de creación de firma.

Por tanto, **la firma electrónica de ACA es firma electrónica reconocida**, es decir, se trata del tipo más seguro de firma electrónica que contempla nuestro ordenamiento.

Como se establece en el apartado cuarto, la firma electrónica reconocida produce los mismos efectos que la firma manuscrita.

Al ser la firma electrónica de ACA firma electrónica reconocida, **aquellos actos de firma que realicemos con nuestro certificado digital de ACA surtirán los mismos efectos que producirían en caso de que hubiéramos empleado la firma manuscrita.**

Además, en el apartado 8 se establece que «el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio».

El Título II se dedica a los certificados electrónicos (digitales).

#### **Artículo 6. Concepto de certificado electrónico y de firmante.**

*1. Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.*

*2. El firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.*

El art. 6 establece el concepto de certificado electrónico y de firmante, de modo que el certificado digital sirve para identificar al firmante pues vincula a éste los datos de verificación de firma.

#### **Artículo 8. Extinción de la vigencia de los certificados electrónicos.**

*1. Son causas de extinción de la vigencia de un certificado electrónico:*

- a) Expiración del período de validez que figura en el certificado.*
- b) Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.*
- c) Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.*

d) Resolución judicial o administrativa que lo ordene.

e) Fallecimiento o extinción de la personalidad jurídica del firmante, fallecimiento, o extinción de la personalidad jurídica del representado, incapacidad sobrevenida, total o parcial, del firmante o de su representado, terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.

f) Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.

g) Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.

h) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

2. El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este período no podrá ser superior a cuatro años.

3. La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su período de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

El art. 8 regula las causas por las cuales un certificado digital pierde validez.

Un **certificado digital** puede encontrarse en una de las situaciones:

- **Válido.** El certificado es válido y produce efectos plenos.
- **Caducado.** El periodo de validez del certificado ha expirado.
- **Revocado.** El certificado ha perdido validez definitivamente y por una causa distinta a la expiración de su plazo de validez (las que establece el art. 8).
- **Suspendido.** El certificado ha perdido temporalmente su validez y podrá recuperarla (volvería a ser válido) o perderla definitivamente (sería revocado).

Las causas de suspensión se contemplan en el art. 9:

**Artículo 9. Suspensión de la vigencia de los certificados electrónicos.**

1. Los prestadores de servicios de certificación suspenderán la vigencia de los certificados electrónicos expedidos si concurre alguna de las siguientes causas:

a) Solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

b) Resolución judicial o administrativa que lo ordene.

c) La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c) y g) del artículo 8. 1.

d) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

2. La suspensión de la vigencia de un certificado electrónico surtirá efectos desde que se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

El concepto de certificado reconocido se desarrolla en el art. 11.1:

**Artículo 11. Concepto y contenido de los certificados reconocidos.**

1. Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten. [...]

Recordemos que la Autoridad de Certificación de la Abogacía (ACA) es un prestador acreditado de servicios de certificación.

Los certificados reconocidos han de presentar un contenido mínimo, establecido en el art. 11.2.

**Artículo 11. Concepto y contenido de los certificados reconocidos. [...]**

2. Los certificados reconocidos incluirán, al menos, los siguientes datos
  - a) La indicación de que se expiden como tales.
  - b) El código identificativo único del certificado.
  - c) La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
  - d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
  - e) La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.
  - f) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
  - g) El comienzo y el fin del período de validez del certificado.
  - h) Los límites de uso del certificado, si se establecen.
  - i) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.
3. Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.
4. Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13.

Los **certificados emitidos por ACA** presentan este contenido mínimo, así como contenido adicional relevante para el ejercicio de la abogacía en un entorno digital:

- Condición de abogado
- Número de colegiado
- Colegio de residencia

Los arts. 15, 16 y la Disposición adicional sexta se ocupan del DNI electrónico:

#### **Artículo 15. Documento nacional de identidad electrónico.**

*1. El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.*

*2. Todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.*

Por tanto, desde el punto de vista funcional **el DNI electrónico resulta equivalente al DNI tradicional** y, además, permite realizar actos de firma electrónica.

Los requisitos y características del DNI electrónico se establecen en el art. 16:

#### **Artículo 16. Requisitos y características del documento nacional de identidad electrónico.**

*1. Los órganos competentes del Ministerio del Interior para la expedición del documento nacional de identidad electrónico cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios de certificación que expidan certificados reconocidos con excepción de la relativa a la constitución de la garantía a la que se refiere el apartado 2 del artículo 20.*

*2. La Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional*

*de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados.*

El régimen de prestación de los servicios de certificación se regula en el Título III.

El art. 17 establece obligaciones en materia de protección de datos de carácter personal.

Por otra parte, el art. 18 establece obligaciones para los prestadores que emitan cualquier tipo de certificados:

**Artículo 18. Obligaciones de los prestadores de servicios de certificación que expidan certificados electrónicos.**

*Los prestadores de servicios de certificación que expidan certificados electrónicos deberán cumplir las siguientes obligaciones:*

*a) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.*

*b) Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica*

*1º Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica que sean compatibles con los datos de firma y con el certificado expedido.*

*2º Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.*

*3º El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado.*

*4º Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.*

*5º Las certificaciones que haya obtenido, en su caso, el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad.*

6º Las demás informaciones contenidas en la declaración de prácticas de certificación.

7º La información citada anteriormente que sea relevante para terceros afectados por los certificados deberá estar disponible a instancia de éstos.

c) Mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados.

d) Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro.

ACA cumple con todas estas obligaciones. A modo de ejemplo, el directorio de certificados de ACA se encuentra accesible desde la página principal de ACA: <http://www.acabogacia.org>.

**Para acceder a la información de un certificado tendremos que introducir la dirección de correo electrónico asociada al mismo.** Este sistema de acceso se ha establecido para evitar accesos masivos al directorio.



El art. 19 impone al prestador de servicios de certificación la obligación de contar con una Declaración de Prácticas de Certificación que ha de estar disponible pública y gratuitamente:

**Artículo 19. Declaración de prácticas de certificación.**

1. Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación en la que detallarán, en el marco de esta ley y de sus disposiciones de desarrollo, las obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

2. La declaración de prácticas de certificación de cada prestador estará disponible al público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita.

3. La declaración de prácticas de certificación tendrá la consideración de documento de seguridad a los efectos previstos en la legislación en materia de protección de datos de carácter personal y deberá contener todos los requisitos exigidos para dicho documento en la mencionada legislación.

La Declaración de Prácticas de Certificación de ACA se encuentra disponible en la siguiente dirección: <https://documentacion.redabogacia.org/docushare/dsweb/View/Collection-1316>.

El art. 20 establece las obligaciones de los prestadores que emiten certificados reconocidos:

**Artículo 20. Obligaciones de los prestadores de servicios de certificación que expidan certificados reconocidos.**

1. Además de las obligaciones establecidas en este capítulo, los prestadores de servicios de certificación que expidan certificados reconocidos deberán cumplir las siguientes obligaciones

a) Demostrar la fiabilidad necesaria para prestar servicios de certificación.

b) *Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.*

c) *Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.*

d) *Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.*

e) *Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante.*

f) *Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.*

g) *Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.*

2. *Los prestadores de servicios de certificación que expidan certificados reconocidos deberán constituir un seguro de responsabilidad civil por importe de al menos 3.000.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan.*

*La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea al menos de 3.000.000 de euros.*

*Las cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores podrán ser modificados mediante real decreto.*

La Autoridad de Certificación de la Abogacía cumple todos estos requisitos. No podía ser de otro modo puesto que ACA emite certificados reconocidos.

El Título IV se dedica a los dispositivos de firma electrónica y sistemas de certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica.

Recordemos que uno de los dos elementos característicos de la firma electrónica reconocida es el empleo de un dispositivo seguro de creación de firma.

El art. 24 establece el concepto y requisitos de un dispositivo seguro de creación de firma:

**Artículo 24. Dispositivos de creación de firma electrónica.**

1. Los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

2. Un dispositivo de creación de firma es un programa o sistema informático que sirve para aplicar los datos de creación de firma.

3. Un dispositivo seguro de creación de firma es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:

a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.

b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.

c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

**Las tarjetas ACA incorporan un chip criptográfico** que es un dispositivo seguro de creación de firma.

Las cuestiones relativas a supervisión y control se regulan en el en el Título V. Por otra parte, el Título VI se dedica a las infracciones y sanciones.

Por último, la Disposición adicional primera establece que el régimen de la Fe pública no se ve afectado por la firma electrónica:

**Disposición adicional primera. Fe pública y uso de firma electrónica.**

1. Lo dispuesto en esta ley no sustituye ni modifica las normas que regulan las funciones que corresponden a los funcionarios que tengan legalmente la facultad de dar fe en documentos en lo que se refiere al ámbito de sus competencias siempre que actúen con los requisitos exigidos en la ley.

2. En el ámbito de la documentación electrónica, corresponderá a las entidades prestadoras de servicios de certificación acreditar la existencia de los servicios prestados en el ejercicio de su actividad de certificación electrónica, a solicitud del usuario, o de una autoridad judicial o administrativa.

## 1.2

## Servicios de la Sociedad de la Información

## MARCO JURÍDICO

- Directiva 2002/58/CE sobre la Privacidad y las Comunicaciones Electrónicas (publicación DOCE L 201 31/07/2002)
- Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (publicación DOCE L 178 17/07/2000)
- Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores (publicación DOCE L 166 11/06/1998)
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (publicación BOE 12/07/2002; corrección de errores BOE 06/08/2002). Ha sufrido dos modificaciones, en virtud de la Disposición Final Primera de la Ley 32/2003 y de la Disposición Adicional Octava de la Ley 59/2003.

A continuación presentamos aquel contenido de la Ley 34/2002 que resulta más relevante para el usuario de los servicios de la sociedad de la información.

El Título I comprende las disposiciones generales.

El ámbito de aplicación se determina en los arts. 2 y 3.

#### **Artículo 2. Prestadores de servicios establecidos en España.**

*1. Esta Ley será de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos.*

*Se entenderá que un prestador de servicios está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.*

*2. Asimismo, esta Ley será de aplicación a los servicios de la sociedad de la información que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.*

*Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que realice toda o parte de su actividad.*

*3. A los efectos previstos en este artículo, se presumirá que el prestador de servicios está establecido en España cuando el prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.*

*La utilización de medios tecnológicos situados en España, para la prestación o el acceso al servicio, no servirá como criterio para determinar, por sí solo, el establecimiento en España del prestador.*

*4. Los prestadores de servicios de la sociedad de la información establecidos en España estarán sujetos a las demás disposiciones del ordenamiento jurídico español que les sean de aplicación, en función de la actividad que desarrollen, con independencia de la utilización de medios electrónicos para su realización.*

**Artículo 3. Prestadores de servicios establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo.**

1. Sin perjuicio de lo dispuesto en los artículos 7.1 y 8, esta Ley se aplicará a los prestadores de servicios de la sociedad de la información establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo cuando el destinatario de los servicios radique en España y los servicios afecten a las materias siguientes:

- a) Derechos de propiedad intelectual o industrial.
- b) Emisión de publicidad por instituciones de inversión colectiva.
- c) Actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios.
- d) Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores.
- e) Régimen de elección por las partes contratantes de la legislación aplicable a su contrato.
- f) Licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente no solicitadas.

2. En todo caso, la constitución, transmisión, modificación y extinción de derechos reales sobre bienes inmuebles sitos en España se sujetará a los requisitos formales de validez y eficacia establecidos en el ordenamiento jurídico español.

3. Los prestadores de servicios a los que se refiere el apartado 1 quedarán igualmente sometidos a las normas del ordenamiento jurídico español que regulen las materias señaladas en dicho apartado.

4. No será aplicable lo dispuesto en los apartados anteriores a los supuestos en que, de conformidad con las normas reguladoras de las materias enumeradas en el apartado 1, no fuera de aplicación la ley del país en que resida o esté establecido el destinatario del servicio.

Por tanto, el ámbito de aplicación de la **LSSICE** (Ley de Servicios de la Sociedad de la Información y Comercio Electrónico) se circunscribe a:

- Actividades económicas
- Realizadas por medios electrónicos
- Cuando exista una vinculación geográfica a España

El Título II regula la prestación de servicios de la sociedad de la información. A este respecto se establece el principio de libre prestación de servicios, que se concreta en los arts. 6-8.

En primer lugar, el principio de libre prestación de servicios se concreta en la ausencia de necesidad de autorización previa (art. 6).

#### **Artículo 6. No sujeción a autorización previa.**

*La prestación de servicios de la sociedad de información no estará sujeta a autorización previa. Esta norma no afectará a los regímenes de autorización previstos en el ordenamiento jurídico que no tengan por objeto específico y exclusivo la prestación por vía electrónica de los correspondientes servicios.*

En segundo lugar, el principio de libre prestación contempla la reciprocidad y la armonización comunitaria:

#### **Artículo 7. Principio de libre prestación de servicios.**

*1. La prestación de servicios de la sociedad de la información que procedan de un prestador establecido en algún Estado miembro de la Unión Europea o del Espacio Económico Europeo se realizará en régimen de libre prestación de servicios, sin que pueda establecerse ningún tipo de restricciones a los mismos por razones derivadas del ámbito normativo coordinado, excepto en los supuestos previstos en los artículos 3 y 8.*

*2. La aplicación del principio de libre prestación de servicios de la sociedad de la información a prestadores establecidos en Estados no miembros del Espacio Económico Europeo se atenderá a los acuerdos internacionales que resulten de aplicación.*

El art. 8 establece restricciones a la prestación de servicios. Tales restricciones se han de realizar con las debidas garantías y procederán en caso de lesión de alguno de los siguientes principios:

**Artículo 8. Restricciones a la prestación de servicios). [...]**

- a) *La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional,*
- b) *La protección de la salud pública o de las personas físicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores,*
- c) *El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y*
- d) *La protección de la juventud y de la infancia. [...]*

Las obligaciones de los prestadores de servicios de la sociedad de la información se regulan en los arts. 9-12.

De cara al usuario, las obligaciones más relevantes son la constancia registral del nombre de dominio (art. 9) y el deber de información general (art. 10).

**Artículo 9. Constancia registral del nombre de dominio.**

1. *Los prestadores de servicios de la sociedad de la información establecidos en España deberán comunicar al Registro Mercantil en el que se encuentren inscritos, o a aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad, al menos, un nombre de dominio o dirección de Internet que, en su caso, utilicen para su identificación en Internet, así como todo acto de sustitución o cancelación de los mismos, salvo que dicha información conste ya en el correspondiente Registro.*

2. *Los nombres de dominio y su sustitución o cancelación se harán constar en cada registro, de conformidad con sus normas reguladoras.*

*Las anotaciones practicadas en los Registros Mercantiles se comunicarán inmediatamente al Registro Mercantil Central para su inclusión entre los datos que son objeto de publicidad informativa por dicho Registro.*

*3. La obligación de comunicación a que se refiere el apartado 1 deberá cumplirse en el plazo de un mes desde la obtención, sustitución o cancelación del correspondiente nombre de dominio o dirección de Internet.*

#### **Artículo 10. Información general.**

*1. Sin perjuicio de los requisitos que, en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información 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:*

*a) 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.*

*b) Los datos de su inscripción en el Registro a que se refiere el artículo 9.*

*c) En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.*

*d) Si ejerce una profesión regulada deberá indicar:*

*1º Los datos del colegio profesional al que, en su caso, pertenezca y número de colegiado.*

*2º El título académico oficial o profesional con el que cuente.*

*3º El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.*

*4º Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.*

*e) El número de identificación fiscal que le corresponda.*

f) 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.

g) Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

2. La obligación de facilitar esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en el apartado 1.

3. Cuando se haya atribuido un rango de numeración telefónica a servicios de tarificación adicional en el que se permita el acceso a servicios de la sociedad de la información y se requiera su utilización por parte del prestador de servicios, esta utilización y la descarga de programas informáticos que efectúen funciones de marcación, deberán realizarse con el consentimiento previo, informado y expreso del usuario.

A tal efecto, el prestador del servicio deberá proporcionar al menos la siguiente información

- a) Las características del servicio que se va a proporcionar.
- b) Las funciones que efectuarán los programas informáticos que se descarguen, incluyendo el número telefónico que se marcará.
- c) El procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en que se producirá dicho fin, y
- d) El procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional.

La información anterior deberá estar disponible de manera claramente visible e identificable.

Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la normativa de telecomunicaciones, en especial, en relación con los requisitos aplicables para el acceso por parte de los usuarios a los rangos de numeración telefónica, en su caso, atribuidos a los servicios de tarificación adicional.

Adicionalmente, el art. 11 establece el deber de colaboración de los prestadores de servicios de intermediación y el art. 12 impone el deber de retención de datos de tráfico relativos a las comunicaciones electrónicas.

El deber de retención de datos ha resultado muy polémico, ya que requiere notables recursos por parte de los prestadores e incide sobre la protección de datos de carácter personal.

El régimen de responsabilidad de los prestadores de servicios de la sociedad de la información (arts. 13-17).

El Título III regula el régimen jurídico de las comunicaciones comerciales por vía electrónica.

Según establece el art. 20, las comunicaciones comerciales han de ser claramente identificables como tales:

**Artículo 20. Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.**

*1. Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y deberán indicar la persona física o jurídica en nombre de la cual se realizan.*

*En el caso en el que tengan lugar a través de correo electrónico u otro medio de comunicación electrónica equivalente incluirán al comienzo del mensaje la palabra «publicidad».*

*2. En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar, además del cumplimiento de los requisitos establecidos en el apartado anterior y en las normas de ordenación del comercio, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación se exprese en de forma clara e inequívoca.*

El art 21 establece la obligación de contar con la autorización previa del destinatario de la comunicación comercial, cuando ésta se realice mediante correo electrónico o medios de comunicación equivalentes:

**Artículo 21. Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.**

*1. 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.*

*2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.*

*En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.*

Por su parte, el art. 22 otorga al destinatario de las comunicaciones comerciales el derecho de revocar el consentimiento en cualquier momento, por medio de una simple notificación. Además, establece el régimen jurídico de las cookies:

#### **Artículo 22. Derechos de los destinatarios de servicios.**

*1. 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.*

*A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado.*

*Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.*

*2. Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.*

*Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.*

El Título IV (arts. 23 a 29) regula la **contratación por vía electrónica**:

- Validez y eficacia de los contratos celebrados por vía electrónica (art. 23).
- Prueba de los contratos celebrados por vía electrónica (art. 24). Este artículo reconoce plena validez al documento electrónico:

**Artículo 24. Prueba de los contratos celebrados por vía electrónica.**

*1. La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él, se sujetará a las reglas generales del ordenamiento jurídico y, en su caso, a lo establecido en la legislación sobre firma electrónica.*

*2. En todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental.*

- Intervención de terceros de confianza (art. 25).
- Ley aplicable (art. 26).
- Obligaciones previas al inicio del procedimiento de contratación (art. 27):

**Artículo 27. Obligaciones previas al inicio del procedimiento de contratación.**

*1. Además del cumplimiento de los requisitos en materia de información que se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información que realice actividades de contratación electrónica tendrá la obligación de informar al destinatario de manera clara, comprensible e inequívoca y antes de iniciar el procedimiento de contratación, sobre los siguientes extremos:*

- a) Los distintos trámites que deben seguirse para celebrar el contrato.*
- b) Si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible.*
- c) Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos, y*

*d) La lengua o lenguas en que podrá formalizarse el contrato.*

*2. El prestador no tendrá la obligación de facilitar la información señalada en el apartado anterior cuando:*

*a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o*

*b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, cuando estos medios no sean empleados con el exclusivo propósito de eludir el cumplimiento de tal obligación.*

*3. Sin perjuicio de lo dispuesto en la legislación específica, las ofertas o propuestas de contratación realizadas por vía electrónica serán válidas durante el período que fije el oferente o, en su defecto, durante todo el tiempo que permanezcan accesibles a los destinatarios del servicio.*

*4. Con carácter previo al inicio del procedimiento de contratación, el prestador de servicios deberá poner a disposición del destinatario las condiciones generales a que, en su caso, deba sujetarse el contrato, de manera que éstas puedan ser almacenadas y reproducidas por el destinatario.*

- Información posterior a la celebración del contrato (art 28):

#### **Artículo 28. Información posterior a la celebración del contrato.**

*1. El oferente está obligado a confirmar la recepción de la aceptación al que la hizo por alguno de los siguientes medios:*

*a) El envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente, a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la aceptación, o*

*b) La confirmación, por un medio equivalente al utilizado en el procedimiento de contratación, de la aceptación recibida, tan pronto como el aceptante haya completado dicho procedimiento, siempre que la confirmación pueda ser archivada por su destinatario.*

*En los casos en que la obligación de confirmación corresponda a un destinatario de servicios, el prestador facilitará el cumplimiento de dicha obligación, poniendo a disposición del destinatario alguno de los medios indicados en este apartado. Esta obligación será exigible tanto si la confirmación debiera dirigirse al propio prestador o a otro destinatario.*

*2. Se entenderá que se ha recibido la aceptación y su confirmación cuando las partes a que se dirijan puedan tener constancia de ello.*

*En el caso de que la recepción de la aceptación se confirme mediante acuse de recibo, se presumirá que su destinatario puede tener la referida constancia desde que aquél haya sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico, o en el dispositivo utilizado para la recepción de comunicaciones.*

*3. No será necesario confirmar la recepción de la aceptación de una oferta cuando:*

*a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o*

*b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, cuando estos medios no sean empleados con el exclusivo propósito de eludir el cumplimiento de tal obligación.*

- Lugar de celebración del contrato (art 29).

Por otra parte, el Título V se dedica a la solución judicial y extrajudicial de conflictos.

En la primera categoría se incluye la acción de cesación regulada en los arts. 30 y 31, mientras que la solución extrajudicial de conflictos se contempla en el art. 32.

El Título VI, *Información y control*, establece las competencias en cuanto supervisión y control, información a usuarios y prestadores de servicios, obligación de comunicación de resoluciones y, por último, deber de colaboración de los prestadores.

El régimen sancionador se contempla en el Título VII, *Infracciones y sanciones*.

El sistema de asignación de nombres de dominio bajo el «.es» se regula en la Disposición adicional sexta.

De especial interés para el usuario de los servicios de la sociedad de la información son las definiciones contenidas en el Anexo:

#### **ANEXO – Definiciones**

*A los efectos de esta Ley, se entenderá por:*

*a) «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:*

*1º La contratación de bienes o servicios por vía electrónica.*

*2º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.*

*3º La gestión de compras en la red por grupos de personas.*

*4º El envío de comunicaciones comerciales.*

*5º El suministro de información por vía telemática.*

*6º El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual.*

*No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes*

*1º Los servicios prestados por medio de telefonía vocal, fax o telex.*

*2º El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.*

3º Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.a) de la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de octubre, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.

4º Los servicios de radiodifusión sonora, y

5º El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

b) «Servicio de intermediación»: servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información.

Son servicios de intermediación la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet.

c) «Prestador de servicios» o «prestador»: persona física o jurídica que proporciona un servicio de la sociedad de la información.

d) «Destinatario del servicio» o «destinatario»: persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información.

e) «Consumidor»: persona física o jurídica en los términos establecidos en el artículo 1 de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

f) «Comunicación comercial»: toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.

A efectos de esta Ley, no tendrán la consideración de comunicación comercial los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, los

servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica.

g) «Profesión regulada»: toda actividad profesional que requiera para su ejercicio la obtención de un título, en virtud de disposiciones legales o reglamentarias.

h) «Contrato celebrado por vía electrónica» o «contrato electrónico»: 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.

i) «Ámbito normativo coordinado»: todos los requisitos aplicables a los prestadores de servicios de la sociedad de la información, ya vengan exigidos por la presente Ley u otras normas que regulen el ejercicio de actividades económicas por vía electrónica, o por las leyes generales que les sean de aplicación, y que se refieran a los siguientes aspectos:

1º Comienzo de la actividad, como las titulaciones profesionales o cualificaciones requeridas, la publicidad registral, las autorizaciones administrativas o colegiales precisas, los regímenes de notificación a cualquier órgano u organismo público o privado, y

2º Posterior ejercicio de dicha actividad, como los requisitos referentes a la actuación del prestador de servicios, a la calidad, seguridad y contenido del servicio, o los que afectan a la publicidad y a la contratación por vía electrónica y a la responsabilidad del prestador de servicios.

No quedan incluidas en este ámbito las condiciones relativas a las mercancías y bienes tangibles, a su entrega ni a los servicios no prestados por medios electrónicos.

j) «Órgano competente»: todo órgano jurisdiccional o administrativo, ya sea de la Administración General del Estado, de las Administraciones Autonómicas, de las Entidades locales o de sus respectivos organismos o entes públicos dependientes, que actúe en el ejercicio de competencias legalmente atribuidas.

## 1.3

## Protección de datos personales

## MARCO JURÍDICO

- Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (publicación DOCE L 201 31/07/2002)
- Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (publicación DOCE L 281 23/11/1995)
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (publicación BOE 14/12/1999)
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal (publicación BOE 25/06/1999)

Se presenta a continuación el contenido más relevante de la LO 15/1999, desde el punto de vista del titular de los datos de carácter personal.

El Título I se dedica a disposiciones generales, resultando de interés las definiciones establecidas en el art. 3:

**Artículo 3. Definiciones.**

*A los efectos de la presente Ley Orgánica se entenderá por*

*a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.*

*b) Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.*

c) *Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.*

d) *Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.*

e) *Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.*

f) *Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.*

g) *Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.*

h) *Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.*

i) *Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado.*

j) *Fuentes accesibles al público: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.*

El concepto de dato de carácter personal resulta esencial a efectos de determinar si nos encontramos en el ámbito de la ley.

El ámbito de aplicación se establece en el art. 2:

**Artículo 2. Ámbito de aplicación.**

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

c) *Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del Régimen del personal de las Fuerzas Armadas.*

d) *Los derivados del Registro Civil y del Registro Central de penados y rebeldes.*

e) *Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.*

El Título II establece los principios de protección de datos.

En virtud del principio de calidad de los datos contenido en el art. 4, se establece un criterio de proporcionalidad entre la naturaleza de los datos recogidos, su exactitud, los usos a los que se van a destinar y el periodo de conservación de los mismos. También impide el tratamiento desleal de los datos personales al prohibir que se usen para una finalidad incompatible con aquella que motivó su recogida.

#### **Artículo 4. Calidad de los datos.**

1. *Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas del Parlamento Europeo y del Consejo para las que se hayan obtenido.*

2. *Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.*

3. *Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.*

4. *Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.*

5. *Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.*

*No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.*

*Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.*

*6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.*

*7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.*

El art. 5 impone un deber de información al afectado previa a la recogida de datos:

#### **Artículo 5. Derecho de información en la recogida de datos.**

*1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*

*a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*

*b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*

*c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*

*d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*

*e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.*

*Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.*

*2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.*

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior cuando expresamente una Ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

De acuerdo con el art. 6, es necesario contar con el consentimiento del afectado:

#### **Artículo 6. Consentimiento del afectado.**

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Los arts. 7 y 8 establecen la existencia de datos personales que merecen una protección especial.

#### **Artículo 7. Datos especialmente protegidos.**

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

#### **Artículo 8. Datos relativos a la salud.**

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad

El art. 9 se ocupa de la seguridad de los datos y se desarrolla en el RD 994/1999 (en breve se promulgará un nuevo reglamento).

#### **Artículo 9. Seguridad de los datos.**

1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

*3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.*

El art. 10 establece un deber de secreto respecto de los datos de carácter personal.

Los arts. 11 y 12 regulan los casos de transferencias de datos personales y subcontrataciones del tratamiento, respectivamente.

De especial interés para el afectado resulta el Título III, donde se regulan los derechos de las personas.

El art. 13 establece el derecho de impugnación de valoraciones basadas únicamente en un tratamiento de datos personales destinado a evaluar la personalidad o características del afectado.

El art. 14 otorga el derecho de consulta al Registro General de Protección de Datos.

Los arts. 15 al 17 consagran derechos que el interesado puede ejercitar frente al responsable del fichero. Se trata de los derechos de acceso, rectificación, cancelación y oposición.

#### **Artículo 15. Derecho de acceso.**

*1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.*

*2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.*

*3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.*

**Artículo 16. Derecho de rectificación y cancelación.**

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificadas o canceladas hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

**Artículo 17. Procedimiento de oposición, acceso, rectificación o cancelación.**

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.

2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

El art. 18 establece la tutela de los derechos señalados, en la vía administrativa y por la Agencia de Protección de Datos.

**Artículo 18. Tutela de los derechos.**

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del Organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

El último derecho que se otorga a los interesados es el derecho a indemnización, contemplado en el art. 19.

El Título IV contiene disposiciones sectoriales, contemplando tanto los ficheros de titularidad pública, como los ficheros de titularidad privada.

El Título V regula las transferencias internacionales de datos, estableciendo el criterio de autorización administrativa previa y contemplando numerosas excepciones a este criterio.

El régimen sancionador se establece en el Título VII.

## 1.4

## Propiedad intelectual

## MARCO JURÍDICO

- Directiva 91/250/CE del Consejo de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador
- Directiva 92/100/CE del Consejo de 19 de noviembre de 1992, sobre derechos de alquiler y préstamo y otros derechos afines a los derechos de autor en el ámbito de la propiedad intelectual
- Directiva 93/98/CE del Consejo de 29 de octubre de 1993, relativa a la armonización del plazo de protección del derecho de autor y de determinados derechos afines
- Directiva 96/9/CE del Parlamento Europeo y del Consejo de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos
- Directiva 29/2001/CE del Parlamento Europeo y del Consejo de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines en la sociedad de la información
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual (publicación BOE 22/05/1996)  
  
Fue modificado por la Ley 5/1998, de 6 de marzo.
- Ley 5/1998, de 6 de marzo, de incorporación al derecho español de la Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la Protección Jurídica de las Bases de Datos (publicación BOE 07/03/1998)

El RDL 1/1996 establece el régimen jurídico de los programas de ordenador en el Título VII de Libro I.

El art. 95 establece que los programas de ordenador se encuentran sujetos a un régimen especial, siendo de aplicación supletoria el régimen general.

El art. 96 define el concepto de programa de ordenador e indica qué elementos accesorios quedan igualmente cubiertos por la protección.

**Artículo 96. Objeto de la protección.**

1. A los efectos de la presente Ley se entenderá por programa de ordenador toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.

A los mismos efectos, la expresión programas de ordenador comprenderá también su documentación preparatoria. La documentación técnica y los manuales de uso de un programa gozarán de la misma protección que este Título dispensa a los programas de ordenador.

2. El programa de ordenador será protegido únicamente si fuese original, en el sentido de ser una creación intelectual propia de su autor.

3. La protección prevista en la presente Ley se aplicará a cualquier forma de expresión de un programa de ordenador. Asimismo, esta protección se extiende a cualesquiera versiones sucesivas del programa así como a los programas derivados, salvo aquellas creadas con el fin de ocasionar efectos nocivos a un sistema informático.

Cuando los programas de ordenador formen parte de una patente o un modelo de utilidad gozarán, sin perjuicio de lo dispuesto en la presente Ley, de la protección que pudiera corresponderles por aplicación del régimen jurídico de la propiedad industrial.

4. No estarán protegidos mediante los derechos de autor con arreglo a la presente Ley las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador incluidos los que sirven de fundamento a sus interfaces.

El art. 97 establece la titularidad de los derechos, contemplando los distintos supuestos de autoría por una o varias personas.

**Artículo 97. Titularidad de los derechos.**

1. Será considerado autor del programa de ordenador la persona o grupo de personas naturales que lo hayan creado, o la persona jurídica que sea contemplada como titular de los derechos de autor en los casos expresamente previstos por esta Ley.

2. Cuando se trate de una obra colectiva tendrá la consideración de autor, salvo pacto en contrario, la persona natural o jurídica que la edite y divulgue bajo su nombre.

3. Los derechos de autor sobre un programa de ordenador que sea resultado unitario de la colaboración entre varios autores serán propiedad común y corresponderán a todos éstos en la proporción que determinen.

4. Cuando un trabajador asalariado cree un programa de ordenador, en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación correspondientes al programa de ordenador así creado, tanto el programa fuente como el programa objeto, corresponderán, exclusivamente, al empresario, salvo pacto en contrario.

5. La protección se concederá a todas las personas naturales y jurídicas que cumplan los requisitos establecidos en esta Ley para la protección de los derechos de autor.

El art. 98 establece la duración de la protección, función de la naturaleza física o jurídica de la personalidad del autor.

#### **Artículo 98. Duración de la protección.**

1. Cuando el autor sea una persona natural la duración de los derechos de explotación de un programa de ordenador será, según los distintos supuestos que pueden plantearse, la prevista en el capítulo 1 del Título III de este Libro.

2. Cuando el autor sea una persona jurídica la duración de los derechos a que se refiere el párrafo anterior será de setenta años, computados desde el día 1 de enero del año siguiente al de la divulgación lícita del programa o al de su creación si no se hubiera divulgado.

El contenido de los derechos de explotación y sus límites se regulan en los arts. 99 y 100, respectivamente.

**Artículo 99. Contenido de los derechos de explotación.**

*Sin perjuicio de lo dispuesto en el artículo 100 de esta Ley los derechos exclusivos de la explotación de un programa de ordenador por parte de quien sea su titular con arreglo al artículo 97, incluirán el derecho de realizar o de autorizar:*

*a) La reproducción total o parcial, incluso para uso personal, de un programa de ordenador, por cualquier medio y bajo cualquier forma, ya fuere permanente o transitoria. Cuando la carga, presentación, ejecución, transmisión o almacenamiento de un programa necesiten tal reproducción deberá disponerse de autorización para ello, que otorgará el titular del derecho.*

*b) La traducción, adaptación, arreglo o cualquier otra transformación de un programa de ordenador y la reproducción de los resultados de tales actos, sin perjuicio de los derechos de la persona que transforme el programa de ordenador.*

*c) Cualquier forma de distribución pública incluido el alquiler del programa de ordenador original o de sus copias.*

*A tales efectos, cuando se produzca cesión del derecho de uso de un programa de ordenador, se entenderá, salvo prueba en contrario, que dicha cesión tiene carácter no exclusivo e intransferible, presumiéndose, asimismo, que lo es para satisfacer únicamente las necesidades del usuario. La primera venta en la Unión Europea de una copia de un programa por el titular de los derechos o con su consentimiento, agotará el derecho de distribución de dicha copia, salvo el derecho de controlar el subsiguiente alquiler del programa o de una copia del mismo.*

**Artículo 100. Límites a los derechos de explotación.**

*1. No necesitarán autorización del titular, salvo disposición contractual en contrario, la reproducción o transformación de un programa de ordenador incluida la corrección de errores, cuando dichos actos sean necesarios para la utilización del mismo por parte del usuario legítimo, con arreglo a su finalidad propuesta.*

*2. La realización de una copia de seguridad por parte de quien tiene derecho a utilizar el programa no podrá impedirse por contrata en cuanto resulte necesaria para dicha utilización.*

*3. El usuario legítimo de la copia de un programa estará facultado para observar, estudiar o verificar su funcionamiento, sin autorización previa del titular, con el fin de determinar las ideas y principios implícitos en cualquier elemento del programa, siempre que lo haga durante cualquiera de las*

operaciones de carga, visualización, ejecución, transmisión o almacenamiento del programa que tiene derecho a hacer.

4. El autor, salvo pacto en contrario, no podrá oponerse a que el cesionario titular de derechos de explotación realice o autorice la realización de versiones sucesivas de su programa ni de programas derivados del mismo.

5. No será necesaria la autorización del titular del derecho cuando la reproducción del código y la traducción de su forma en el sentido de los párrafos a) y b) del artículo 99 de la presente Ley, sea indispensable para obtener la información necesaria para la interoperabilidad de un programa creado de forma independiente con otros programas, siempre que se cumplan los siguientes requisitos:

a) Que tales actos sean realizados por el usuario legítimo o por cualquier otra persona facultada para utilizar una copia del programa, o, en su nombre, por parte de una persona debidamente autorizada.

b) Que la información necesaria para conseguir la interoperabilidad no haya sido puesta previamente y de manera fácil y rápida, a disposición de las personas a que se refiere el párrafo anterior.

c) Que dichos actos se limiten a aquellas partes del programa original que resulten necesarias para conseguir la interoperabilidad.

6. La excepción contemplada en el apartado 5 de este artículo será aplicable siempre que la información así obtenida:

a) Se utilice únicamente para conseguir la interoperabilidad del programa creado de forma independiente.

b) Sólo se comunique a terceros cuando sea necesario para la interoperabilidad del programa creado de forma independiente.

c) No se utilice para el desarrollo, producción o comercialización de un programa sustancialmente similar en su expresión, o para cualquier otro acto que infrinja los derechos de autor.

7. Las disposiciones contenidas en los apartados 5 y 6 del presente artículo no podrán interpretarse de manera que permitan que su aplicación perjudique de forma injustificada los legítimos intereses del titular de los derechos o sea contraria a una explotación normal del programa informático.

La protección registral se contempla en el art. 101.

Por otra parte, la infracción de los derechos y las medidas de protección se regulan en los arts. 102 y 103, respectivamente. Las medidas de protección son las propias del régimen general establecido en el RDL 1/1996.

El tema relativo a la propiedad intelectual que resulta más polémico hoy en día es el de las redes de pares o "Peer to peer" (P2P). Las redes P2P se han convertido en un fenómeno social y consisten en redes de intercambio de archivos entre usuarios, de modo que cada ordenador hace las funciones de cliente y de servidor. Es decir, cada ordenador que ejecuta la aplicación P2P ofrece a los demás una serie de archivos y, simultáneamente, puede descargar los archivos compartidos por los demás.

La polémica en relación con las redes P2P reside en si se produce o no una vulneración de los derechos de propiedad intelectual de los archivos intercambiados.

Otra cuestión de actualidad relativa a la protección jurídica del software la constituye su eventual patentabilidad. Sin ánimo de tratar el problema con la profundidad que merece, baste con señalar la situación actual:

- El 06/07/2005 el Parlamento Europeo decidió por amplia mayoría (648 votos a favor, 14 en contra y 18 abstenciones) rechazar la directiva sobre patentes de software. Por tanto, al día de hoy nuestro ordenamiento no ampara la patentabilidad de los programas de ordenador.
- La Oficina Europea de Patentes continúa con la práctica que venía manteniendo y que consiste en admitir patentes de software.

Como se puede apreciar, la situación actual produce inseguridad en relación con la patentabilidad del software.

## 1.5

## Telecomunicaciones

Dada la amplitud de la materia, nos circunscribiremos a las normas básicas sobre telecomunicaciones.

**MARCO JURÍDICO**

- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (publicación DOCE L 201 de 31 de julio de 2002)
- Directiva 2002/19/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (publicación DOCE L 108, de 24 de abril de 2002)
- Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (publicación DOCE L 108, de 24 de abril de 2002)
- Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de de comunicaciones electrónicas (publicación DOCE L 108, de 24 de abril de 2002)
- Directiva 2002/22/DE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones (publicación DOCE L 108, de 24 de abril de 2002)
- Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (modificada por la Ley 4/2004, de 29 de diciembre)

A continuación se presentan los aspectos más relevantes para el usuario de los servicios de telecomunicaciones de la Ley 32/2003.

El Capítulo I del Título III (*Obligaciones de servicio público y derechos y obligaciones de carácter público en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas*) regula las obligaciones de servicio público, entre las cuales se encuentra el servicio universal.

El Capítulo III del Título III lleva por rúbrica: *Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas.*

El art. 33 se refiere al secreto de las comunicaciones:

**Artículo 33. Secreto de las comunicaciones.**

*Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.*

*Asimismo, los operadores deberán adoptar a su costa las medidas que se establezcan reglamentariamente para la ejecución de las interceptaciones dispuestas conforme a lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.*

Por su parte, el art. 34 incide sobre la protección de datos de carácter personal.

El art. 35 contempla la interceptación de comunicaciones a nivel técnico:

**Artículo 35. Interceptación de las comunicaciones electrónicas por los servicios técnicos.**

*1. Con pleno respeto al derecho al secreto de las comunicaciones y a la exigencia, conforme a lo establecido en la Ley de Enjuiciamiento Criminal, de autorización judicial para la interceptación de contenidos, cuando para la realización de las tareas de control para la eficaz utilización del dominio público radioeléctrico sea necesaria la utilización de equipos, infraestructuras e instalaciones técnicas de interceptación de señales no dirigidas al público en general, será de aplicación lo siguiente:*

*a) La Administración de las telecomunicaciones deberá diseñar y establecer sus sistemas técnicos de interceptación de señales en forma tal que se reduzca al mínimo el riesgo de afectar a los contenidos de las comunicaciones.*

*b) Cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los soportes en los que éstos aparezcan no podrán ser ni almacenados ni divulgados y serán inmediatamente destruidos.*

2. Las mismas reglas se aplicarán para la vigilancia del adecuado empleo de las redes y la correcta prestación de los servicios de comunicaciones electrónicas.

3. Lo establecido en este artículo se entiende sin perjuicio de las facultades que a la Administración atribuye el artículo 43.2.

Para reforzar el derecho al secreto de las comunicaciones, el art. 36 se refiere a la adopción de medidas de cifrado.

#### **Artículo 36. Cifrado en las redes y servicios de comunicaciones electrónicas.**

1. Cualquier tipo de información que se transmita por redes de comunicaciones electrónicas podrá ser protegida mediante procedimientos de cifrado.

2. El cifrado es un instrumento de seguridad de la información.

Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, así como la obligación de facilitar sin coste alguno los aparatos de cifra a efectos de su control de acuerdo con la normativa vigente.

El art. 38 establece el elenco de derechos de los usuarios y de los consumidores finales de los servicios de telecomunicaciones.

#### **Artículo 38. Derechos de los consumidores y usuarios finales.**

1. Los operadores que exploten redes o que presten servicios de comunicaciones electrónicas y los consumidores que sean personas físicas y otros usuarios finales podrán someter las controversias que les enfrenten al conocimiento de las juntas arbitrales de consumo, de acuerdo con la legislación vigente sobre defensa de los consumidores y usuarios.

Para el supuesto de que no se sometan a las juntas arbitrales de consumo o que éstas no resulten competentes para la resolución del conflicto, el Ministerio de Ciencia y Tecnología establecerá reglamentariamente un procedimiento conforme al cual los usuarios finales podrán someterle dichas

controversias. En cualquier caso, los procedimientos que se adopten deberán ser rápidos y gratuitos y establecerán el plazo máximo en el que deberá notificarse la resolución expresa, transcurrido el cual se podrá entender desestimada la reclamación por silencio administrativo. La resolución que se dicte podrá impugnarse ante la jurisdicción contencioso administrativa.

2. Las normas básicas de utilización de los servicios de comunicaciones electrónicas disponibles al público en general que determinarán los derechos de los consumidores que sean personas físicas y otros usuarios finales se aprobarán por real decreto que, entre otros extremos, regulará:

- a) La responsabilidad por los daños que se les produzcan.
- b) Los derechos de información de los consumidores que sean personas físicas y usuarios finales, que deberá ser veraz, eficaz, suficiente, transparente y actualizada.
- c) Los plazos para la modificación de las ofertas.
- d) Los derechos de desconexión de determinados servicios, previa solicitud del usuario.
- e) El derecho a obtener una compensación por la interrupción del servicio.
- f) El derecho a celebrar contratos por parte de los consumidores que sean personas físicas y usuarios finales con los operadores que faciliten la conexión o el acceso a la red de telefonía pública, así como el contenido mínimo de dichos contratos.
- g) Los supuestos en que serán exigibles y el contenido mínimo de los contratos celebrados entre consumidores que sean personas físicas u otros usuarios finales y prestadores de servicios de comunicaciones electrónicas que no sean los que facilitan conexión o acceso a la red telefónica pública.
- h) El derecho a resolver anticipadamente y sin penalización el contrato, en los supuestos de propuestas de modificación de las condiciones contractuales por motivos válidos especificados en aquél y sin perjuicio de otras causas de resolución unilateral.
- i) Los supuestos de aprobación por parte del Ministerio de Ciencia y Tecnología de contratos tipo entre consumidores que sean personas físicas u otros tipos de usuarios finales y operadores que exploten redes o presten servicios de comunicaciones electrónicas con obligaciones de servicio público o con poder significativo en los mercados de referencia específicos correspondientes.
- j) El derecho a recibir información comparable, pertinente y actualizada sobre la calidad de los servicios de comunicaciones electrónicas disponibles al público.

*k) El derecho a elegir un medio de pago para el abono de los correspondientes servicios entre los comúnmente utilizados en el tráfico comercial.*

*En el citado reglamento podrá ampliarse la aplicación del régimen de protección de consumidores y usuarios finales a otras categorías de usuarios.*

*3. En particular, los abonados a los servicios de comunicaciones electrónicas tendrán los siguientes derechos*

*a) A que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnación de la factura del servicio o para que el operador pueda exigir su pago.*

*b) A que sus datos de tráfico sean utilizados con fines comerciales o para la prestación de servicios de valor añadido únicamente cuando hubieran prestado su consentimiento informado para ello.*

*c) A recibir facturas no desglosadas cuando así lo solicitasen.*

*d) A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado.*

*e) A detener el desvío automático de llamadas efectuado a su terminal por parte de un tercero.*

*f) A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea en las llamadas que genere o la presentación de la identificación de su línea al usuario que le realice una llamada.*

*g) A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada.*

*h) A no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de venta directa sin haber prestado su consentimiento previo e informado para ello.*

4. Los usuarios de los servicios de comunicaciones electrónicas que no tengan la condición de abonados tendrán asimismo los derechos reconocidos en los párrafos a), b), d) y en el primer inciso del párrafo f) del apartado anterior.

5. Los usuarios finales no podrán ejercer los derechos reconocidos en los párrafos d) y f) del apartado 3 cuando se trate de llamadas efectuadas a entidades que presten servicios de llamadas de urgencia que se determinen reglamentariamente, en especial a través del número 112.

Del mismo modo, y por un período de tiempo limitado, los usuarios finales no podrán ejercer el derecho reconocido en el párrafo f) del apartado 3 cuando el abonado a la línea de destino haya solicitado la identificación de las llamadas maliciosas o molestas realizadas a su línea.

Lo dispuesto en el párrafo a) del apartado 3 se entiende sin perjuicio de lo dispuesto en el artículo 12 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

6. La elaboración y comercialización de las guías de abonados a los servicios de comunicaciones electrónicas y la prestación de los servicios de información sobre ellos se realizará en régimen de libre competencia, garantizándose, en todo caso, a los abonados el derecho a la protección de sus datos personales, incluyendo el de no figurar en dichas guías. A tal efecto, las empresas que asignen números de teléfono a los abonados habrán de dar curso a todas las solicitudes razonables de suministro de información pertinente para la prestación de los servicios de información sobre números de abonados y guías accesibles al público, en un formato aprobado y en unas condiciones equitativas, objetivas, orientadas en función de los costes y no discriminatorias, estando sometido el suministro de la citada información y su posterior utilización a la normativa en materia de protección de datos vigente en cada momento.

7. El Ministerio de Ciencia y Tecnología podrá introducir cláusulas de modificación de los contratos celebrados entre los operadores y los consumidores que sean personas físicas y usuarios finales, para evitar el trato abusivo a éstos.

8. Lo establecido en este artículo se entiende sin perjuicio de la aplicación de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

El apartado 2 enuncia derechos, si bien el desarrollo de su contenido se traslada a otras normas.

Por otra parte, el apartado 5 establece limitaciones al ejercicio de algunos de los derechos considerados.

El Título VIII regula el régimen de inspección y sancionador.

Para una mejor comprensión de la ley, el Anexo II contiene un glosario de términos empleados en la norma:

#### **ANEXO II – Definiciones**

1. *Abonado: cualquier persona física o jurídica que haya celebrado un contrato con un proveedor de servicios de comunicaciones electrónicas disponibles para el público para la prestación de dichos servicios.*

2. *Acceso: la puesta a disposición de otro operador, en condiciones definidas y sobre una base exclusiva o no exclusiva, de recursos o servicios con fines de prestación de servicios de comunicaciones electrónicas. Este término abarca, entre otros aspectos, los siguientes: el acceso a elementos de redes y recursos asociados que pueden requerir la conexión de equipos por medios fijos y no fijos (en particular, esto incluye el acceso al bucle local y a recursos y servicios necesarios para facilitar servicios a través del bucle local), el acceso a infraestructuras físicas, como edificios, conductos y mástiles, el acceso a sistemas informáticos pertinentes, incluidos los sistemas de apoyo operativos, el acceso a la conversión del número de llamada o a sistemas con una funcionalidad equivalente, el acceso a redes fijas y móviles, en particular con fines de itinerancia, el acceso a sistemas de acceso condicional para servicios de televisión digital; el acceso a servicios de red privada virtual.*

3. *Bucle local o bucle de abonado de la red pública telefónica fija: el circuito físico que conecta el punto de terminación de la red en las dependencias del abonado a la red de distribución principal o instalación equivalente de la red pública de telefonía fija.*

4. *Consumidor: cualquier persona física o jurídica que utilice o solicite un servicio de comunicaciones electrónicas disponible para el público para fines no profesionales.*

5. *Derechos exclusivos: los derechos concedidos a una empresa por medio de un instrumento legal, reglamentario o administrativo que le reserve el derecho a prestar un servicio o a emprender una actividad determinada en una zona geográfica específica.*

6. *Derechos especiales: los derechos concedidos a un número limitado de empresas por medio de un instrumento legal, reglamentario o administrativo que, en una zona geográfica específica*

*a) Designen o limiten, con arreglo a criterios que no sean objetivos, proporcionales y no discriminatorios, a dos o más el número de tales empresas autorizadas a prestar un servicio o emprender una actividad determinada, o*

b) Confiera a una empresa o empresas, con arreglo a tales criterios, ventajas legales o reglamentarias que dificulten gravemente la capacidad de otra empresa de prestar el mismo servicio o emprender la misma actividad en la misma zona geográfica y en unas condiciones básicamente similares.

7. Dirección: cadena o combinación de cifras y símbolos que identifica los puntos de terminación específicos de una conexión y que se utiliza para encaminamiento.

8. Operador con poder significativo en el mercado: operador que, individual o conjuntamente con otros, disfruta de una posición equivalente a una posición dominante, esto es, una posición de fuerza económica que permite que su comportamiento sea, en medida apreciable, independiente de los competidores, los clientes y, en última instancia, los consumidores que sean personas físicas.

9. Equipo avanzado de televisión digital: decodificadores para la conexión a televisores o televisores digitales integrados capaces de recibir servicios de televisión digital interactiva.

10. Equipo terminal: equipo destinado a ser conectado a una red pública de comunicaciones electrónicas, esto es, a estar conectado directamente a los puntos de terminación de aquella o interfuncionar, a su través, con objeto de enviar, procesar o recibir información.

11. Especificación técnica: la especificación que figura en un documento que define las características necesarias de un producto, tales como los niveles de calidad o las propiedades de su uso, la seguridad, las dimensiones, los símbolos, las pruebas y los métodos de prueba, el empaquetado, el marcado y el etiquetado. Se incluyen dentro de la citada categoría las normas aplicables al producto en lo que se refiere a la terminología.

12. Espectro radioeléctrico: las ondas radioeléctricas en las frecuencias comprendidas entre 9 KHz y 3000 GHz las ondas radioeléctricas son ondas electromagnéticas propagadas por el espacio sin guía artificial.

13. Explotación de una red de comunicación electrónica: la creación, el aprovechamiento, el control o la puesta a disposición de dicha red.

14. Interconexión: la conexión física y lógica de las redes públicas de comunicaciones utilizadas por un mismo operador o por otro distinto, de manera que los usuarios de un operador puedan comunicarse con los usuarios del mismo operador o de otro distinto, o acceder a los servicios prestados por otro operador. Los servicios podrán ser prestados por las partes interesadas o por terceros que tengan acceso a la red. La interconexión constituye un tipo particular de acceso entre operadores de redes públicas.

15. *Interfaz de programa de aplicación (API): la interfaz de software entre las aplicaciones externas, puesta a disposición por los operadores de radiodifusión o prestadores de servicios, y los recursos del equipo avanzado de televisión digital para los servicios de radio y televisión digital.*

16. *Interferencia perjudicial: toda interferencia que suponga un riesgo para el funcionamiento de un servicio de radionavegación o de otros servicios de seguridad o que degrade u obstruya gravemente o interrumpa de forma repetida un servicio de radiocomunicación que funcione de conformidad con la reglamentación comunitaria o nacional aplicable.*

17. *Nombre: combinación de caracteres (números, letras o símbolos).*

18. *Número: cadena de cifras decimales.*

19. *Número geográfico: el número identificado en el plan nacional de numeración que contiene en parte de su estructura un significado geográfico utilizado para el encaminamiento de las llamadas hacia la ubicación física del punto de determinación de la red.*

20. *Números no geográficos: los números identificados en el plan nacional de numeración que no son números geográficos.*

*Incluirán, entre otros, los números de teléfonos móviles, los de llamada gratuita y los de tarificación adicional.*

21. *Operador: persona física o jurídica que explota redes públicas de comunicaciones electrónicas o presta servicios de comunicaciones electrónicas disponibles al público y ha notificado a la Comisión del Mercado de las Telecomunicaciones el inicio de su actividad.*

22. *Punto de terminación de la red: el punto físico en el que el abonado accede a una red pública de comunicaciones. Cuando se trate de redes en las que se produzcan operaciones de conmutación o encaminamiento, el punto de terminación de la red estará identificado mediante una dirección de red específica, la cual podrá estar vinculada al número o al nombre de un abonado. El punto de terminación de red es aquel en el que terminan las obligaciones de los operadores de redes y servicios y al que, en su caso, pueden conectarse los equipos terminales.*

23. *Radiocomunicación: toda telecomunicación transmitida por medio de ondas radioeléctricas.*

24. *Recursos asociados: aquellos sistemas, dispositivos u otros recursos asociados con una red de comunicaciones electrónicas o con un servicio de comunicaciones electrónicas que permitan o apoyen la prestación de servicios a través de dicha red o servicio; incluyen los sistemas de acceso condicional y las guías electrónicas de programas.*

25. *Red de comunicaciones electrónicas: los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes, incluida Internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada.*

26. *Red pública de comunicaciones: una red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público.*

27. *Red telefónica pública: una red de comunicación electrónica utilizada para la prestación de servicios telefónicos disponibles al público. Sirve de soporte a la transferencia, entre puntos de terminación de la red, de comunicaciones vocales, así como de otros tipos de comunicaciones, como el fax y la transmisión de datos.*

28. *Servicio de comunicaciones electrónicas: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o de las actividades que consistan en el ejercicio del control editorial sobre dichos contenidos, quedan excluidos, asimismo, los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas.*

29. *Servicio de televisión de formato ancho: el servicio de televisión constituido, total o parcialmente, por programas producidos y editados para su presentación en formato ancho completo. La relación de dimensiones 16: 9 constituye el formato de referencia para los servicios de televisión de este tipo.*

30. *Servicio telefónico disponible al público: el servicio disponible al público a través de uno o más números de un plan nacional o internacional de numeración telefónica, para efectuar y recibir llamadas nacionales e internacionales y tener acceso a los servicios de emergencia, pudiendo incluir adicionalmente, cuando sea pertinente, la prestación de asistencia mediante operador, los servicios de información sobre números de abonados, guías, la oferta de teléfonos públicos de pago, la prestación de servicios en condiciones especiales, la oferta de facilidades especiales a los clientes con discapacidad o con necesidades sociales especiales y la prestación de servicios no geográficos.*

31. *Sistema de acceso condicional: toda medida técnica o mecanismo técnico que condicione el acceso en forma inteligible a un servicio protegido de radiodifusión sonora o televisiva al pago de una cuota u otra forma de autorización individual previa.*

32. *Telecomunicaciones: toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.*

33. *Teléfono público de pago: un teléfono accesible al público en general y para cuya utilización pueden emplearse como medios de pago monedas, tarjetas de crédito/débito o tarjetas de prepago, incluidas las tarjetas que utilizan códigos de marcación.*

34. *Usuario: una persona física o jurídica que utiliza o solicita un servicio de comunicaciones electrónicas disponible para el público.*

35. *Usuario final: el usuario que no explota redes públicas de comunicaciones ni presta servicios de comunicaciones electrónicas disponibles para el público ni tampoco los revende.*

36. *Autoridad Nacional de Reglamentación: el Gobierno, los departamentos ministeriales, órganos superiores y directivos y organismos públicos, que de conformidad con esta ley ejercen las competencias que en la misma se prevén.*

## Ejercicios Prácticos

**EJERCICIO 1: Verificación cumplimiento de requisitos en RedAbogacía**

1. Comprobar en la página web [www.redabogacia.org](http://www.redabogacia.org) el cumplimiento de la LSSICE: Restricciones a la prestación de servicios (art. 8).
2. Comprobar en la página web [www.redabogacia.org](http://www.redabogacia.org) el cumplimiento de la LSSICE: Constancia registral del nombre de dominio (art. 9).
3. Comprobar en la página web [www.redabogacia.org](http://www.redabogacia.org) el cumplimiento de la LSSICE: Información general (art. 10).
4. Comprobar en la página web [www.redabogacia.org](http://www.redabogacia.org) el cumplimiento del deber de información en la recogida de datos (art. 5 LOPD).

## 2

## LA FIRMA ELECTRÓNICA EN LAS RELACIONES JURÍDICO-PÚBLICAS

## 2.1

## Introducción

El certificado digital surge gracias al desarrollo de las nuevas tecnologías y para aprovechar las ventajas que ofrece en tiempo y costes. En este contexto, nace la firma electrónica con el objetivo de aportar seguridad y confianza máximas en las transacciones entre particulares, empresas y Administraciones Públicas.

El certificado digital es un documento en formato electrónico a través del cual un organismo autorizado, llamado **Autoridad de Certificación (CA)**, garantiza la identidad de una persona física o jurídica. El certificado digital se emite con la aprobación de la Autoridad de Certificación que delega en una **Autoridad de Registro (RA)**, que lo entrega al **Suscriptor**, la persona física o jurídica titular del certificado.

El certificado digital va firmado por la Autoridad de Certificación y contiene una clave pública y unos datos que sirven para verificar la identidad del suscriptor.

Nadie duda hoy en día del grado de interrelación que existe entre el crecimiento económico sostenible y el nivel de desarrollo de la sociedad de la información de una economía. El desarrollo de la sociedad de la información implica innovación tecnológica, eficiencia en los procesos productivos y eficacia en el empleo de recursos de todo orden, especialmente en lo que a los recursos humanos se refiere.

**El desarrollo de la sociedad de la información en España es moderado** en comparación con su potencial. Estudios revelan que en nuestro país todavía hay mucho recelo a la hora de confiar en la seguridad y confidencialidad de las redes electrónicas. Son varios los factores que pueden explicar este hecho:

- Factores sociológicos
- Factores económicos
- Factores tecnológicos

Por esta razón es tan imprescindible el desarrollo de un instrumento centrado exclusivamente en dotar de seguridad a las comunicaciones electrónicas como es la firma electrónica/digital.

## 2.2

## Eficacia y necesidad de la firma electrónica en las relaciones jurídico-públicas

Para completar las explicaciones expuestas en el capítulo anterior sobre la Ley de la firma electrónica, haremos alusión a los tipos de certificados emitidos por ACA.

Existen dos tipos de certificados, de usuario final y de uso interno. Dentro de los certificados de usuario final, se dispone de certificado de colegio, certificado de empleado y certificado de persona jurídica. Estos últimos, identifican a una persona jurídica, ya sean colegios de abogados, Consejos Autonómicos o despachos colectivos de abogados y en general a una persona jurídica relacionada de alguna forma con los Colegios de Abogados de España, los Consejos Autonómicos o el Consejo General de la Abogacía Española. La persona jurídica estará representada por una persona física, denominada representante, cuyos datos serán incluidos dentro del certificado y será el responsable de la custodia del mismo.

La Ley 59/2003 resulta expresamente aplicable al empleo de la firma electrónica en el ámbito jurídico-público, si bien permite a las Administraciones Públicas establecer condiciones adicionales para el empleo de la firma electrónica en el procedimiento administrativo, con la finalidad de salvaguardar las garantías de cada procedimiento.

En las relaciones entre los particulares, la certificación del momento en que se emiten o reciben los documentos electrónicos no puede encomendarse más que a un tercero dado que ninguna de las partes del negocio es capaz de asumir una posición imparcial acerca de tales datos. No ocurre lo mismo en las relaciones de derecho público en las que la Administración interviniente, dada la finalidad que debe perseguir, es capaz de conferir fehaciencia al dato de la fecha y hora en que la declaración se produce.

### Empleo de la firma electrónica por las personas jurídicas

**La directiva 1999/93/CE sobre firma electrónica sólo permitía a las personas físicas ser titulares de certificados electrónicos en el ámbito de la gestión de los tributos.** Pasados ya algunos años desde su entrada en vigor, se ha hecho necesario reflexionar acerca de la conveniencia de ir más allá en la atribución de la condición de firmante a la persona jurídica.

**La ley 59/2003**, establece en su artículo cuarto la necesidad de las Administraciones Públicas de crear servicios telemáticos basados en la firma electrónica bajo los principios elementales de objetividad, transparencia y no discriminación, impulsando de forma directa el uso de las comunicaciones telemáticas con sus administrados.

El uso de la firma electrónica como elemento de seguridad en las comunicaciones entre Administración y ciudadano abre un nuevo campo de actuaciones y servicios que favorecen la agilidad y cercanía entre ambos agentes.

En este sentido la Administración Pública española, consciente de la necesidad de adecuarse tecnológicamente, ha fijado como fecha límite el 1 de enero del 2020 para que los ciudadanos puedan realizar cualquier trámite administrativo online con todas las garantías que ofrece la firma electrónica.

Las necesidades del tráfico, en particular, del comercio electrónico, la extraordinaria expansión de nuevas fórmulas de contratación y, sobre todo, la incorporación de equipos y aplicaciones que permiten tratar automáticamente la información hasta el punto de suplir la voluntad humana en cada relación de negocio concreta, aconsejan replantearse la cuestión.

Cuando contrata un depósito a plazo con una entidad financiera, ordena una transferencia bancaria, hace la reserva de un billete de avión o de otro medio de transporte o «hace la compra» en un supermercado virtual, no está emitiendo una declaración de voluntad frente a otra persona física que actúa por representación de la contraparte. Debido a las necesidades actuales de esta sociedad de la información en la que vivimos, **la nueva Ley ha reconocido abiertamente la posibilidad de que las personas jurídicas sean titulares de este tipo de certificados**. Es importante destacar que la apuesta que ha hecho la Ley 59/2003 pasa por admitir de plano y con todas sus consecuencias dicha titularidad. **La Ley atribuye directamente la titularidad del certificado a la persona jurídica**, si bien se reconoce que los trámites necesarios para su obtención y uso deben hacerse con la intermediación de personas físicas.

Aún así, la Ley es prudente y recuerda que no pueden desaparecer las personas físicas cuando las personas jurídicas actúan en el tráfico económico que se realiza a través de técnicas electrónicas, informáticas y electrónicas. La persona jurídica es una creación artificial del derecho; no existe en el mundo tangible. Olvidar y hacer desaparecer a la persona física cuando actúa la persona jurídica puede echar por tierra la seguridad jurídica.

### 2.3

### Problemas procesales de la firma electrónica

Las tecnologías de la información permiten que un gran número de actividades personales y profesionales se realicen en nuestra sociedad vía electrónica: videoconferencia, correo electrónico, transferencias bancarias, trámites con la Administración.

Ejercitar la defensa de los intereses confiados, implica conservar las pruebas necesarias para su presentación durante el proceso judicial, un derecho irrenunciable de las partes en el ejercicio de la tutela judicial efectiva.

**La prueba electrónica** está constituida por cualquier información obtenida a través de un dispositivo electrónico o medio digital, que sirve para adquirir convencimiento de la certeza de un hecho en un juicio, es decir, un e-mail, una firma electrónica o una factura digital.

Las pruebas tradicionales están migrando desde el soporte papel hacia un entorno virtual, donde los procesos de gestión y criterios de admisibilidad cambian por completo.

Además, la prueba electrónica está adquiriendo una mayor importancia en los procesos judiciales, exigiendo a todos los actores del ámbito jurídico incluir estas pruebas en sus estrategias legales. Esta nueva realidad está cambiando radicalmente el lugar y las estrategias que abogados e investigadores deben seguir para la obtención y presentación de este nuevo tipo de pruebas.

Aunque el soporte de la prueba ha evolucionado paralelamente a las relaciones interpersonales, resulta paradójico que, de acuerdo a lo dispuesto en la Ley de Enjuiciamiento Civil, su valor probatorio se haga depender del soporte y desfavorezca a la prueba presentada en soporte electrónico frente a la presentada en cualquiera de los soportes tradicionales.

A la hora de definir los **documentos a presentar durante un proceso probatorio**, la LEC hace una **clasificación del documento electrónico como un documento aparte del documento público o privado**, distinguiendo:

- Documento público: (regulado por el art. 317 y ss.) que constituye prueba plena y es considerado siempre válido.
- Documento privado: (regulado por el art. 324 y ss.) que constituye prueba plena y se considerará válido únicamente cuando las partes no lo impugnaren.
- Documento electrónico: la LEC subdivide el documento electrónico en dos categorías:
  - los documentos firmados electrónicamente que se encuentran al amparo de lo establecido en el art 3 de la Ley de firma electrónica (art. 326.3 de la LEC).
  - cualquier otro documento electrónico (sms, correo electrónico, documento word, video, grabación) estará sometido a la sana crítica del juez (art 382 de la LEC).

Si analizamos las posibilidades del medio electrónico frente al tradicional a la hora de acreditar la validez de la prueba, cabe objetivar su mayor fiabilidad. Son valorables, entre otros, la dificultad técnica

que la falsificación de lo electrónico requiere, la trazabilidad que permite, la capacidad de acreditar la autoría de la información o la autoría de los diferentes agentes intervinientes en su manipulación o transmisión. Otras ventajas del medio técnico son la precisión sobre día, hora y hasta segundo exacto en que se ha producido la prueba y la rapidez en su captación y flexibilidad, como determinadas empresas de análisis forense son hoy capaces de acreditar.

Sin embargo, la **falta de legislación de la prueba electrónica en su dimensión global**, provoca una serie de limitaciones que influyen en la legítima defensa. Debe replantearse el problema para ajustarse a las demandas de una sociedad cada vez más tecnológica y preguntarse si dejar el valor probatorio de lo electrónico al arbitrio de jueces no siempre dotados de los conocimientos tecnológicos necesarios, podría suponer una discriminación clara de la prueba electrónica frente a la tradicional.

La abogacía, consciente de la acuciante necesidad de un tercero de confianza garantiza la condición de abogado en Internet a través de la **Autoridad de Certificación de la Abogacía (ACA)**, que goza de la confianza de las partes comunicadas. En esta línea se han desarrollado servicios que **custodian las comunicaciones de sus abogados dando fe en el tiempo**, de las garantías que se exigen para demostrar la validez de la prueba electrónica.

## Puntos Clave



La interrelación que existe entre el crecimiento económico sostenible y el nivel de desarrollo de la sociedad de la información son determinantes en una economía.



Los documentos a presentar durante un proceso probatorio pueden clasificarse según la LEC en:

- Documento público
- Documento privado
- Documento electrónico
  - Documento firmado electrónicamente (con certificado digital).
  - Documento electrónico (sms, correo electrónico, documento word, video, grabación).



La falta de legislación de la prueba electrónica en su dimensión global puede provocar una serie de limitaciones que influyen en la legítima defensa de sus clientes.

## 3

## INTEROPERABILIDAD

## 3.1

## Introducción

La administración electrónica (o e-Government) es un signo del esfuerzo de renovación económica, social y medioambiental tanto de la UE como de los gobiernos que comienzan a ponerlo en práctica. Su contribución a la mejora de la concepción y aplicación de políticas públicas es ya indiscutible y recientemente se ha estudiado con especial atención su **contribución a la competitividad y la innovación de las economías europeas**.

La administración electrónica ha permitido a la Administración avanzar en todos los niveles:

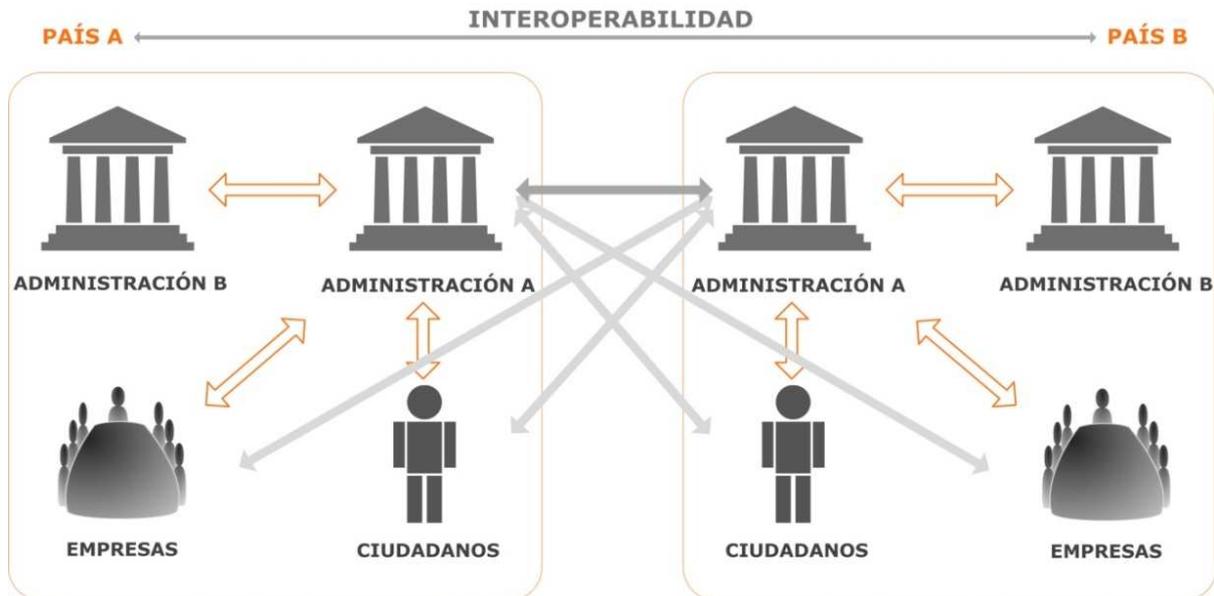
- Eliminar colas.
- Acercar las Administraciones públicas al ciudadano.
- Agilizar procedimientos administrativos.

Es necesario dedicar atención al desarrollo de su dimensión transfronteriza, en la que debe tener aún **más prioridad la interoperabilidad**. Una colaboración más estrecha entre administraciones de diferentes Estados miembros favorecerá la puesta a disposición de los ciudadanos y de las empresas europeas de mejores servicios y una aplicación más eficaz de las políticas de la UE.

Aumentar la colaboración exige mejorar la comunicación entre cada vez más administraciones del sector público, un reto que requiere el esfuerzo conjunto de los Estados miembros.

La interoperabilidad es el resultado de este esfuerzo por colaborar entre administraciones. Consiste en la utilización de las nuevas tecnologías en los procesos de las Administraciones Públicas, tanto en los procesos internos (toma de decisiones, relaciones internas, etc.) como en los procesos externos (relaciones con los ciudadanos, otras administraciones, etc.).

El denominado **e-Government o e-Administración** consiste en la utilización de las nuevas tecnologías en los procesos de las Administraciones Públicas, tanto en los procesos internos (toma de decisiones, relaciones internas, etc.) como en los procesos externos (relaciones con los ciudadanos, otras administraciones, etc.).



**La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos**, reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

La presente Ley, será de aplicación:

- a. A las Administraciones Públicas, entendiéndose por tales la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.
- b. A los ciudadanos en sus relaciones con las Administraciones Públicas.
- c. A las relaciones entre las distintas Administraciones Públicas.

Son fines de la presente Ley:

1. Facilitar el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos.
2. 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.
3. Crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.
4. Promover la proximidad con el ciudadano y la transparencia administrativa, así como la mejora continuada en la consecución del interés general.
5. Contribuir a la mejora del funcionamiento interno de las Administraciones Públicas, incrementando la eficacia y la eficiencia de las mismas mediante el uso de las tecnologías de la información, con las debidas garantías legales en la realización de sus funciones.
6. Simplificar los procedimientos administrativos y proporcionar oportunidades de participación y mayor transparencia, con las debidas garantías legales.
7. Contribuir al desarrollo de la sociedad de la información en el ámbito de las Administraciones Públicas y en la sociedad en general.

## 3.2

## Marco de Interoperabilidad de las AA.PP. europeas y españolas

**Contexto Europeo**

Para mejorar la competitividad de las economías europeas es necesario modernizar el sector público europeo y mejorar la interacción entre las organizaciones ya que:

- El mercado único depende de Administraciones Públicas modernas y eficaces que facilitan la movilidad entre ciudadanos y empresas.
- Las Administraciones Públicas modernas deben asentarse en sofisticadas infraestructuras de TIC y procedimientos eficaces de administración electrónica.

Para conseguir esto se pide a los estados miembros que establezcan una infraestructura sobre interoperabilidad que permita poner puntos de contacto únicos a disposición de las empresas móviles para completar los procedimientos administrativos relacionados con la movilidad. La cooperación y coordinación a nivel europeo es fundamental para desarrollar servicios paneuropeos.

Se ha elaborado un planteamiento básico sobre interoperabilidad europea, cuyas bases ya se han establecido:

- Una primera versión del documento *European Interoperability Framework for pan-European eGovernment Services* [Marco europeo de interoperabilidad (MEI) para servicios paneuropeos de administración electrónica] con directrices, políticas, normas y especificaciones para contribuir a que los socios trabajen juntos.
- Programas de investigación y desarrollo relacionados con la administración electrónica.
- Consultas de asesoramiento sobre iniciativas nacionales de administración electrónica.

**Contexto Español**

La interoperabilidad en nuestro país se ha orientado a la implantación de nuevos sistemas de notificaciones y presentación de escritos en órganos judiciales y comunicación entre abogados y procuradores con los Juzgados y Tribunales por medio de sistemas informáticos que comienzan a implantarse. Además la Unión Europea ha puesto el Proyecto STORK de identidad segura orientado a implementar el reconocimiento de la identidad electrónica, para permitir a empresas, ciudadanos y

empleados utilizar sus identidades nacionales en cualquier país miembro. El proyecto se apoya en el desarrollo de los sistemas nacionales de ID y fomenta el reconocimiento mutuo de las identidades electrónicas entre los estados miembros, está liderado por los países participantes y se centra en hacer posible la prestación transfronteriza de los servicios TIC, que ya están operativos a nivel nacional e incluso regional o local. España quiere crear dentro de este proyecto una plataforma de validación a nivel europeo.

Por todo ello, por parte del Ministerio de Justicia, y a través de la Dirección General para la modernización de la Administración de Justicia, se viene realizando un importante y sostenido esfuerzo para adecuar y actualizar el equipamiento tecnológico de los Juzgados y Tribunales. Así, una de las principales líneas de actuación supone el denominado Plan de Modernización Tecnológica de la Administración de Justicia y los Registros Civiles, que buscan:

- Facilitar la accesibilidad del ciudadano a una justicia rápida.
- Adecuar las soluciones tecnológicas a los procesos y a la organización judicial para la consecución de una óptima gestión administrativa y procesal.
- Dotar de mecanismos para la toma de decisiones, a todos los niveles de la Administración de Justicia.
- Definir y consensuar los medios, estándares y normativas necesarios para la consecución de la interoperabilidad y compartición de información a nivel nacional.

La interoperabilidad de los sistemas de información y comunicación electrónica de la Justicia se persigue mediante la instauración gradual de un sistema de tramitación de asuntos en la Administración de Justicia denominado MINERVA.

## Puntos Clave



La administración electrónica ha permitido a la Administración avanzar en el ámbito de la interoperabilidad de los servicios de información.



La interoperabilidad es el resultado de este esfuerzo por colaborar entre administraciones.



**Contexto europeo:** es necesario modernizar el sector público europeo y mejorar la interacción entre las organizaciones para:

- Crear una red de Administraciones Públicas modernas y eficaces que facilitan la movilidad entre ciudadanos y empresas.
- Lograr la eficacia de las Administraciones mediante procedimientos eficaces de administración electrónica.



**Contexto español:** el Ministerio de Justicia ha venido realizando un importante y sostenido esfuerzo para adecuar y actualizar el equipamiento tecnológico de los Juzgados y Tribunales mediante el denominado Plan de Modernización Tecnológica de la Administración de Justicia y los Registros Civiles.

## SÍNTESIS DE LA PRIMERA SESIÓN

Durante esta primera sesión se ha profundizado en el marco jurídico de las Tecnologías de la Información en nuestro país, exponiendo y explicando los artículos más interesantes de nuestra legislación en materia de nuevas tecnologías: firma electrónica, servicios de la sociedad de la información, protección de datos personales, propiedad intelectual y telecomunicaciones.

La eficacia de la firma electrónica ha quedado plenamente demostrada desde que en el 2003 se aprobó la Ley 59/2003. Aún así existen problemas procesales asociados a la firma electrónica, que invitan a seguir avanzando en el desarrollo del marco jurídico para garantizar la legítima defensa de los ciudadanos para evitar una posible discriminación entre la firma electrónica y la firma tradicional.

Un aspecto clave para evolucionar hacia políticas, normas y procedimientos que hagan más eficientes a nuestras administraciones, es la interoperabilidad entre organismos. Es necesaria una colaboración más estrecha entre administraciones de diferentes estados miembros para mejorar los servicios y las políticas sobre las que se asiente una adecuada infraestructura electrónica.

Es necesario modernizar el sector público europeo y nacional para mejorar la interacción entre las organizaciones y así crear una red de Administraciones Públicas modernas con procedimientos eficaces para todos.

## AUTOEVALUACIÓN 1

### 1. Los tipos de firma electrónica que existen son:

- a. Firma básica, firma reconocida y firma simple
- b. Firma reconocida, firma avanzada y firma simple
- c. Firma simple, firma compuesta y firma reconocida

### 2. La firma electrónica con certificado ACA es:

- a. Firma electrónica reconocida
- b. Firma electrónica avanzada
- c. Aún no se ha establecido de qué tipo es

### 3. El certificado digital emitido por ACA presenta como contenido mínimo:

- a. Condición de abogado, colegio de residencia y número de colegiado
- b. Condición de abogado, DNI del abogado y número de colegiado
- c. Colegio de residencia y número de abogado

### 4. ¿El DNI electrónico resulta igual que el DNI tradicional?

- a. Sí
- b. No
- c. Depende del uso que se requiera

### 5. Un certificado digital puede encontrarse en alguna de las siguientes situaciones:

- a. Válido, caducado o suspendido
- b. Válido o suspendido
- c. Válido, caducado, revocado o suspendido

**6. ¿Qué definición da la legislación de “Servicios de la sociedad de la información”?**

- a. Todo servicio automático que requiere de una certificación digital
- b. Todo servicio prestado telemáticamente
- c. Todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario

**7. Según el artículo 3 de la Ley de protección de datos personales, se define dato de carácter personal como:**

- a. Cualquier información concerniente a personas físicas identificadas o identificables
- b. Cualquier información concerniente a datos privados de organizaciones
- c. Cualquier dato de carácter general

**8. Según el marco jurídico de las telecomunicaciones ¿Cualquier tipo de información que se transmita por redes de comunicaciones electrónicas podrá ser protegida mediante procedimientos de cifrado?**

- a. Dependerá del tipo de información
- b. No
- c. Sí

**9. Según la Ley de Enjuiciamiento Civil ¿qué tipos de documentos pueden distinguirse?**

- a. Documento público o privado
- b. Documento público, privado o electrónico
- c. Documento público o electrónico

**10. El documento electrónico puede clasificarse en:**

- a. Documento firmado electrónicamente y documento electrónico (correo, sms, video, grabación...)
- b. Documento electrónico digital y documento electrónico interactivo
- c. El documento electrónico no tiene clasificación

**11. ¿Qué se entiende por e-Administración?**

- a. Concepto asociado a los servicios electrónicos
- b. Concepto asociado a las operaciones electrónicas de la administración con el ciudadano
- c. Concepto asociado a la administración electrónica

**12. La interoperabilidad en el sistema judicial se consigue mediante ...**

- a. Modernización tecnológica de los sistemas de información
- b. La instauración gradual de sistemas de tramitación automática como por ejemplo el denominado sistema Minerva y LexNet
- c. El uso generalizado de sistemas de información

**13. El e-Government utiliza las nuevas tecnologías en...**

- a. Procesos internos de la Administración
- b. Procesos externos con los ciudadanos
- c. Procesos internos y externos de la Administración

**14. ¿La nueva Ley ha reconocido abiertamente la posibilidad de que las personas jurídicas sean titulares de este tipo de certificados?**

- a. Sí
- b. No
- c. Lo ha reconocido para determinados casos

**15. La firma electrónica reconocida es:**

- a. La firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma
- b. La firma electrónica que permite identificar al firmante y detectar cualquier cambio anterior de los datos firmados. Está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control
- c. Es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante

***Soluciones: en los anexos***

# Segunda sesión

## Seguridad de la Información

**Al finalizar esta sesión habrá adquirido los siguientes conocimientos...**

- ❑ Los problemas de seguridad más frecuentes en entornos informáticos
- ❑ Las herramientas para solventar los problemas de seguridad anteriores
- ❑ La seguridad en el correo electrónico: cómo firmar y cifrar un correo
- ❑ Cómo firmar digitalmente un documento

## 1

## SEGURIDAD INFORMÁTICA

## 1.1

## Importancia de la Información

La Información es un recurso vital. Es parte importante en el trabajo diario de cualquier abogado pero es imprescindible que la información electrónica que maneja diariamente esté protegida en uso, divulgación, interrupción o destrucción no autorizada.

Como veíamos en el módulo básico, el término seguridad informática busca la **confidencialidad, autenticación, integridad** y **no repudio** de la información y de los datos.

**Confidencialidad**

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

**Autenticación**

La Autenticación es el acto de establecimiento o confirmación de algo (o alguien) como auténtico. La autenticación de un objeto puede significar la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad.

**Integridad**

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas. La violación de integridad se presenta cuando un empleado, programa o proceso, ya sea por accidente o con mala intención, modifica o borra los datos importantes que son parte de la información.

**No repudio**

Previene que un emisor niegue haber remitido un mensaje, cuando realmente lo ha emitido, y que un receptor niegue su recepción, cuando realmente lo ha recibido.

Existe otra vertiente de la seguridad, la disponibilidad, si bien en el caso de servicios electrónicos para la abogacía, esta vertiente recae sobre la plataforma de prestación de servicio: RedAbogacía.

RedAbogacía garantiza la disponibilidad de la información mediante el empleo de las técnicas y herramientas más avanzadas existentes en el mercado. Entre esas técnicas se encuentran la redundancia de aquellos elementos implicados en el almacenamiento y difusión de la información, así como un elaborado sistema de copias de seguridad.

## 1.2

## Problemas de Seguridad

La seguridad puede verse afectada por cualquiera de los siguientes componentes: el uso indebido de la tecnología, la falta de procesos de planificación de seguridad o el desconocimiento de las personas acerca de las distintas medidas de seguridad informática.

PROBLEMAS VINCULADOS A LA SEGURIDAD	
TECNOLOGÍA	Sabotaje informático Espionaje informático
PROCESOS	Copias de seguridad desfasadas Intrusión de programas maliciosos
PERSONAS	No aplicación de políticas de seguridad No activación de filtros antispam No activación y no actualización de antivirus

## USO INDEBIDO DE LA TECNOLOGÍA:

El uso indebido de la tecnología puede provocar serios problemas en la seguridad e integración de la información si un usuario accede de manera ilícita a los sistemas de archivos privados de otra persona sin previa autorización.

**SABOTAJE INFORMÁTICO:** el sabotaje informático comprende aquellas conductas tipificadas atendiendo a la acción delictiva, y que puede ser un sistema de tratamiento de la información o de sus partes componentes. El atentado a estos objetos mediante el acceso ilícito a los sistemas puede ser:

- Destrucción de la información o datos.
- Inutilización.
- Modificación.
- Obstaculización.

**ESPIONAJE INFORMÁTICO:** el espionaje informático comprende aquellas figuras delictivas que atienden al modo operativo que se ejecuta y que puede ser:

- Delitos de apoderamiento indebido (apropiarse de la información).
- Uso indebido de la información (usar la información para cualquier otro fin).
- Conocimiento indebido de la información mediante el acceso no autorizado a un sistema de la información ajeno. Estas figuras se encuentran conocidas como "hacking".
- Delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información (robos de información).
- Suplantación de la identidad.

#### **FALTA DE PROCESOS DE PLANIFICACIÓN DE LA SEGURIDAD:**

La planificación de la seguridad se refiere a todas aquellas acciones llevadas a cabo para realizar planes que mejoren la seguridad de la información. Los problemas que se derivan de no tener una mínima planificación son:

- Copias de seguridad desfasadas en contenidos de datos.
- Bases de datos de antivirus no actualizados.
- Intrusión de programas maliciosos.

La no actualización de los antivirus puede llevar a que programas externos realicen operaciones en nuestro ordenador que dañen nuestro sistema de archivos. Estos son denominados virus y realizan funciones no legítimas en los sistemas informáticos en los que se instalan. Algunos realizan operaciones perjudiciales para el usuario y lo hacen sin su conocimiento ni autorización. El ejemplo más claro de programas maliciosos son los virus informáticos. Como ya introdujimos en el módulo básico un virus es un programa que ocupando un mínimo espacio son capaces de ejecutarse automáticamente sin que el usuario de su consentimiento e infectar todo el sistema del usuario.

**PROGRAMAS MALICIOSOS:** Existen una gran variedad de virus en función de su forma de actuar:

1. El primer tipo de virus crea un archivo con el mismo nombre y en el mismo lugar donde se encuentra el archivo EXE que quiere infectar. Al ejecutar el virus, éste infecta al archivo original.
2. Este tipo de virus se añade al archivo a infectar y se activa cada vez que el archivo infectado es ejecutado.

A continuación expondremos algunos de los **tipos de virus más conocidos:**

- **Gusano o worm:** son programas que tratan de reproducirse a si mismo, no produciendo efectos destructivos sino el fin de dicho programa es el de colapsar el sistema o ancho de banda, replicándose a si mismo.
- **Caballo de Troya o Camaleones:** son programas que permanecen en el sistema pero no ocasionan acciones destructivas, sino que capturan datos, generalmente password, enviándolos a otro sitio, o dejan indefenso el ordenador donde se ejecuta, abriendo agujeros en la seguridad del sistema, con la siguiente profanación de nuestros datos.

La diferencia fundamental entre virus y troyano es que el virus se reproduce, sea modificando ficheros, mandándose por Internet, etc. y un troyano no, ya que trata de provocar trastornos a quien se lo envía.

- **Joke program:** es un virus que se presenta a modo de imagen o sucesivas imágenes que invitan a jugar al usuario mientras destruyen los datos del sistema informático.
- **Bombas lógicas o de tiempo:** se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas. Si no se produce la condición permanece oculto al usuario.
- **Retro Virus:** este programa busca cualquier antivirus, localiza un fallo dentro del antivirus y normalmente lo destruye. La propagación de estos programas maliciosos puede hacerse por varias vías:
  - Correo electrónico.
  - Instalación de software de origen no fiable.
  - Acceso a páginas web que ejecutan código malicioso.

**PERSONAL DESINFORMADO EN MATERIA DE SEGURIDAD**

Otro problema que puede ocasionar graves problemas de seguridad en los sistemas informáticos es la existencia de personal responsable de información que no tenga cultura en el uso de la seguridad informática. Esta desinformación conduce a no utilizar mecanismos de seguridad como (antivirus, firewalls, filtros o antispam...) que evitaría en muchos casos la entrada de dichos intrusos, o a no actualizar los mecanismos de protección del sistema.

Puntos Clave



## 2

## SOLVENTAR PROBLEMAS DE SEGURIDAD

## 2.1

## Clasificación de herramientas

Las herramientas destinadas a solventar los problemas expuestos en el capítulo anterior, pueden de igual forma agruparse en 3 grupos: solución a problemas de tecnología, problemas de procesos y problemas por falta de personal con conocimientos en materia de seguridad.

SOLUCIONES VINCULADAS A LA SEGURIDAD	
TECNOLOGÍA	Estándares, encriptación y protección Características de seguridad en los productos Productos y herramientas de seguridad
PROCESOS	Planificación de la seguridad Prevención Detección Reacción y recuperación
PERSONAS	Personal dedicado Entrenamiento Cultura de Seguridad Informática Relación con clientes y proveedores

## 2.2

## Solución a problemas de tecnología

Los problemas ocasionados por la ejecución de problemas de tecnología pueden solucionarse con:

- **Cifrado:** el cifrado nos permite salvaguardar la confidencialidad de la información. Mediante el cifrado transformamos la información de modo que resulte ininteligible. Para devolver la información a su estado original es necesario realizar la transformación inversa (descifrado).
- **Encriptación:** la firma electrónica garantiza la integridad de la información gracias al uso de dos claves: clave pública y privada, e impide la suplantación de identidad del firmante.

- **Productos y herramientas de seguridad:** la Autenticación nos permite evitar la suplantación de identidades y algunos accesos ilícitos a los sistemas. Cuando se intenta acceder con autenticación, el sistema:
  - Pide la identidad del usuario.
  - Comprueba la autorización de acceso al usuario.

RedAbogacía ofrece un incomparable grado de seguridad en la autenticación de los usuarios, pues se basa en el uso de los certificados ACA, totalmente reconocidos.

### 2.3

### Solución a problemas de procesos

Los problemas ocasionados por la ejecución de procesos ya sean con permiso del usuario o sin permiso que provocan daños y desperfectos en archivos del sistema pueden solucionarse con:

- **Una adecuada planificación de la seguridad**
- **Mecanismos de prevención y detección:** existen diversas formas de prevenir y detectar procesos perjudiciales para nuestro sistema, los más conocidos son :

- **Filtros antispam:** con los que detectamos el correo no solicitado y permite eliminarlo o trasladarlo a otra carpeta.

Los servicios de correo electrónico alojados en RedAbogacía cuentan con protección antispam.

- **Antivirus:** permiten la detección, neutralización y eliminación de programas maliciosos. Normalmente estos sistemas lanzan procesos de actualización de las bases de datos del antivirus para mantener el equipo siempre seguro.
- **Cortafuegos:** previenen la realización de conexiones no deseadas a nuestro ordenador, lo cual evita posibles intrusiones y ataques a nuestro sistema.

- **Reacción y recuperación**

- **Actualizaciones:** es importante disponer de software actualizado y mecanismos de actualización automática.
- **Copias de seguridad:** la realización de copias de seguridad y puntos de restauración permiten la recuperación de información en caso de que se produzca algún desastre informático.

## 2.4

**Solución a problemas de personal poco cualificado en asuntos de seguridad**

Los problemas ocasionados por personal poco cualificado o desinformado en asuntos de seguridad informática pueden solucionarse con:

- **Personal dedicado a la seguridad informática:** si los volúmenes de información son muy elevados y requieren de una gran seguridad por tratarse de información confidencial o reservada es necesario disponer de personal especializado capaz de tomar medidas que eviten que personas no autorizadas manipulen los equipos informáticos.
- **Cultura, formación en materia de seguridad informática y entrenamiento:** la formación de los usuarios permite evitar aquellos problemas de seguridad debidos a desconocimiento o al incorrecto uso de las herramientas informáticas.

Puntos Clave



## 3

## SEGURIDAD EN EL CORREO ELECTRÓNICO

## 3.1

## El papel del certificado digital en el correo electrónico

Enviar un correo electrónico se puede hacer de manera segura mediante el empleo de certificados digitales que le permitirán firmar y cifrar los mensajes, incluyendo los archivos adjuntos, y evitar que sean leídos y manipulados por personas no autorizadas.

**La firma de los mensajes le asegura:**

1. La identidad del remitente.
2. La integridad del mensaje, es decir, la posibilidad de detectar cualquier alteración del mismo.

Por su parte, el cifrado de los mensajes le aporta confidencialidad. Únicamente los destinatarios del mensaje podrán descifrarlo.

Adicionalmente, si emplea un certificado reconocido y un dispositivo seguro de creación de firma tendrá firma electrónica reconocida y, por tanto, equivalencia de efectos con la firma manuscrita: la firma electrónica con certificado ACA es firma electrónica reconocida.

## 3.2

## Cómo puedo firmar digitalmente un correo electrónico

Puede que su Outlook tenga la barra de herramientas configurada para firmar electrónicamente un correo electrónico, de tal forma que para firmarlo sólo tendrá que escribir el correo correspondiente, introducir la tarjeta en el lector ACA y pulsar el botón **"Firmar"**. Pulse el botón **"Enviar"**, y le pedirá el PIN de la tarjeta para realizar la firma del correo.

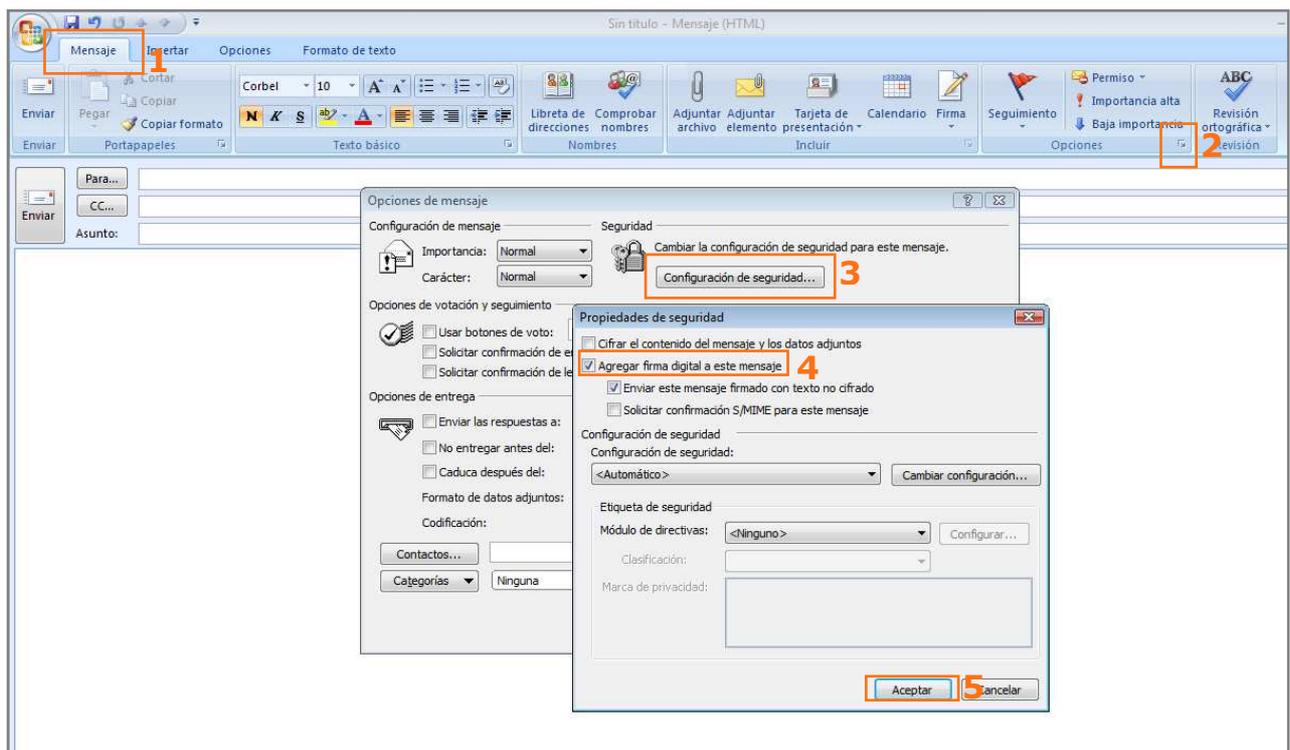


**Outlook Express:** Pulse el botón **"Firmar"** que se encuentra en la barra de herramientas superior.



**Outlook:**

- Abrir un nuevo mensaje.
- En la pestaña **"Mensajes"** + **"Opciones"**, haga clic en el botón **"Configuración de seguridad"** y marque la casilla **"Agregar firma digital a este mensaje"** + **"Aceptar"**.



- Redacte el mensaje y envíelo.

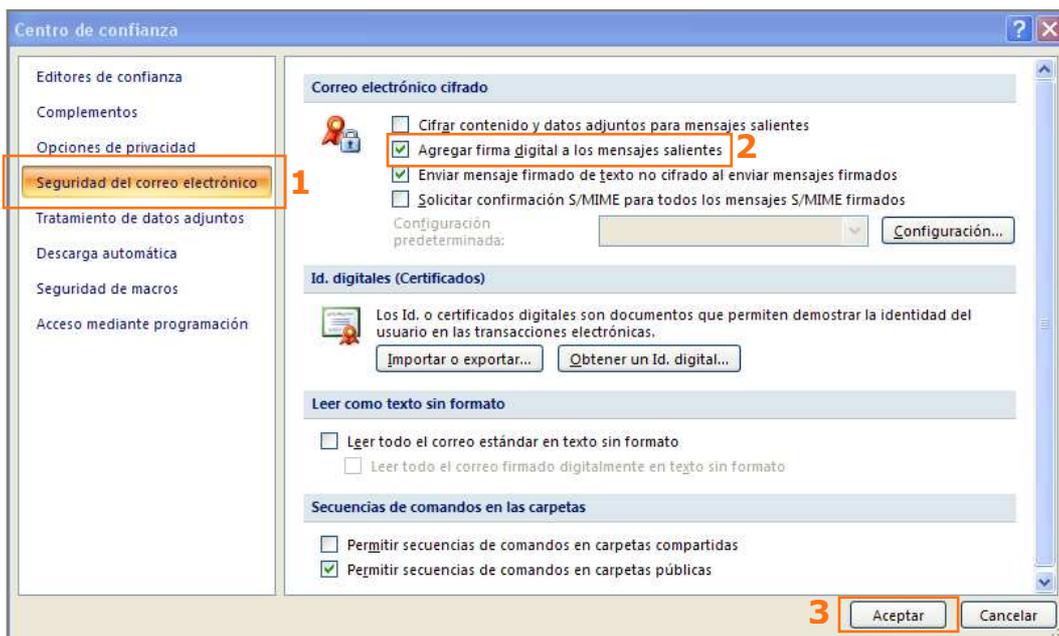
## OPCIONES AVANZADAS OUTLOOK

Si no tiene la barra de herramientas configurada tiene dos opciones antes de firmar el correo: hacer una configuración predeterminada de la firma electrónica o agregar la firma siempre que quiera mandar un correo con firma digital:

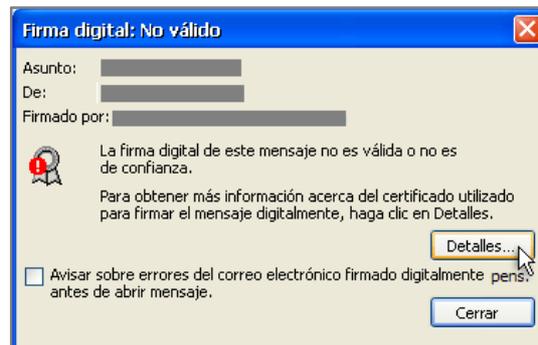
1. Si hace una **configuración predeterminada de la firma digital**, el correo se firmará automáticamente, sin necesidad de agregar su firma electrónica. Para esta opción siga los pasos que mostramos a continuación:
  - Introduzca la tarjeta en el lector de tarjetas ACA, empezará a parpadear una lucecita hasta que se queda fija.
  - Abra el **Outlook**.
  - Diríjase a:
    - **"Herramientas" + "Centro de confianza"** (para Outlook 2007).
    - **"Herramientas" + "Opciones" + "Seguridad"** (para Outlook 2003).
  - Seleccione la pestaña **"Seguridad del correo electrónico"**.
  - En el apartado **"Correo electrónico cifrado"** seleccione **"Configuración"**.



- Aquí detectará su tarjeta. Si detecta su firma aparecerán sus datos, en caso contrario tendrá que reiniciar el ordenador con la tarjeta dentro del lector y volver a realizar los pasos anteriores.
- En esta ventana **"Cambiar la Configuración de Seguridad"** deberán de aparecer sus datos en el desplegable.
- Elija su **"Certificado de firma"** en el desplegable inferior.
- Pulse **"Aceptar"** y ya está configurado.
- Entre de nuevo en **"Herramientas" + "Centro de confianza"**.
- Seleccione la pestaña **"Seguridad del correo electrónico"** y marque **"Agregar firma digital a los mensajes salientes" + "Aceptar"**, y a partir de ahora todos sus correos llevarán firma digital automáticamente.

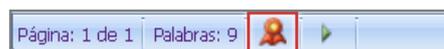


2. Cuando abra un correo, el **Outlook le informará sobre la validez de la firma digital del correo** y le indicará que el remitente ha firmado digitalmente el mensaje enviado. Del mismo modo, el cliente de correo le informará si la firma no es válida:

**3.3****Cómo puedo firmar digitalmente un documento**

Si desea proporcionar seguridad en cuanto a la autenticidad, integridad y origen de un documento, puede agregar una firma digital invisible a cualquier documento de Word, Excel y PowerPoint.

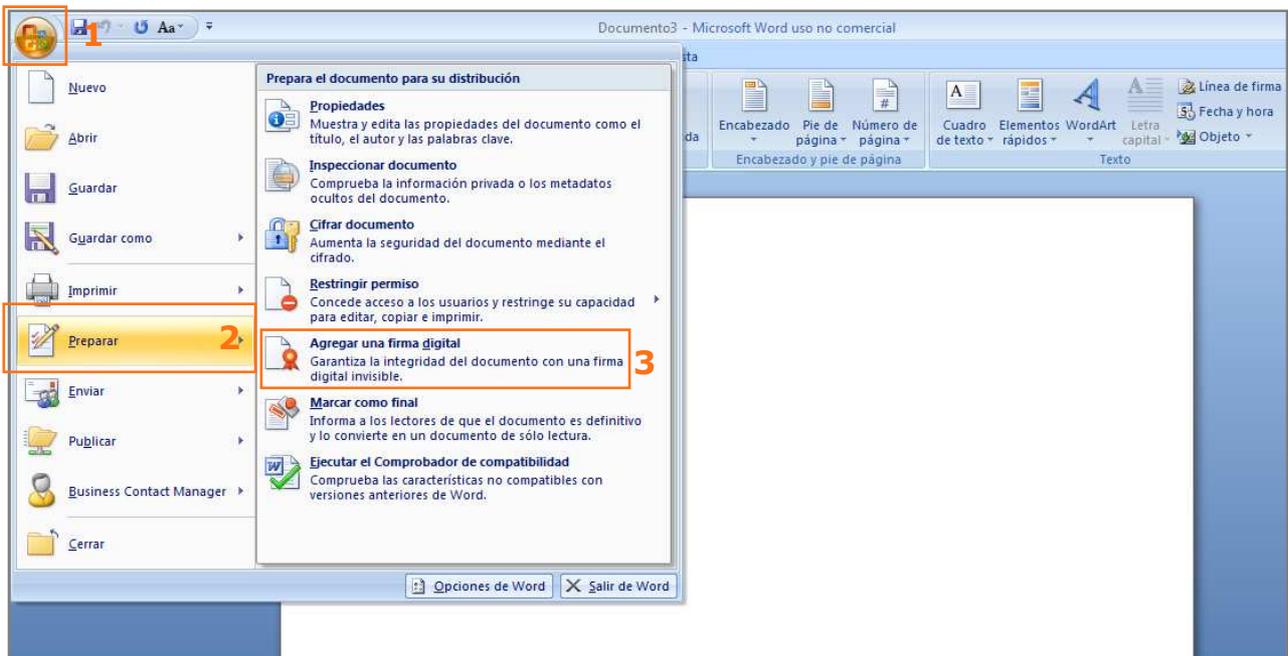
Una firma digital invisible no se ve en el contenido del propio documento, pero los destinatarios del documento pueden determinar si se ha firmado digitalmente viendo la firma digital del documento o buscando el botón Firmas en la barra de estado situada en el lado inferior de la pantalla.



Una vez firmado digitalmente un documento, será de sólo lectura para impedir la realización de modificaciones.

Los pasos que debe seguir son:

1. Introduzca su tarjeta en el lector.
2. Abra el documento de Office que quiera firmar digitalmente (Word, Excel, PowerPoint).
3. Haga clic en el **botón de Microsoft Office** , seleccione **"Preparar"** y, a continuación, haga clic en **"Agregar una firma digital"**.



4. Si desea consignar la razón de firmar el documento, escriba esta información en el cuadro de diálogo "Firmar" + "Razón para firmar este documento".
5. Haga clic en "Firmar".

Para versiones anteriores al Microsoft Office 2007: Cree un nuevo documento y seleccione "Opciones" del menú "Herramientas". Dentro del menú seleccione "Seguridad". Seleccione la opción "Firmas digitales" y se abrirá la ventana de firmas. Seleccione la opción "Agregar" para ver las firmas disponibles y seleccione la que desee. Al finalizar el proceso un icono en el pie del documento indicará que está firmado digitalmente.

## 3.4

## Cifrado del correo electrónico

**Outlook Express**

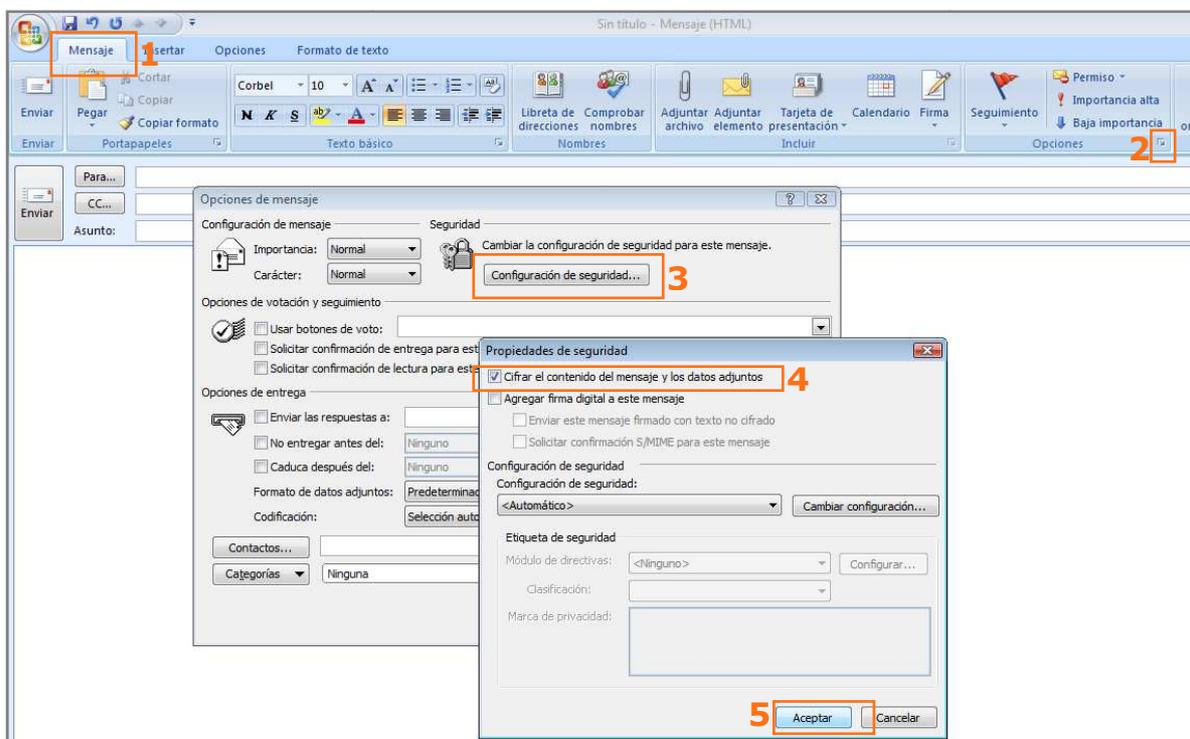
Si desea cifrar un mensaje tan solo tiene que pulsar sobre el botón **"Cifrar"**. En este caso es necesario disponer de la clave pública de los destinatarios para poder realizar el cifrado.

Cuando quiera leer un mensaje cifrado que haya recibido, necesitará introducir la tarjeta en el lector y se le pedirá el PIN para poder descifrar el mensaje, sino no podrá descifrar el mensaje.

**Outlook**

Si desea cifrar un mensaje en Outlook, sólo tiene que:

- Escribir el mensaje de correo correspondiente.
- En la pestaña **"Mensajes" + "Opciones"**, haga clic en **"Configuración de seguridad"** y marque la casilla **"Cifrar el contenido del mensaje y los datos adjuntos" + "Aceptar"**.



- Envíe el correo.

### ¿Cuál es la diferencia entre cifrar un correo y firmar un correo?

---

- **Con la firma**, el mensaje es legible para cualquier persona, pero está asegurando que el emisor del mensaje que aparece en el campo emisor es realmente quien dice ser (**autenticación** del remitente). Además, la firma digital también le asegura que nadie ha modificado el mensaje original, es decir, **integridad**.
- **Con el cifrado**, por el contrario, lo que se consigue es que nadie, excepto el receptor del mensaje, pueda ver su contenido, es decir, **confidencialidad**.

## Puntos Clave



Firmar digitalmente un correo asegura la confidencialidad del contenido entre el emisor y receptor, evitando con ello que sea leído y manipulado por personas no autorizadas.



Para **firmar digitalmente un correo electrónico**:

- Introduzca previamente la tarjeta en el lector y escriba el correo electrónico.
- Para firmarlo:
  - **Con Outlook Express:** Pulse el botón **"Firmar"** que se encuentra en la barra de herramientas superior.
  - **Con Outlook:** **"Mensajes" + "Opciones" + "Configuración de seguridad"** y marque la casilla **"Agregar firma digital a este mensaje" + "Aceptar"**.



Para **firmar digitalmente un documento**:

- **Con Microsoft Office 2007:** Abra el documento de Office que quiera firmar digitalmente y pulse el **botón de Microsoft Office**  + **"Preparar"**, y haga clic en **"Agregar una firma digital" + "Firmar"**.



Para **cifrar un correo**:

- **Con Outlook Express:** Pulse el botón **"Cifrar"** que se encuentra en la barra de herramientas superior.
- **Con Outlook:** En la pestaña **"Mensajes" + "Opciones"**, haga clic en el botón **"Configuración de seguridad"** y marque la casilla **"Cifrar el contenido del mensaje y los datos adjuntos" + "Aceptar"**.

**Ejercicios Prácticos****EJERCICIO 1: Correo Electrónico con firma digital**

En este ejercicio practicaré el uso de la firma electrónica/digital (con certificado) en el correo electrónico, garantizando así la seguridad del envío y recepción de correos electrónicos con otros agentes.

- Diríjase a su cliente de correo electrónico y escriba todos los datos necesarios para hacer efectiva su emisión.
  - Destinatarios principales.
  - Poner en copia (CC) a otros destinatarios que no son principales.
  - Poner en copia oculta (CCO) a otros destinatarios que no son los principales.
  - El asunto y el cuerpo del mensaje.
- Diríjase a la opción correspondiente (dependiendo del cliente del correo) para firmar digitalmente el mismo.

**EJERCICIO 2: Firma de documentos**

En este ejercicio practicaré el uso de la firma digital (con certificado) en documentos electrónicos.

- Cree un documento en Word y fírmelo digitalmente.

## SÍNTESIS DE LA SEGUNDA SESIÓN

Durante esta segunda sesión ha visto cómo los problemas de seguridad en entornos informáticos están clasificados según sean problemas vinculados a la tecnología, a la falta de planificación de la seguridad o al poco conocimiento del personal en materia de seguridad.

Los problemas de seguridad vinculados a la tecnología son ocasionados fundamentalmente por conductas de espionaje y sabotaje informático que provocan la destrucción, inutilización, modificación y obstaculización de la información de los equipos informáticos.

Los problemas de seguridad vinculados a la falta de planificación derivan de la poca frecuencia de realización de copias de seguridad y actualización de bases de datos de antivirus, lo que provoca que programas externos accedan al ordenador y realicen operaciones que puedan dañar los archivos de su equipo informático.

Por último, están los problemas derivados de la falta de información en materia de seguridad por parte de los usuarios.

Para solventar cada uno de los anteriores problemas existen herramientas que pueden ayudar a minimizar o evitar el impacto de los mismos: el cifrado y la encriptación de los mensajes que intercambia con otras personas, la instalación de antivirus y filtros antispam, las actualizaciones y copias de seguridad, y la formación o entrenamiento de acciones que mejoren la seguridad de nuestro equipo informático.

Una forma de asegurar que sus comunicaciones con terceras personas sean confidenciales y libres de manipulación, es el correo electrónico con certificado digital o la firma de documentos con firma electrónica.

La seguridad es un tema muy importante en entornos informáticos, ya que una invasión a la misma puede provocar la destrucción de archivos con información vital para el funcionamiento normal de su trabajo diario.

## AUTOEVALUACIÓN 2

**1. Los problemas vinculados a la seguridad informática pueden estar provocados por:**

- a. La tecnología y los virus informáticos
- b. La tecnología, la falta de planificación en la seguridad y la falta de información por parte de los usuarios
- c. La tecnología y desinformación en materia de seguridad de los usuarios

**2. La diferencia fundamental entre un virus y un troyano es:**

- a. El virus accede a través de Internet y el troyano no
- b. No hay ninguna diferencia entre ambos
- c. El virus se reproduce dentro del sistema informático y el troyano no

**3. El cifrado y la encriptación serían soluciones a los problemas derivados de:**

- a. La planificación de procesos
- b. El uso indebido de la tecnología
- c. La falta de información y entrenamiento de las personas en materia de seguridad

**4. ¿Existe alguna diferencia entre firma digital y cifrado de un mensaje?**

- a. Sí, con la firma digital garantizamos autenticación e integridad del mensaje mientras que con el cifrado aseguramos la confidencialidad
- b. No, ninguna
- c. Sí, el cifrado da más garantías de confidencialidad e integridad que la firma digital

**5. Los cortafuegos informáticos son...**

- a. Una herramienta de detección de intrusiones ilícitas
- b. Una herramienta de prevención de intrusiones ilícitas
- c. Un mecanismo de neutralización

**6. El sabotaje informático comprende aquellas actitudes ilícitas orientadas a...**

- a. La destrucción, inutilización, modificación y obstaculización de la información
- b. El conocimiento indebido de la información
- c. La revelación indebida de la información

**7. ¿Cuáles de los siguientes conceptos no están asociados con los virus?**

- a. Bombas lógicas
- b. Troyanos
- c. Filtros antispam

**8. ¿Cuáles de las siguientes herramientas nos permiten la recuperación de información?**

- a. Actualizaciones de antivirus
- b. Copias de seguridad
- c. Puntos de restauración del sistema

**9. ¿Cuáles de los siguientes documentos es posible firmar digitalmente?**

- a. Documentos de Word
- b. Documentos de Excel
- c. Las opciones a y b son correctas

**10. Si firma un documento digitalmente...**

- a. Será de escritura y lectura, pero se podrán ver las posibles alteraciones del mismo tras ser firmados.
- b. Este será de sólo lectura para impedir la realización de modificaciones.
- c. Será de escritura y lectura y no podrán verse las posibles alteraciones del mismo tras ser firmados.

**Soluciones: en los anexos**

# Tercera sesión

## Servicios electrónicos para el ejercicio de la abogacía

**Al finalizar esta sesión habrá adquirido los siguientes conocimientos...**

- ❑ Uso de los servicios colegiales de utilidad profesional: Buromail, Iuris et Legis, Campus virtual, RedAbogacía Libros, e-Mensajes, Oficina postal, Oficina virtual de catastro.
- ❑ Breve descripción de los servicios con las administraciones estatales, autonómicas y locales.

1

SERVICIOS COLEGIALES DE UTILIDAD PROFESIONAL

Recordamos que RedAbogacía ofrece múltiples servicios orientados a facilitar el ejercicio profesional del abogado a través del portal [www.redabogacia.org](http://www.redabogacia.org). Éstos se encuentran clasificados en función de si se trata de servicios colegiales o servicios de las Administraciones Públicas.

Los **servicios colegiales** se subdividen en dos grupos:

- Servicios de relación con el colegio de abogados (explicados en el módulo básico del curso).
- Servicios de utilidad profesional (se explicarán 6 servicios en este capítulo y 3 servicios más en el módulo avanzado del curso).

Y los **servicios con las Administraciones Públicas** se subdividen en:

- Estatales, autonómicos y locales (se explicarán en el siguiente capítulo de este módulo).

1.1

Buromail

**BUROMAIL**

**DESCRIPCIÓN**

Servicio que permite realizar la tramitación certificada de documentos a través de correo electrónico con otros usuarios de Certificado ACA.

**USUARIOS**

Abogados, colegios de abogados y otras instituciones del colectivo de la abogacía.

**FUNCIONALIDADES**

Las funcionalidades se encuentran en el lateral izquierdo de la pantalla de inicio al servicio.

1. NUEVO MENSAJE
2. LIBRETA DESTINATARIOS
3. CARPETAS
4. PREFERENCIAS
5. CONFIGURACIÓN DE ALERTAS
6. MANUAL DE USUARIO
7. DESCONECTAR

**VENTAJAS**

- Estos correos electrónicos generan prueba, con plena validez jurídica, de envío y de recepción por parte del destinatario.
- El abogado podrá configurar avisos tanto a su móvil como a cualquier correo electrónico que le avisará de la recepción de un nuevo mensaje.
- Garantía en el servicio ofrecido a los ciudadanos: El certificado digital asegura ante terceros la condición de abogado de forma inequívoca, ya que ha sido emitido por su colegio de abogados bajo la supervisión del Consejo General de la Abogacía.

La utilización del servicio Buromail a través de su Certificado Digital ACA implica el uso de la firma digital, esto supone que los datos que ha declarado van a ser firmados digitalmente y serán almacenados con las necesarias medidas de seguridad.

**MÁS INFORMACIÓN**

Opción Manual de Usuario (menú lateral izquierdo).

FUNCIONALIDAD 1

NUEVO MENSAJE

1

CREAR UN NUEVO MENSAJE



2

ELEGIR DESTINATARIOS



3

ENVIAR O GUARDAR DATOS

- ✓ **Recuerde** que es necesario tener la tarjeta criptográfica con su certificado ACA introducida en el lector para entrar en la zona privada de su colegio.

1

CREAR UN NUEVO MENSAJE

Para crear un nuevo mensaje es necesario que acceda a la zona privada de la plataforma tecnológica de RedAbogacía y seleccione el servicio Buromail que se encuentra en el menú del lateral izquierdo.

Visualizará una pantalla de inicio y un conjunto de funcionalidades en la zona izquierda de la ventana. Seleccione la primera opción que es **"Nuevo mensaje"**.

Le aparecerá un formulario que tendrá que completar con los datos del mensaje.

## 2

ELEGIR  
DESTINATARIOS

Redacte el nuevo mensaje en el formulario que aparece en la ventana e introduzca los siguientes campos:

- **Destinatarios:** podrán ser usuarios que se hayan dado de alta en este servicio con anterioridad o usuarios externos que no estén dados de alta, con lo que se permite introducir cualquier tipo de cuenta de correo electrónico.
- **Destinatarios CC:** destinatarios internos o externos con cuentas de correo electrónico de cualquier tipo, pero sin posibilidad de "Confirmación de Lectura", es decir, se garantiza mediante firma digital el envío del mensaje pero no la recepción.
- **Destinatarios BCC:** destinatarios internos y externos con las mismas características que en el caso anterior.
- **Asunto:** título del mensaje.
- **Texto:** texto libre que constituye el cuerpo del mensaje.
- **Ficheros adjuntos:** enlace que permite adjuntar escritos que considere oportunos.

El formulario muestra un campo de texto etiquetado como "Ficheros Adjuntos:" con un cursor de texto. A la derecha del campo hay dos botones: "Añadir" y "Quitar". Debajo del campo de texto hay un botón "Examinar...".

- **Confirmación de lectura:** haga clic en este enlace para garantizar que el texto del mensaje enviado ha sido leído por el destinatario principal.
- **Idioma:** permite elegir el idioma que utilizará para la palantilla "fechado y firma".
- **Cifrado del mensaje:** sólo se podrá marcar esta opción si el mensaje va enviado a un único destinatario y este es usuario del servicio Buromail.

3

ENVIAR O GUARDAR  
DATOS

Una vez completos todos los campos correspondientes, pulse sobre el botón **“Enviar”**.

Pero usted también puede:

- No enviar el mensaje y guardarlo para así realizar el envío en otro momento el formulario, para ello pulse en el botón **“Guardar como borrador”**.
- Enviar el mensaje y guardarlo en el borrador, para ello tendrá que elegir la opción de **“Conservar borrador despues de firmar”**, de no marcar esta opción el mensaje no será guardado.

## FUNCIONALIDAD 2

## LIBRETA DE DESTINATARIOS

El servicio Libreta de Destinatarios, permite el mantenimiento de una libreta de direcciones con los destinatarios más frecuentemente utilizados por el usuario. Para acceder al mismo, hacer clic en **“Libreta Destinatarios”**, opción ubicada en el menú del lateral izquierdo.

Nada más acceder a la libreta aparece la ventana donde se muestran todos los contactos que posee el usuario, dando detalles de cada uno (nombre, dirección de correo y descripción), y la posibilidad de modificar dichos datos. Se podrá filtrar este listado por tres campos: nombre, primer apellido y segundo apellido.

La libreta de destinatarios permite las siguientes funciones:

- Crear contacto.
- Borrar contacto.
- Alta abogado por nombre.
- Alta abogado por ámbito regional.
- Modificar contacto.
- Grupos.
- Crear grupo.
- Borrar grupo.
- Modificar grupo.

FUNCIONALIDAD 3

CARPETAS

Este servicio proporciona acceso a los mensajes disponibles de manera organizada en carpetas:



Los mensajes se clasifican en las siguientes carpetas según su naturaleza:

- 1. Bandeja de entrada:** contiene los mensajes de correo recibidos por el usuario, dando la información del número total de mensajes y, también, del número de ellos no leídos.
- 2. Acuses de recibo:** contiene los mensajes que informan al abogado del envío del mensaje con fecha y hora, junto al contenido íntegro del escrito enviado, es decir, el documento principal y los documentos anexos que se hayan adjuntado.
- 3. Confirmación de lectura:** a través de esta carpeta el sistema informa al abogado de la fecha y hora en la que el mensaje ha sido leído por su/s destinatario/s.
- 4. Borradores:** almacena los mensajes que el usuario ha decidido guardar una vez enviado o ha decidido guardar para enviar en un momento posterior.
- 5. Papelera:** a través de esta carpeta el sistema almacena los mensajes eliminados.

Cada una de las distintas carpetas, ofrece la opción de ver el mensaje de forma detallada, moverlo a otra carpeta o borrarlo. Una vez dentro de cada carpeta el usuario podrá visualizar los mensajes con sólo pulsar el botón izquierdo del ratón sobre el título del campo, así como descargar el mensaje completo y sus adjuntos en la opción **"datos del mensaje"**.

## FUNCIONALIDAD 4

## PREFERENCIAS

El servicio Preferencias se utiliza para seleccionar e introducir aspectos referidos al perfil del usuario en función de las necesidades del mismo, tales como:

- **Cambio de idioma:** el abogado puede elegir el idioma en el que desea recibir los avisos de RedAbogacía: castellano, catalán, gallego o euskera.
- **Avisos confidenciales:** solo podrán ser abiertos por el interesado con su certificado digital. Los avisos de recepción por e-mail y SMS no podrán incluir información del contenido.
- **Elementos por página:** número de avisos a mostrar por página.
- **Dispositivos:** se mostrarán los diferentes dispositivos de aviso a utilizar.

## FUNCIONALIDAD 5

## CONFIGURACIÓN DE ALERTAS

El abogado podrá configurar avisos tanto a su móvil como a cualquier correo electrónico que el avisará de la recepción de un nuevo mensaje.

## FUNCIONALIDAD 6

## MANUAL DE USUARIO

Este servicio está ubicado en el Menú del lateral izquierdo y para acceder al mismo tan solo tiene que hacer clic en el enlace "**Manual Usuario**".

## FUNCIONALIDAD 7

## DESCONEXIÓN

La funcional Desconexión permite al usuario abandonar el sistema.

1.2

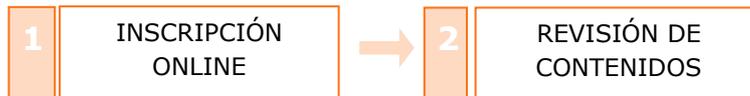
Campus virtual

CAMPUS VIRTUAL	
<b>DESCRIPCIÓN</b>	Plataforma de e-learning que ofrece contenidos formativos con la posibilidad de examinarse para posteriormente obtener un certificado de aprovechamiento expedido por el colegio de residencia y el CGAE.
<b>USUARIOS</b>	Abogados, colegios de abogados y otras instituciones del colectivo de la abogacía.
<b>FUNCIONALIDADES</b>	<p>Las funcionalidades se encuentran en el lateral izquierdo de la pantalla de inicio al servicio.</p> <ol style="list-style-type: none"> <li>1. CURSOS</li> <li>2. OBTENCIÓN DEL TÍTULO</li> <li>3. DOCUMENTOS</li> <li>4. MANUAL DE USUARIO</li> </ol>
<b>VENTAJAS</b>	<ul style="list-style-type: none"> <li>▪ Posibilidad del aprendizaje a distancia y a la medida según las necesidades del abogado.</li> <li>▪ Permite al abogado seguir formándose, en aquellas materias que lo requieran para el mejor desarrollo de sus actividades.</li> <li>▪ Desde el Campus virtual se facilita al alumno la asistencia de un tutor online para la resolución de consultas sobre temario, forma de acceso a los exámenes a incidencias técnicas a través de un botón disponible en cada uno de los módulos.</li> </ul>
<b>MÁS INFORMACIÓN</b>	Opción Manual de Usuario (menú lateral izquierdo).

FUNCIONALIDAD 1

CURSOS

Esta funcionalidad le permitirá realizar cursos online.

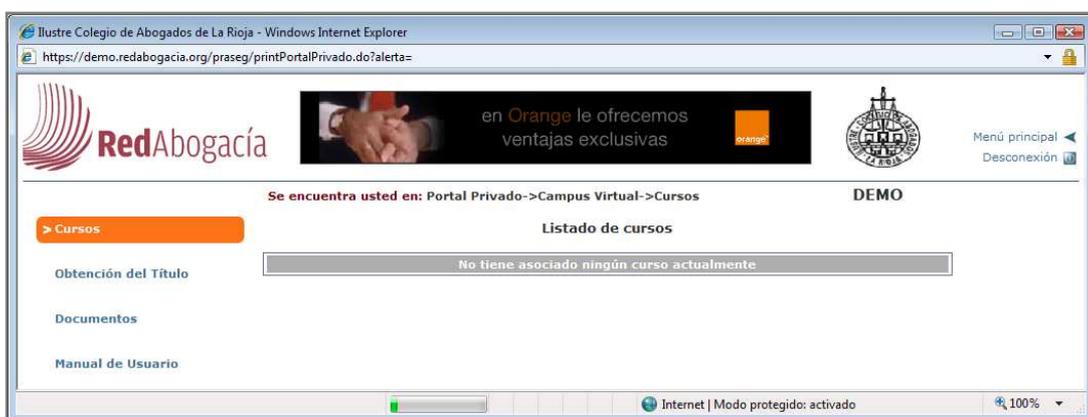


- ✓ **Recuerde** que es necesario tener la tarjeta criptográfica con su certificado ACA introducida en el lector para entrar en la zona privada de su colegio.

1 INSCRIPCIÓN  
ONLINE

Para acceder a los cursos, desde el menú de la izquierda pulse el módulo de **"CURSOS"** y seleccione el curso que le interese realizar en ese momento.

Si el usuario no tiene asociado ningún curso, el sistema le indicará esta condición y deberá realizar la inscripción que corresponda para que así el sistema asocie al usuario con el curso solicitado.



En caso contrario, se accederá a un listado de los cursos correspondientes.

En el listado se especifica el Módulo (nombre del curso al que se ha inscrito) y el video (enlace a sus correspondientes contenidos).

La inscripción online se podrá realizar cuando RedAbogacía oferte nuevos cursos, accediendo al banner correspondiente en la página principal de [www.redabogacia.org](http://www.redabogacia.org).

2

REVISIÓN DE  
CONTENIDOS

Al acceder al campus virtual, el alumno sólo podrá ver los contenidos de los modulos a los que haya optado asistir, sea de forma online o presencial. La autenticación con certificado digital garantiza la identidad del alumno, lo que asegura un control por parte del tutor online en todo momento.

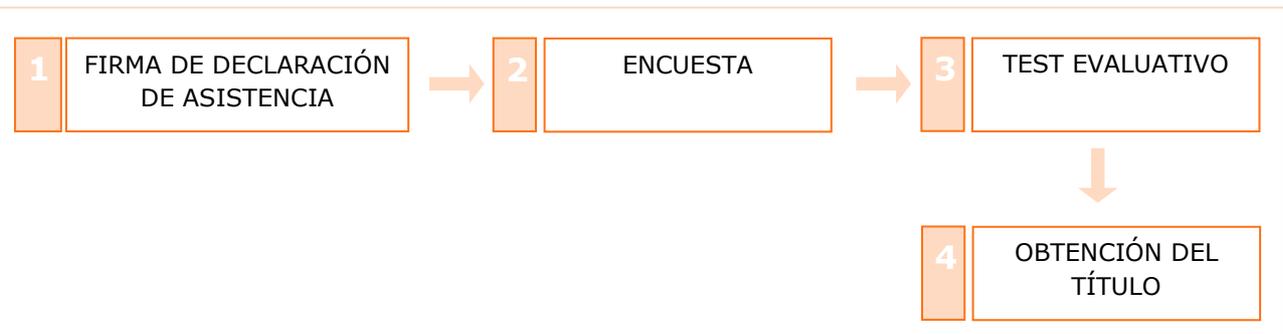
Cada módulo dispone de un índice navegable que permite avanzar sobre el contenido al propio ritmo. Si lo desea, el alumno puede imprimir y guardar el contenido, así como consultar una serie de manuales de uso y documentación de apoyo que permite profundizar en algunos temas.

## FUNCIONALIDAD 2

## OBTENCIÓN DEL TÍTULO

Para obtener el certificado de aprovechamiento seleccionamos el módulo **"Obtención del Título"** del menú de la izquierda.

Este módulo funcional permite realizar los pasos necesarios para obtener el/los certificado/s de aprovechamiento/s.



1 FIRMA DE DECLARACIÓN DE ASISTENCIA

Una vez finalizado un módulo y para poder acceder al test, el colegiado ha de firmar con su certificado digital una declaración de asistencia por la que afirma haber revisado los contenidos correspondientes al módulo del que se trate.

Al pulsar sobre el curso pendiente de firmar, se muestra la declaración de asistencia.

Si pulsa sobre el botón **"Aceptar"** se procede a realizar la firma digital de la declaración de asistencia, requisito imprescindible para poder acceder al test evaluativo.

2 ENCUESTA

Una vez firmada la declaración de asistencia deberá completar una encuesta de valoración de la calidad del curso impartido, tanto en lo referido a los contenidos como a los materiales y tutores o profesores, para realizar futuras mejoras.

Consejo General de la Abogacía Española - Microsoft Internet Explorer

ver. 1.13 MENU PRINCIPAL DESCONEXION RED ABOGACÍA

Jueves, 29 de Mayo de 2008

Portal Privado->Campus Virtual->Obtención del Título

Manual de Usuario Obtención del título Mostrar contenidos curso

**DEMO**

Se dispone a realizar el examen de Examen Módulo Básico. Éste consta de 15 preguntas y será necesario responder correctamente al menos 1 preguntas.

1.- Los periféricos de entrada sirven para

- Que se produzca una comunicación bidireccional entre el ordenador y el usuario.
- Que el ordenador nos comunique información.
- Que nosotros introduzcamos información en el ordenador.

2.- El modo de arranque "Seguro" del sistema operativo consiste en

- El sistema arranca con normalidad.
- El sistema arranca habilitando únicamente la funcionalidad más básica.
- El sistema se protege frente a virus.

3.- El modo de arranque "Última configuración buena conocida" del sistema operativo consiste en

- El sistema arranca empleando la configuración más reciente que haya funcionado sin problemas.
- El sistema arranca habilitando únicamente la funcionalidad más básica.
- El sistema arranca con normalidad.

4.- ¿Cuál de los siguientes modos de inicio de sesión resulta más deseable desde el punto de vista de la seguridad?

- Inicio de sesión automático.
- Inicio de sesión normal.
- Inicio de sesión seguro.

5.- El puntero del ratón es

- Es un símbolo que puede tener distintas formas y dibujos y que permite ejecutar programas.
- Es un símbolo con forma de flecha que se desplaza por la pantalla al mover el ratón.

3

## TEST EVALUATIVO

Las preguntas no respondidas o respondidas incorrectamente, no suman ni restan puntos. Una vez respondidas las preguntas necesarias, se pulsará el botón **"Aceptar"**.

**Resultado Suspenso**

Si al completar el examen, éste estuviera suspenso, se abrirá una nueva ventana donde aparecerá un listado con las preguntas del examen contestadas incorrectamente. Pulse **"Ver preguntas fallidas"**.

Se puede realizar un nuevo examen pulsando el botón **"Realizar nuevo examen"** desde la pantalla de **"Examen suspenso"**. En ese momento volverá a la pantalla de examen con una nueva prueba de evaluación. Se puede repetir el proceso de forma indefinida hasta que apruebe el test.

**Resultado Aprobado**

Si ha superado la prueba de evaluación aparecerá un texto donde se le recordará que puede descargarse el certificado de aprovechamiento.

4

OBTENCIÓN DEL  
TÍTULO

Para descargarse el certificado hay que pulsar el botón **"Descargar Certificado de Aprovechamiento"**. Se abrirá una pantalla en formato PDF, donde se podrá ver el certificado y a su vez, tendrá la posibilidad de guardarlo en el disco duro.

**FUNCIONALIDAD 3****DOCUMENTOS**

La funcionalidad documentos da acceso a cada uno de los módulos del curso para la descarga de contenidos.

**FUNCIONALIDAD 4****MANUAL DE USUARIOS**

Este servicio está ubicado en el Menú del lateral izquierdo y para acceder al mismo tan solo tiene que hacer clic en el enlace **"Manual Usuario"**.

1.3

Iuris et Legis

IURIS ET LEGIS

DESCRIPCIÓN

Este servicio ofrece al abogado un acceso gratuito, rápido y sencillo a bases de datos de códigos y jurisprudencia propiedad de editoriales jurídicas, sin necesidad de instalar Cds o DVDs, sin limitaciones de espacio y sin tener que desplazarse a su colegio de abogados.

USUARIOS

Abogados, colegios de abogados y otras instituciones del colectivo de la abogacía.

FUNCIONALIDADES

Las funcionalidades se encuentran en el lateral izquierdo de la pantalla de inicio al servicio.

1. CONTENIDOS ACCESO LIBRE CÓDIGOS-LA LEY
2. REVISTA LEGISLACIÓN
3. DIARIO DE NOTICIAS
4. VISUALIZADOR CICERO

VENTAJAS

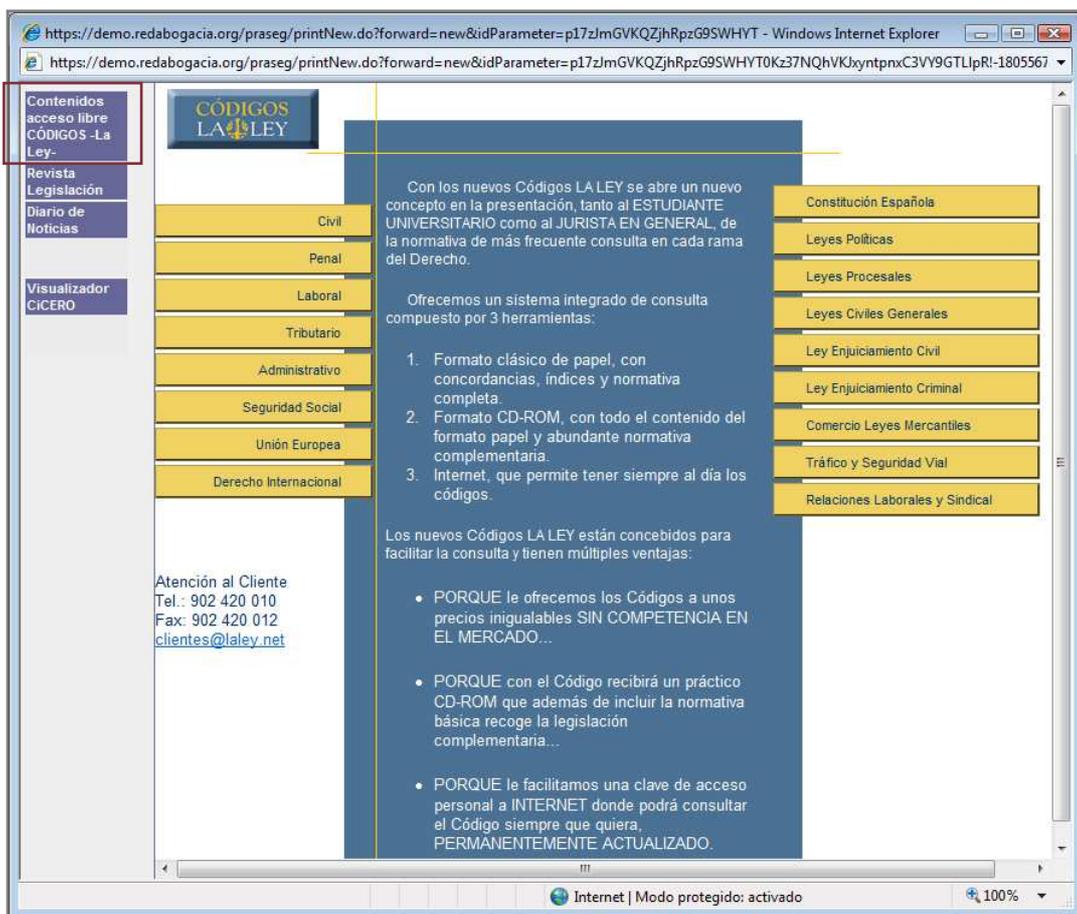
Contenidos gratuitos:

- Acceso a los Códigos LA LEY.
- Revista de legislación LA LEY.
- Cícero (Software para visionar los juicios).

FUNCIONALIDAD 1

ACCESO LIBRE CÓDIGOS-LA LEY

Acceso libre a códigos La Ley: Sistema integrado de consulta en cada una de las ramas del Derecho donde la información se encuentra perfectamente organizada.



FUNCIONALIDAD 2

REVISTA LEGISLACIÓN

Opción que da entrada al servicio de publicaciones, bases de datos, tienda online, programa de gestión de despachos información sobre jornadas profesionales.

Contenidos acceso libre CÓDIGOS -La Ley-  
Revista Legislación  
Diario de Noticias  
Visualizador CICERO

LA LEY grupo Wolters Kluwer

Wolters Kluwer España LA LEY CISS

Inicio

noviembre  
L M X J V S D  
01 02  
03 04 05 06 07 08 09  
10 11 12 13 14 15 16  
17 18 19 20 21 22 23  
24 25 26 27 28 29 30

octubre  
L M X J V S D  
01 02 03 04 05  
06 07 08 09 10 11 12  
13 14 15 16 17 18 19  
20 21 22 23 24 25 26  
27 28 29 30 31

Proyectos de Ley  
Proposiciones de Ley  
Para imprimir  
Información Editorial

**REVISTA DE LEGISLACIÓN**  
**BOLETÍN OFICIAL DEL ESTADO**  
Nº 281 DE 21 DE NOVIEMBRE DE 2008  
**I. Disposiciones generales (BOE)**  
**MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACION**

- Acuerdo de Cooperación entre el Reino de España y la República Portuguesa en el ámbito del turismo, hecho en Madrid el 25 de noviembre de 2006. (BOE n.º 281, de 21 Nov. 2008, marg. 18820) [LA LEY 18897/2008] (BOE)
- Resolución de 18 de noviembre de 2008, de la Dirección General del Tesoro y Política Financiera, por la que se establecen las condiciones de actuación de los Creadores de Mercado de Deuda Pública del Reino de España. (BOE n.º 281, de 21 Nov. 2008, marg. 18821) [LA LEY 16693/2008] (BOE)

**MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO**

- Resolución de 18 de noviembre de 2008, de la Subsecretaría, por la que se publica el Acuerdo de Consejo de Ministros de 14 de noviembre de 2008, por el que se modifica la normativa reguladora de los préstamos sujeta en el Plan elaborado por el Ministerio de

FUNCIONALIDAD 3

DIARIO DE NOTICIAS

Opción que ofrece las noticias más relevantes del ámbito jurídico.

Contenidos acceso libre CÓDIGOS -La Ley-  
Revista Legislación  
Diario de Noticias  
Visualizador CICERO

EL DIARIO DE NOTICIAS  
en su correo electrónico  
jurídico

20 de Noviembre de 2008

- Esquerra Republicana planteará la próxima semana en el Congreso el "primer asalto" a la "vergonzante" Ley de Memoria Histórica
- Llamazares avisa de que las causas contra el franquismo puedan acabar en tribunales extranjeros o en Estrasburgo
- La Sala de lo Penal seguirá analizando el incidente de competencia que Javier Zaragoza planteó contra Garzón
- Una asociación pide un Real Decreto que evite la inhibición de los jueces en los procesos contra el franquismo
- Divar asegura que sus convicciones religiosas "jamás"

FUNCIONALIDAD 4

VISUALIZADOR CICERO

CICERO es una herramienta diseñada para grabar, almacenar y visualizar de manera automática los juicios celebrados en las Salas de Vistas. Permite en un tiempo record, localizar cualquier sesión previamente grabada y acceder a la parte del video que interese en cada momento. Su garantía se debe a los miles de videos grabados en el Tribunal Supremo, Audiencia Nacional, Tribunales Superiores de Justicia, Audiencias Provinciales y en diferentes Juzgados de Primera Instancia.



1.4

RedAbogacía Libros

REDABOGACÍA LIBROS
DESCRIPCIÓN
<p>Librería online, a través de la cual, los titulares con certificado digital ACA podrán comprar libros especializados en títulos jurídicos, así como títulos sociales, humanidades, ciencias, informática o medicina.</p>
USUARIOS
<p>Usuarios abogados con certificado digital ACA.</p>
FUNCIONALIDADES
<p>Las funcionalidades se encuentran en la parte superior de la pantalla de inicio al servicio.</p> <ol style="list-style-type: none"> <li>1. BUSCADOR</li> <li>2. MI COMPRA</li> <li>3. INICIO</li> <li>4. MI CUENTA</li> <li>5. MIS NOVEDADES</li> <li>6. MIS PEDIDOS</li> <li>7. AYUDA</li> </ol>
VENTAJAS
<ul style="list-style-type: none"> <li>▪ Un 3% de descuento en las compras</li> <li>▪ Envío a domicilio gratuito.</li> </ul>

Accedemos a este servicio a través del enlace situado en la zona inferior de la página principal de RedAbogacía.



Pulse sobre dicho enlace y se abrirá una página como la que se muestra a continuación en la que podrá hacer búsquedas de libros de interés, registrar novedades y comprar aquellos libros que desee.



- ✓ **Recuerde** que es necesario tener la tarjeta criptográfica con su certificado ACA introducida en el lector para entrar en la zona privada de su colegio.

## FUNCIONALIDAD 1

## BUSCADOR

RedAbogacía Libros incorpora diversos sistemas de búsqueda de títulos a los que accederá desde la página principal ("**Inicio**" en el menú superior):

- **Búsqueda rápida:** introduzca alguna palabra clave de su búsqueda y pulse sobre el botón "**Buscar**", situado en la parte superior derecha de la pantalla de inicio.



Formulario de búsqueda rápida con un campo de texto y un botón "Buscar".

- **Buscador avanzado:** búsqueda selectiva por título, autor, editorial y reseña. La búsqueda por reseña amplifica enormemente la búsqueda pues examina el término a buscar en todas las reseñas de todos los libros de nuestra base de datos.

1. Pulse sobre el enlace "**buscador avanzado**", bajo la casilla para búsqueda rápida.
2. Se abrirá una ventana donde podrá introducir los parámetros de búsqueda.



**Buscador avanzado**

Rellene los campos que conozca sobre el/los libro/s que esté buscando.

AUTOR

TÍTULO

EDITORIAL

RESEÑA

**Buscar**

3. Pulse "**Buscar**", y el sistema le mostrará los resultados según los criterios introducidos.

- **Búsqueda por temas:** Agiliza la navegación por el índice de materias. Para navegar por temas, vaya a la barra de temas situada en la parte superior desde donde se le irán desplegando los distintos subtemas.



- **Búsqueda por categorías:** Podrá navegar dentro de las distintas categorías, pulsando sobre ellas en el menú izquierdo.



- **Si no lo encuentra se lo buscamos:** la librería virtual le ofrece un servicio de búsqueda personalizado en caso de no encontrar un libro concreto o sobre una materia determinada.

FUNCIONALIDAD 2

MI COMPRA

Con esta opción el abogado podrá ir agregando títulos y pagar con tarjeta de crédito o contra reembolso al finalizar su visita. RedAbogacía garantiza la confidencialidad de los datos suministrados por sus clientes y de las transacciones realizadas gracias al uso de certificado digital y de certificado de servidor seguro SSL.

Cuando encuentre el libro que le interesa pulse en enviar al carrito. En la cesta de la compra puede ir guardando todos los artículos que desee.

1. Pulse sobre el botón **"Ver más libros"**.



2. Seleccione el libro que desea comprar y el sistema le mostrará el detalle del mismo.
3. Si desea comprarlo pulse sobre el enlace **"Enviar al carrito"** que está representado con un icono en forma de carrito de la compra.
4. Cuando haya finalizado la selección de libros a comprar, pulse sobre el botón **"Pagar"** y se iniciará el proceso de pago solicitándole su certificado y los siguientes datos: dirección, tipo de pago, tipo de envío.

### FUNCIONALIDAD 3

### INICIO

**"inicio"** le permitirá volver siempre a la página principal donde podrá utilizar los buscadores o ver las últimas recomendaciones.



**FUNCIONALIDAD 4**

**MI CUENTA**

Esta opción le permite consultar o modificar todos los datos relativos a su cuenta.

**FUNCIONALIDAD 5**

**MIS NOVEDADES**

Esta opción permite recibir por email las novedades bibliográficas sobre sus materias preferidas (jurídico, ciencias sociales, humanidades, literatura, informática, ciencias, medicina o colecciones), basta con suscribirse al boletín de novedades de RedAbogacía Libros.

**FUNCIONALIDAD 6**

**MIS PEDIDOS**

Consulta del estado de sus pedidos: el abogado podrá comprobar el detalle de los pedidos realizados por fecha y estado en que se encuentran:

- **En proceso:** el pedido ha sido debidamente registrado por Tirant pero aún no ha sido procesado. Los pedidos en este estado pueden ser anulados.
- **Pagado:** el pedido ha sido procesado y cobrado por RedAbogacía Libros pero el paquete aún no ha sido recogido por la agencia de transportes/correos.
- **Enviado:** El pedido ha sido enviado y está en manos de la agencia de transportes/correos.
- **Pendiente de recibir los artículos:** el pedido ha sido procesado pero hay que esperar algunos artículos fuera de stock para poder completar el pedido.
- **Tarjeta no aceptada:** hubo algún problema a la hora de realizar el cobro a través de la pasarela de pagos y por lo tanto no pudo ser cobrado y el pedido no fue enviado.

**FUNCIONALIDAD 7**

**AYUDA**

Esta opción le mostrará como realizar las acciones principales de este servicio.

1.5

e-Mensajes

e-MENSAJES	
<b>DESCRIPCIÓN</b>	
Este servicio le ofrece la posibilidad de realizar envíos masivos de email, fax, sms y sms certificados desde su ordenador.	
<b>USUARIOS</b>	
Usuarios abogados con certificado digital ACA.	
<b>FUNCIONALIDADES</b>	
Las funcionalidades se encuentran en la parte superior de la pantalla de inicio al servicio.	
<ol style="list-style-type: none"> <li>1. ENVIAR E-MAIL</li> <li>2. ENVIAR FAX</li> <li>3. ENVIAR SMS</li> <li>4. ENVIAR SMS CERTIFICADO (BURO-SMS)</li> </ol>	
<b>VENTAJAS</b>	
<ul style="list-style-type: none"> <li>▪ El abogado podrá gestionar su libreta de direcciones y programar sus envíos de e-mail, fax, sms y sms certificados.</li> <li>▪ Ahorro de costes: con tarifas inferiores a otros operadores.</li> <li>▪ También podrá consultar los envíos que haya realizado por fecha, tipo de envío y destinatario.</li> <li>▪ Facilita el envío y gestión de comunicados masivos (email, fax, sms y sms certificados) de forma rápida y sencilla.</li> <li>▪ El abogado podrá enviar alertas, comunicar reuniones, eventos, nuevos servicios (el lanzamiento de una web), cambio de domicilio... o incluso enviar todo tipo de felicitaciones a sus clientes.</li> </ul>	

OTRAS FUNCIONALIDADES COMPLEMENTARIAS

- **Elementos enviados:** el usuario podrá consultar los mensajes enviados ordenados por fecha de envío, entre dos fechas determinadas y eliminar aquellos mensajes que desee con tan sólo pulsar en el botón “**Borrar**”.
- **Libreta de direcciones:** el usuario podrá gestionar la libreta de destinatarios: añadir un contacto, actualizarlo, exportar los contactos e importar contactos.
- **Grupos de Envío:** permite visualizar todos los grupos de envíos, los contactos pertenecientes al mismo, dando la opción de añadir y eliminar contactos.
- **Plantillas de Envío:** Las plantillas de envío son tipos de comunicados definidos por el administrador de envíos de la institución. Estas plantillas unifican la estructura HTML que tendrán los mensajes escritos por los emisores y que irán adjuntos a los sobres de envío.

En el listado de plantillas de envío aparecen las plantillas que serán utilizadas para componer los mensajes mostrando para cada una su nombre, asunto, si está publicada y su idioma.

- **Configuración:** Opción que trata la configuración de los archivos adjuntos: ruta absoluta, ruta relativa, tamaño máximo, tiempo de vida, tamaño máximo de las marcas de agua.
- **Informes:** muestra el listado de mensajes enviados de cada colegio. Aparecerán los campos colegio, envíos, correos enviados y el total. Estos resultados se pueden filtrar con un buscador mediante la fecha de inicio, fecha de fin y la institución.
- **Manual de usuario:** Proporciona el acceso a la descarga del manual de usuario de la aplicación.

Si desea conocer en profundidad alguna de las funcionalidades complementarias anteriores, le invitamos a que se descargue el manual de usuario y consulte el apartado 3 que trata sobre módulos funcionales.

Durante las opciones del servicio e-Mensajes visualizará una serie de iconos que pasaremos a explicar a continuación:

-  Podrá adjuntar ficheros.
-  Podrá importar contactos desde un fichero CSV o XLS.
-  Podrá visualizar la vista previa del correo.
-  Podrá enviar el mensaje.
-  Podrá borrar del formulario todos los datos del correo.
-  Podrá programar envíos.

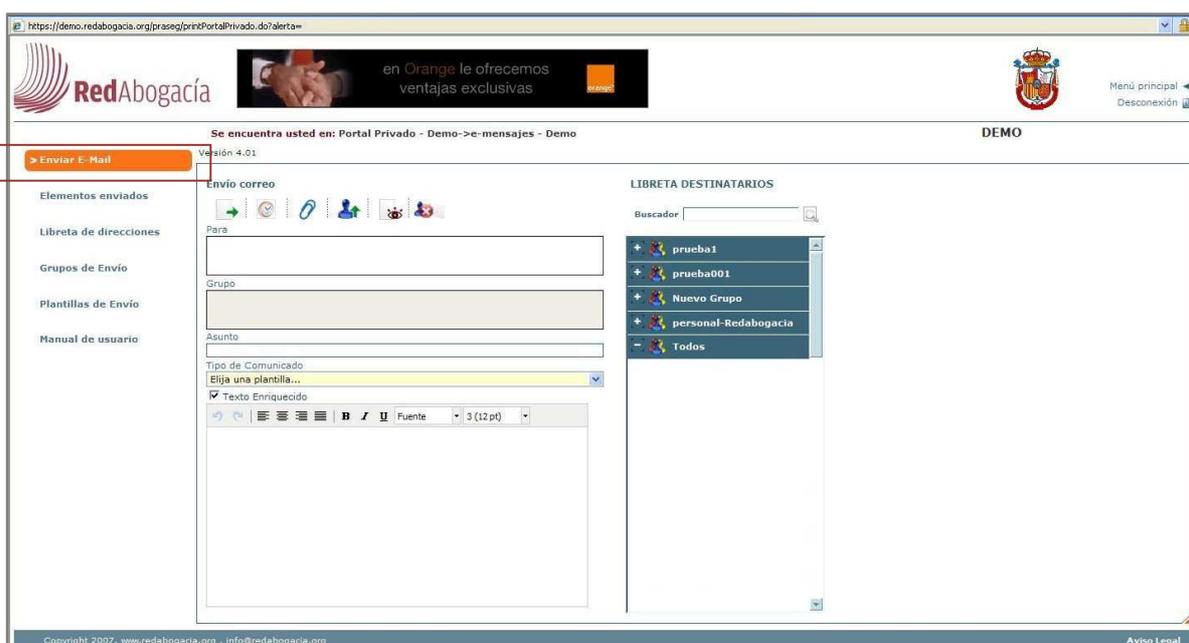
- ✓ **Recuerde** que es necesario tener la tarjeta criptográfica con su certificado ACA introducida en el lector para entrar en la zona privada de su colegio.

FUNCIONALIDAD 1

ENVIAR E-MAIL

Los pasos que deberá seguir para enviar un e-mail son:

- 1. Creación de un nuevo mensaje:** redacte el texto del nuevo mensaje con su asunto o título. También puede adjuntar archivos.
- 2. Elección de los destinatarios:** Seleccionar los distintos destinatarios o grupos de dos formas posibles:
  - Escribiendo la dirección de email directamente.
  - Consulta en la libreta personal de destinatarios: esta libreta, previamente creada por el usuario, muestra todos sus contactos: nombre y dirección de correo.
- 3. Enviar:** Una vez redactado el mensaje y elegidos los destinatarios podrá seleccionar vista previa y/o enviar directamente.

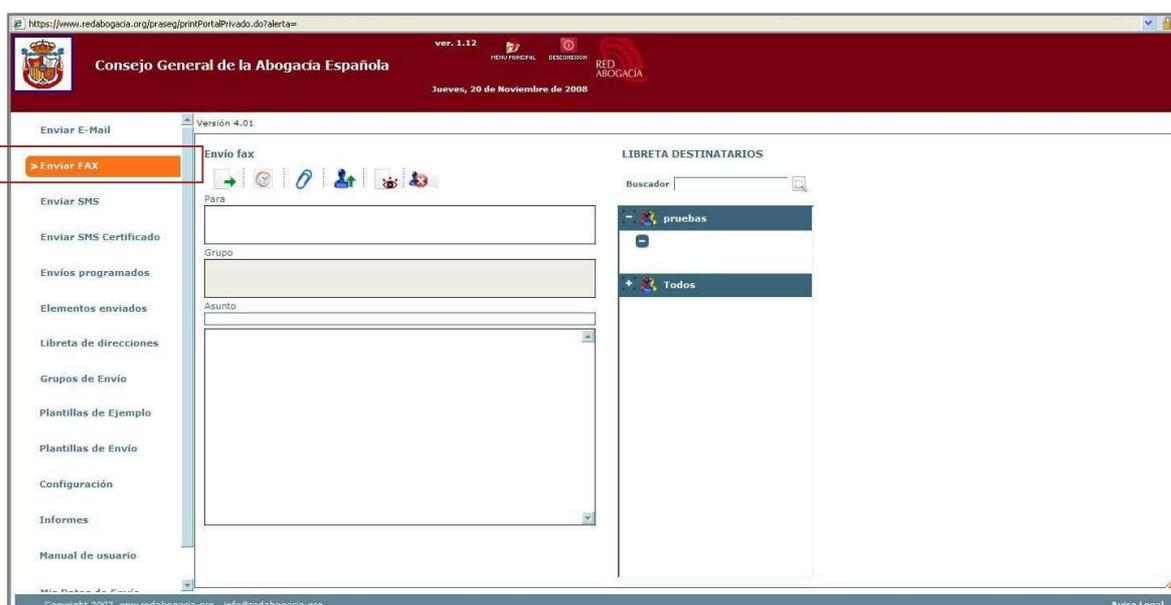


FUNCIONALIDAD 2

ENVIAR UN FAX

Los pasos que deberá seguir para enviar un fax son:

1. **Creación de un nuevo mensaje de fax:** redactar el texto del nuevo mensaje (no es obligatorio) con su asunto o título (es obligatorio). También puede adjuntar archivos.
2. **Elección de los destinatarios:** seleccionar los distintos destinatarios o grupos de dos formas posibles:
  - Escribiendo el número de fax directamente.
  - Consulta en la libreta personal de destinatarios: esta libreta, previamente creada por el usuario, muestra todos sus contactos: nombre y fax.
3. **Enviar:** Una vez redactado el fax y elegidos los destinatarios podrá seleccionar vista previa y/o enviar directamente.

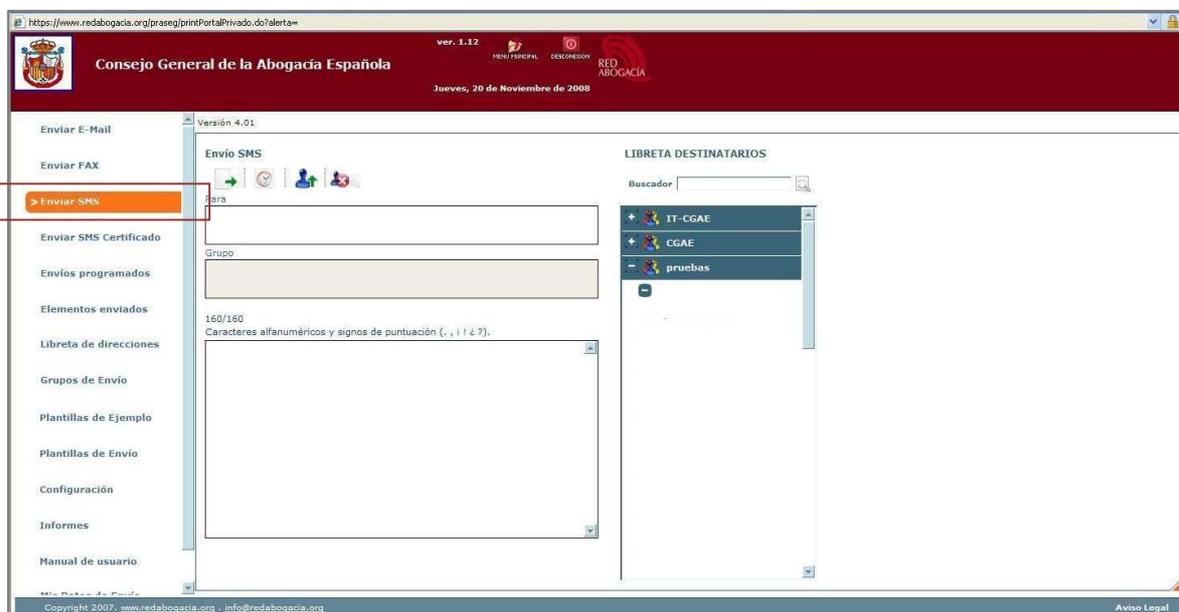


FUNCIONALIDAD 3

ENVIAR UN SMS

Los pasos que deberá seguir para utilizar el servicios de sms son:

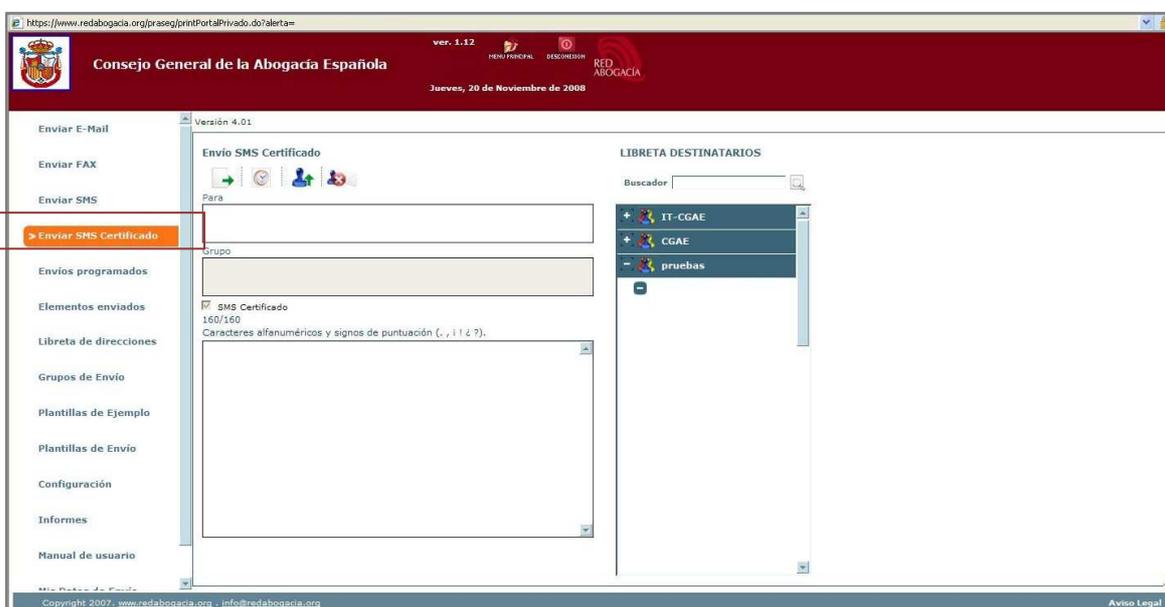
1. **Creación de un nuevo mensaje de sms:** redactar el texto del nuevo mensaje.
2. **Elección de los destinatarios:** seleccionar los distintos destinatarios o grupos de dos formas posibles:
  - Escribiendo el número de teléfono directamente.
  - Consulta en la libreta personal de destinatarios: esta libreta, previamente creada por el usuario, muestra todos sus contactos: nombre y teléfono.
3. **Enviar:** Una vez redactado el sms y elegidos los destinatarios estará listo para enviarse.



FUNCIONALIDAD 4

ENVIAR UN SMS CERTIFICADO

Los pasos que deberá seguir para utilizar el servicios de sms certificado son los mismos que si usara el servicio de sms normal, pero recibirá un pdf que certifica el día, hora de envío y texto del sms. Es un documento que se firma digitalmente.



1.6

Oficina postal

OFICINA POSTAL	
<b>DESCRIPCIÓN</b>	Este servicio proporciona acceso a los servicios de Correos y telégrafos por Internet, permitiendo enviar Telegramas, Cartas e incluso Burofaxes utilizando el carné con certificado ACA
<b>USUARIOS</b>	Usuarios abogados con certificado digital ACA.
<b>FUNCIONALIDADES</b>	<p>Las funcionalidades se encuentran en la parte superior de la pantalla de inicio al servicio.</p> <ol style="list-style-type: none"> <li>1. CORREO DIGITAL</li> <li>2. IDENTIFICACIÓN DE CERTIFICADOS</li> <li>3. TELEGRAMAS</li> <li>4. FILATELIA</li> <li>5. BUROFAX</li> <li>6. MODIFICACIÓN DE DATOS</li> </ol>
<b>MÁS INFORMACIÓN</b>	Para tener acceso a estos servicios, el usuario debe registrarse en el sistema de Correos online (para obtener una información más detallado consulte el manual de usuario que puede descargarse desde el menú del lateral izquierdo y lea atentamente el apartado 3). Una vez esté registrado correctamente aparecerán en su menú izquierdo las 6 opciones anteriores.

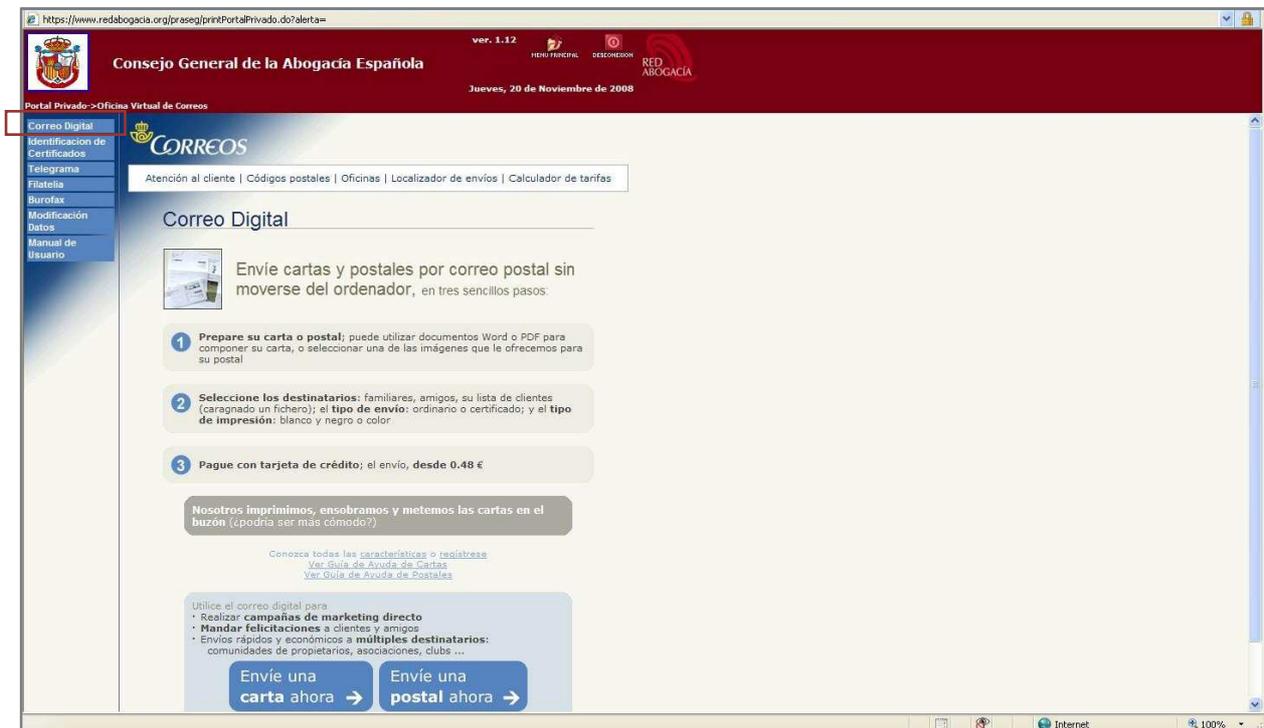
- ✓ **Recuerde** que es necesario tener la tarjeta criptográfica con su certificado ACA introducida en el lector para entrar en la zona privada de su colegio.

FUNCIONALIDAD 1

CORREO DIGITAL

Esta opción permite el envío de cartas y postales por Internet que Correos imprime, ensobra y envía, en solo tres pasos:

1. Configure la carta directamente o desde documentos Word o PDF.
2. Seleccione los destinatarios, el tipo de envío y el tipo de impresión preferidos (color o blanco y negro).
3. Pague con tarjeta de crédito por Internet desde 0,48€.



FUNCIONALIDAD 2

IDENTIFICACIÓN DE CERTIFICADOS

Estar opción facilita el envío de certificados a grupos de destinatarios por parte de las empresas, siguiendo estos pasos:

1. Dé de alta al conjunto de destinatarios de forma manual o cargando un fichero con sus direcciones, e indicando si se desea aviso de recibo o reembolso.
2. Pague directamente a través de Internet, utilizando el servicio de Franqueo electrónico de Correos online, o en las oficinas de Correos al realizar su admisión.
3. Pague directamente desde el propio ordenador las etiquetas o sobres que identifican los certificados, así como la relación de envíos.

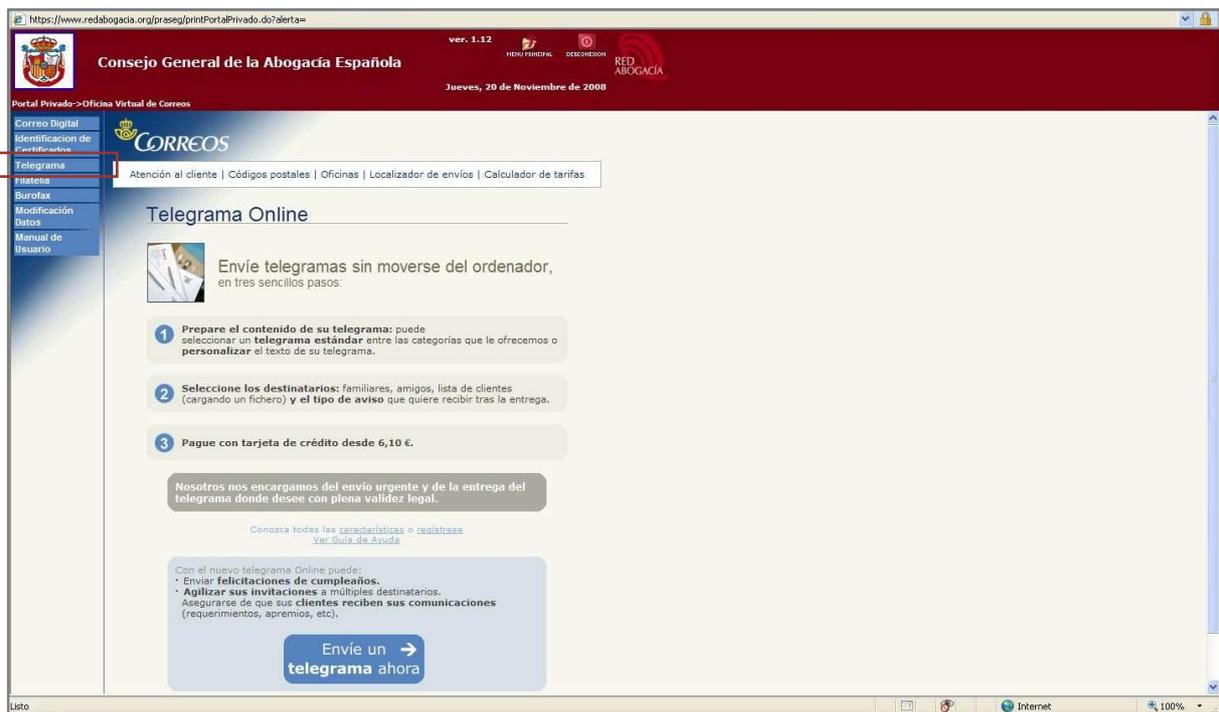


FUNCIONALIDAD 3

TELEGRAMAS

Se ofrecen plantillas de contenido por temas. El abogado podrá:

1. Seleccionar un contenido estándar entre las categorías disponibles o personalizar el texto de su telegrama.
2. Elegir destinatarios: Familiares, amigos, lista de clientes... y el tipo de aviso que quiere recibir tras la entrega.
3. Pagar con tarjeta de crédito desde 7,28 €.



FUNCIONALIDAD 4

FILATELIA ONLINE

El abogado podrá tramitar su alta como abonado, recibiendo en su domicilio todas las novedades filatélicas que se produzcan en las opciones de abono elegidas. También tendrá opción a adquirir cualquier producto que desee del catálogo filatélico de Correos que le será enviado a domicilio.



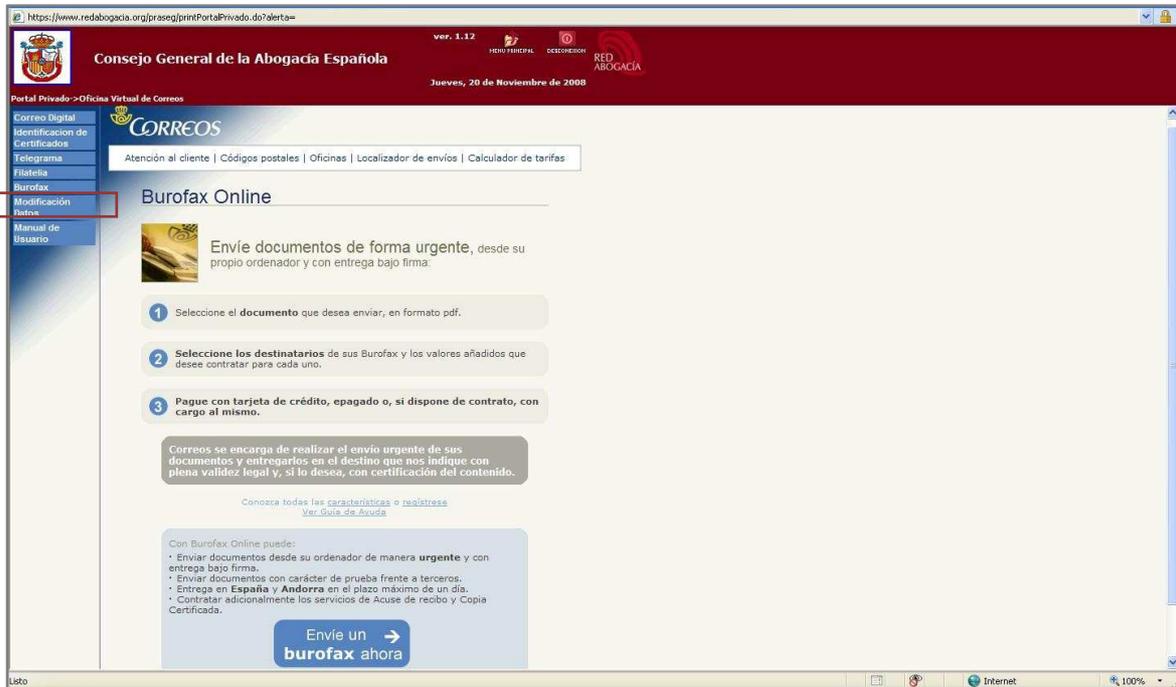
FUNCIONALIDAD 5

BUROFAX

Esta opción permite el envío de documentos de forma urgente, desde el propio ordenador y con entrega bajo firma. Correos se encarga de realizar el envío urgente de los documentos y entregarlos en destino con plena validez legal y certificación del contenido opcional.

Para utilizar este servicio son necesarios sólo tres pasos:

1. Seleccionar el documento que desea enviar, en formato PDF.
2. Elegir los destinatarios de los Burofax y los valores añadidos que desee contratar para cada uno.
3. Pagar con tarjeta de crédito, o si dispone de contrato, con cargo al mismo.



**FUNCIONALIDAD 5**

**MODIFICACIÓN DE DATOS**

Desde esta funcionalidad podrá modificar los datos de dirección que inicialmente se introdujeron al darse de alta en el sistema de Correos Online. Para ello hay que hacer clic sobre esta opción de menú **“Modificación Datos”** y le aparecerá el formulario de modificación a completar.

1.7

Oficina de catastro

OFICINA DE CATASTRO	
<b>DESCRIPCIÓN</b>	Este servicio proporciona una Conexión con Catastro para realizar Consultas y Certificaciones de bienes inmuebles.
<b>USUARIOS</b>	Dos tipos de usuarios: usuarios titulares catastrales con certificación electrónica y usuarios con acceso libre.
<b>FUNCIONALIDADES</b>	Las funcionalidades dependen del tipo de usuario.
<b>VENTAJAS</b>	Para hacer uso de este servicio es necesario que acceda a la zona privada del portal de RedAbogacía. Se visualizará una pantalla de bienvenida al servicio. Pulse sobre el enlace <b>“Información Titular Catastral”</b> , la aplicación le redirigirá a la oficina virtual del catastro y en función de si dispone de certificado digital ACA o no las funcionalidades que podrá efectuar en la oficina serán distintas. (Se explican a continuación de manera más detallada).

La Oficina Virtual del Catastro proporciona los siguientes servicios catastrales a los diferentes usuarios de los mismos:

USUARIOS TITULARES CATASTRALES CON CERTIFICACIÓN ELECTRÓNICA

Este servicio le permitirá la consulta de datos y obtención de certificados catastrales electrónicos: los titulares catastrales podrán consultar los datos catastrales de los bienes inmuebles de su titularidad que estén incorporados a la Base de Datos Nacional del Catastro y obtener certificados catastrales electrónicos. Los certificados catastrales electrónicos tienen la misma validez que los expedidos por los órganos competentes del Catastro en papel con la firma manuscrita. Existen varias opciones:

The screenshot shows the RedAbogacía website interface. At the top, there is a banner for 'en Orange le ofrecemos ventajas exclusivas' with the Orange logo. Below this, the navigation bar includes 'Menú principal' and 'Desconexión'. The main content area is titled 'Oficina Virtual del Catastro' and displays the path: 'Se encuentra usted en: Portal Privado - Demo->Oficina del Catastro->Información DEMO'. The main menu includes 'Inicio', 'Consulta Titular Catastral', and 'ASOC PARA EL DESARROLLO TURISTICO Y CULTURAL LA ZARANDILLA'. The 'Consulta del Titular Catastral' section is expanded, showing a list of options: 'Consulta y Certificación de Bienes Inmuebles del titular', 'Consulta y Certificación de Bien Inmueble. Cartografía', 'Visualizar certificaciones solicitadas sobre Bienes del Titular', 'Modificar el estado de las certificaciones solicitadas por el Titular', and 'Consulta masiva'. The 'Consulta masiva' option has sub-items: 'Enviar consulta masiva al Catastro', 'Descargar resultados de consulta masiva al Catastro', and 'Información Servicio de consulta masiva'. A 'Volver' button is located at the bottom of the list.

- Certificado de todos los bienes del titular (o bien de la circunstancia de no ser titular).
- Certificado de un bien inmueble.
- Gestión de certificaciones obtenidas por los titulares: Este servicio permite al titular catastral activar o desactivar los certificados catastrales que haya obtenido con anterioridad. Si se opta por desactivar un certificado obtenido previamente, no podrá ser comprobada por terceros ni la integridad de su contenido, ni su autenticidad, por lo que perderá su validez legal.
- Acceso a consultas y certificados electrónicos realizados por terceros: Mediante este servicio cada titular catastral podrá conocer, en todo momento, los accesos electrónicos a los datos protegidos de los bienes inmuebles de su titularidad realizados por los usuarios registrados autorizados por la Dirección General del Catastro.
- Acceso al registro de la Agencia Estatal de la Administración Tributaria, para fomentar el uso de las comunicaciones electrónicas con certificado digital en la mayoría de sus relaciones con los sujetos obligados. Este acceso facilita la presentación telemática por Internet de

autoliquidaciones y declaraciones resumen a partir del mes de Octubre de 2008 a los obligados tributarios con la siguiente forma jurídica: Sociedad Anónima (S.A) y Sociedad de Responsabilidad Limitada (S.R.L).

### USUARIOS CON ACCESO LIBRE

Cualquier persona tiene acceso libre a los siguientes servicios no protegidos como:

- Comprobación de certificados catastrales electrónicos: Cualquier persona podrá realizar la comprobación de la autenticidad e integridad de un certificado catastral electrónico, siempre que disponga de una copia del mismo o del código electrónico de verificación, salvo que haya sido desactivado por quien lo emitió.
- Consulta de datos catastrales no protegidos: Se podrán consultar libremente los datos catastrales no protegidos (incluida la cartografía catastral) incorporados a la Base de Datos Nacional del Catastro, es decir, los que no hacen referencia al titular y valor catastral.

### RECOMENDACIONES DE SEGURIDAD

Todas las comunicaciones que se realizan con el servidor de la Oficina Virtual del Catastro son cifradas. Por tanto los datos intercambiados en ambos sentidos (usuario y contraseña y datos catastrales) no pueden ser interceptados por terceros.

Algunas recomendaciones de seguridad en el uso de la aplicación:

- Cuando esté accediendo a la aplicación en modo personalizado (bien como usuario registrado o como titular) y se ausente de su puesto de trabajo, cierre el navegador con el que está trabajando o bloquee la pantalla de su ordenador con una contraseña.
- Algunos navegadores proporcionan la posibilidad de recordar la pareja usuario/contraseña en posteriores accesos. No utilice esta opción.
- Si accede desde su puesto de trabajo o un lugar público, no deje instalado su certificado en su ordenador personal. Si lo hace, proteja su acceso mediante contraseña.

Puntos Clave



**BUROMAIL\_** Servicio que permite realizar la tramitación certificada de documentos a través de correo electrónico con otros usuarios de Certificado ACA.

FUNCIÓN PRINCIPAL\_NUEVO BUROMAIL



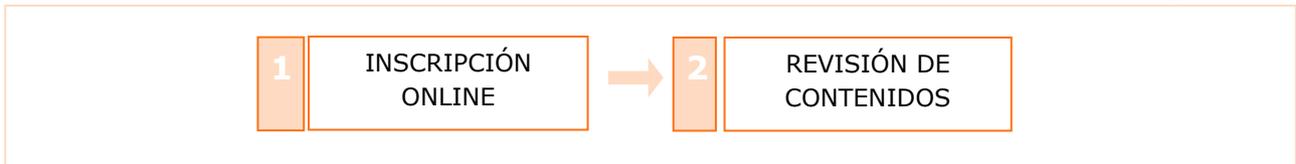
OTRAS FUNCIONALIDADES

Libreta destinatarios | Carpetas | Preferencias | Configuración de alertas | Manual de usuario | Desconectar



**CAMPUS VIRTUAL\_** Plataforma de e-learning que ofrece contenidos formativos con la posibilidad de examinarse para posteriormente obtener un certificado de aprovechamiento expedido por el colegio de residencia y el CGAE.

FUNCIÓN PRINCIPAL\_CURSOS



OTRAS FUNCIONALIDADES

Obtención del título | Documentos | Manual de usuario



**IURIS ET LEGIS\_** Este servicio ofrece al abogado un acceso gratuito, rápido y sencillo a bases de datos de códigos y jurisprudencia propiedad de editoriales jurídicas, sin necesidad de instalar Cds o DVDs, sin limitaciones de espacio y sin tener que desplazarse a su colegio de abogados.

FUNCIONALIDADES

Contenidos acceso libre códigos-La Ley | Revista Legislación | Diario de noticias | El Vigía de Colex-Data | Visualizador Cicero | Acceso a Colex-Data

 **REDABOGACÍA LIBROS\_** Librería online, a través de la cual, los titulares con certificado digital ACA podrán comprar libros especializados en títulos jurídicos, así como títulos sociales, humanidades, ciencias, informática o medicina.

FUNCIONALIDADES

Buscador | Mi compra | Inicio | Mi cuenta | Mis novedades | Mis pedidos | Ayuda

 **e-MENSAJES\_** Este servicio le ofrece la posibilidad de realizar envíos masivos de email, fax, sms y sms certificados desde su ordenador.

FUNCIONALIDADES

Enviar e-mail | Enviar fax | Enviar sms | Enviar sms certificado

Todas estas funcionalidades tienen el mismo patrón:



 **OFICINA POSTAL\_** Este servicio proporciona acceso a los servicios de Correos y telégrafos por Internet, utilizando el certificado digital.

FUNCIONALIDADES

Correo digital | Identificación de certificados | Telegramas | Filatelia | Burofax | Modificación de datos

 **OFICINA CATASTRO\_** Este servicio proporciona una Conexión con Catastro para realizar Consultas y Certificaciones de bienes inmuebles.

## 2

## SERVICIOS DE LAS ADMINISTRACIONES PÚBLICAS

La Administración Pública ofrece muchos servicios electrónicos a los abogados tanto a nivel estatal como local y regional. Resumiremos en este capítulo las funciones digitales principales de cada Administración.

## 2.1

## Servicios de las AAPP estatales

- **Agencia Española de Protección de Datos:** permite el registro de sus ficheros de acuerdo a la obligatoriedad dispuesta por la LOPD.
- **Agencia Tributaria:** desde la Oficina Virtual de Hacienda puede presentar declaraciones y consultas tributarias en nombre propio y/o de terceros.
- **Dirección General del Catastro:** puede consultar datos relativos a los bienes inmuebles a través de la referencia catastral.
- **Instituto Nacional de Empleo:** desde la Oficina Virtual del INEM puede consultar y obtener certificaciones de vida laboral.
- **Ministerio de Administraciones Públicas:** con el certificado digital se puede solicitar al Ministerio de Administraciones Públicas la creación de una dirección única de comunicación por parte de los Organismos públicos.
- **Ministerio de Fomento:** la oficina virtual permite el pago de tasas por Internet y un registro para la gestión electrónica de recursos, reclamaciones previas a la vía civil y procedimientos de revisión de actos administrativos de Ministerio de Fomento.
- **Ministerio de Industria:** la oficina virtual del Ministerio de Industria, Turismo y Comercio permite la presentación de ayudas, subvenciones y permisos, solicitudes de empleo, solicitudes relacionadas con el comercio exterior, recursos, reclamaciones y consultas.
- **Oficina de Patentes y Marcas:** permite realizar solicitudes de marcas o patentes.

## 2.2

## Servicios de las AAPP autonómicas

- **Agencia Española de Protección de Datos:** permite el registro de sus ficheros de acuerdo a la obligatoriedad dispuesta por la LOPD
- **Xunta de Galicia :**
  - Registro Telemático de la Xunta de Galicia. Tramitación electrónica.
  - Servicio de envío de anuncios al Diario Oficial de Galicia.
  - Licitación electrónica. Presentación de ofertas y consulta de situación.
  - Consulta de expedientes iniciados en la Xunta de Galicia.
  - Consulta del registro de contratistas de la Xunta de Galicia.
  - Oficinas virtuales del ámbito de Economía y Hacienda.
  - Acceso electrónico a los expedientes derivados del turno de oficio.
- **Principado de Asturias:**
  - Gestión de tributos del Principado de Asturias.
  - Notificaciones a la Administración.
  - Presentación de recursos administrativos.
  - Obtención de duplicados de expedientes.
  - Denuncias por infracciones administrativas.
  - Gestión de trámites tales como Licencias de caza y pesca, etc.
- **Junta de Extremadura :**
  - Solicitud de Reclamación por Responsabilidad Patrimonial.
  - Escrito de interposición de Recurso de Alzada.
  - Escrito de interposición de Recurso de Reposición.
  - Solicitud de Reconocimiento de Compatibilidad para segunda actividad, pública o privada.
  - Solicitud de participación en Pruebas de Acceso a la Función Pública de Extremadura.
  - Solicitud de participación en Pruebas Selectivas para la Constitución de Listas de Espera en la Función Pública de Extremadura.
  - Solicitud de Autorización de Obras Contiguas a Carreteras de Titularidad Autonómica.
  - Solicitud de Participación en la Olimpiada Matemática.
  - Solicitud de expedición del Carnet Joven Euro<26.
  - Presentación de Reclamaciones y Sugerencias relativas a la actividad sanitaria dirigidas al Defensor de los Usuarios del Sistema Sanitario Público de Extremadura.

- Solicitud de Obtención de una Segunda Opinión Médica en el Ámbito del Sistema Sanitario Público de Extremadura.
- Solicitud de Tarjeta Acreditativa de Grado de Minusvalía para personas que tengan reconocido con carácter definitivo un grado de minusvalía igual o superior al 33 por ciento.
- Solicitud de Ayudas a Corporaciones Locales para Obras del AEPSA.
- **Junta de Andalucía:**
  - Ayudas.
  - Certificados y Documentos.
  - Consultas de expedientes.
  - Impuestos.
  - Licencias y Autorizaciones.
  - Servicios de Información.
  - Trámites y Registros.
- **Gobierno de Navarra:**
  - Trámites con Hacienda.
  - Transportes.
  - Cultura.
  - Territorio.
  - Turismo.
  - Ámbito rural.
  - Formación y Educación.
  - Empleo.
  - Medio Ambiente.
  - Salud.
  - Ocio.
  - Participación Ciudadana.
  - Otros.
- **Gobierno de Cantabria:**
  - Reclamaciones y Sugerencias.
  - Demandas de Conciliación.
  - Certificado de capacitación profesional para el ejercicio de las actividades de transportista de viajeros.
  - Cantabria en Red.

- Certificado de capacitación profesional de consejero de seguridad para el transporte de mercancías peligrosas.
- Ingreso en centros de atención a primera infancia.
- **Generalitat Valenciana:**
  - Pagos y gestión de tributos.
  - Gestión de ayudas de la Administración.
  - Gestión de contratación de Becas.
  - Solicitud de certificados administrativos.
  - Conciliación laboral previa a la vía judicial (SMAC).
- **Generalitat de Cataluña:**
  - Gestión de tributos y sanciones.
  - Gestiones administrativas laborales, altas y bajas laborales, consulta de vida laboral.
  - Compraventa de valores del estado.
  - Consulta de expediente administrativos.
  - Registro y creación de empresas.
  - Gestión de avisos de comunicaciones de la Administración con el ciudadano.
- **Diputación Foral de Bizkaia:**
  - Envío de liquidaciones y autoliquidaciones.
  - Pago de tributos.
  - Solicitud de aplazamientos.
  - Solicitud de certificados.
  - Obtención de cartas de pago, totales o parciales.
  - Contestación a requerimientos.
  - Interposición de recursos de reposición con documentación asociada.
  - Presentación de consultas vinculantes.
- **Comunidad de Madrid:**
  - Presentación de solicitudes y formularios sobre procedimientos administrativos.
  - Pago de tasas y precios públicos.
  - Gestión integral de tributos sobre el juego.
  - Consultar la situación de los expedientes.
  - Consulta de situación de pagos a realizar por la Comunidad de Madrid.

## 2.3

## Servicios de las AAPP locales

- **Diputación de Badajoz:**
  - Consulta y modificación de Datos Fiscales.
  - Consulta y autogestión de Órdenes de Domiciliación.
  - Obtención de Documentos de Pago de Deudas Tributarias, y Justificantes de Pago.
  - Presentación Telemática de Documentos (Registro Telemático).
- **Ayuntamiento de Ponferrada:**
  - Acceso a los atestados judiciales de la policía.
- **Ayuntamiento de Santiago de Compostela:**
  - Registro electrónico de entrada de escritos vía correo electrónico.
- **Ayuntamiento de Alicante:**
  - Acceso a los atestados judiciales.
- **Ayuntamiento de Barcelona:**
  - Actividad económica y empleo.
  - Asuntos sociales.
  - Animales.
  - Circulación, vehículos y transportes.
  - Comercio, industria y consumo.
  - Comunicación e imagen.
  - Educación.
  - Hacienda.
  - Mantenimiento de la ciudad y el medio ambiente.
  - Población y participación ciudadana.
  - Seguridad ciudadana.
  - Territorio, urbanismo y vivienda.
  - Vía pública.

## Puntos Clave



Las Administraciones Públicas ofrecen muchos servicios electrónicos a distintos niveles:

- **NIVEL ESTATAL:** Presentación de declaraciones de la renta, certificados de vida laboral, ayudas y subvenciones, permisos, solicitud de marcas...
- **NIVEL AUTONÓMICO:** Licitaciones, ofertas, consultas, denuncias por infracciones, gestión de tributos, certificados, licencias...
- **NIVEL LOCAL:** Los ayuntamientos ofrecen servicios electrónicos de todos los ámbitos, en relación con su territorio.

## SÍNTESIS DE LA TERCERA SESIÓN

Durante esta tercera sesión se ha profundizado en los servicios electrónicos colegiales de utilidad profesional para el abogado, que le permiten desempeñar numerosas acciones dentro de su ámbito laboral.

El servicio Buromail permite al abogado realizar la tramitación certificada de documentos a través de correo electrónico con otros usuarios de Certificado ACA. La importancia de este servicio es que estos correos generan prueba con plena validez jurídica. Este servicio además permite: gestionar la libreta de destinatarios, configurar las carpetas de los correos, las preferencias y las alertas.

El servicio Campus Virtual es una plataforma e-learning que ofrece contenidos formativos con la posibilidad de examinarse para posteriormente obtener un certificado de aprovechamiento expedido por el colegio de residencia y el CGAE. Además se brinda la posibilidad de realizar un aprendizaje a distancia, según las necesidades del abogado.

El servicio Iuris et Legis ofrece al abogado un acceso gratuito, rápido y sencillo a bases de datos de códigos y jurisprudencia propiedad de editoriales jurídicas, sin necesidad de instalar Cds o DVDs, sin limitaciones de espacio y sin tener que desplazarse a su colegio de abogados.

El servicio RedAbogacía Libros actúa como una librería online, a través de la cual, los titulares con certificado digital ACA podrán comprar libros especializados en títulos jurídicos, así como títulos sociales, humanidades, ciencias, informática o medicina. Además permite hacer uso de otras funcionalidades como: acceder a las novedades, a los pedidos ya realizados a modo de consulta...

e-Mensajes es un servicio que ofrece la posibilidad de realizar envíos masivos de email, fax, sms y sms certificados desde su ordenador, además el abogado podrá gestionar su libreta de direcciones para facilitar la gestión de las comunicaciones y ahorrar costes debido a una reducción de las tarifas con respecto a otros operadores.

La Oficina Postal es un servicio que proporciona acceso a los servicios de Correos y telégrafos por Internet, permitiendo enviar Telegramas, Cartas e incluso Burofaxes, utilizando el nuevo carné.

Y por último la Oficina de Catastro proporciona una Conexión con Catastro para realizar Consultas y Certificaciones de bienes inmuebles.

Otros servicios como LexNet y Backup se expondrán en el módulo avanzado.

## AUTOEVALUACIÓN 3

**1. Los servicios que ofrece RedAbogacía pueden clasificarse en ...**

- a. Servicios de utilidad profesional y servicios con la Administración Pública
- b. Servicios colegiales y servicios de utilidad profesional
- c. Servicios colegiales y servicios con la Administración Pública

**2. Los servicios colegiales pueden a su vez subdividirse en...**

- a. Servicios de utilidad profesional y servicios de relación con el colegio de abogados
- b. Servicios de relación con el colegio de abogados y servicios con la Administración Pública
- c. Servicios autonómicos, locales y estatales

**3. Los correos electrónicos emitidos a través del servicio Buromail, ¿generan prueba con validez jurídica?**

- a. Sí
- b. No
- c. Depende de la institución a la que se dirija

**4. Indique qué funcionalidad no está disponible desde el servicio Buromail:**

- a. Configuración de alertas
- b. Enviar un sms certificado
- c. Gestionar libreta de destinatarios

**5. A través del servicio del Campus virtual usted podrá...**

- a. Buscar libros especializados en títulos jurídicos, humanidades, ciencias sociales...
- b. Realizar una compra de un libro formativo en materia jurídica
- c. Acceder a los contenidos formativos para posteriormente y obtener un certificado de aprovechamiento por el CGAE

**6. Para la obtención del título emitido por el CGAE tras la realización de un curso, es necesario seguir los pasos...**

- a. Firma de declaración de asistencia, encuesta y test evaluativo
- b. Encuesta y test evaluativo
- c. Test evaluativo y encuesta

**7. Si al redactar un email los destinatarios se escriben en el campo "Destinatarios CC"...**

- a. No se garantizan ni el envío ni la recepción del mensaje
- b. Se garantiza la recepción del mensaje mediante la firma digital, pero no el envío
- c. Se garantiza el envío del mensaje mediante la firma digital, pero no la recepción

**8. El servicio Iuris et Legis permite...**

- a. Acceso a bases de datos del Ministerio de Justicia
- b. Acceso gratuito, rápido y sencillo a bases de datos de códigos y jurisprudencia propiedad de editoriales jurídicas
- c. Acceso gratuito a códigos y jurisprudencia, todos ellos propiedad del colegio de abogados al que pertenezca

**9. RedAbogacía Libros es ...**

- a. Una librería online
- b. Una biblioteca online
- c. Un campus virtual de consulta de libros jurídicos

**10. ¿El servicio RedAbogacía libros ofrece al abogado alguna ventaja económica?**

- a. Sí
- b. No
- c. Depende del libro que quiera

**11. El servicio RedAbogacía Libros dispone de un buscador con el que puede realizar...**

- a. Búsquedas rápidas, avanzadas y por temas
- b. Búsquedas rápidas y avanzadas
- c. Búsqueda avanzada y por temas

**12. El servicio e-Mensajes permite...**

- a. Enviar e-mail, sms, y sms certificados
- b. Enviar e-mail, sms certificados, sms y faxes
- c. Enviar e-mail, sms certificados y faxes

**13. El servicio de Oficina postal proporciona...**

- a. Acceso a los servicios de Correos y telégrafos
- b. Acceso a los servicios de correos y telégrafos por Internet, permitiendo enviar telegramas, cartas e incluso sms certificados
- c. Acceso a los servicios de correos, permitiendo enviar telegramas, cartas e incluso sms certificados

**14. Las funcionalidades del servicio de catastro dependen del...**

- a. Tipo de servicio
- b. Tipo de servicio y usuario
- c. Tipo de usuario

**15. Los servicios colegiales de relación con el colegio de abogados son:**

- a. Comunicación de intervención profesional, pases a prisión y censo de letrados
- b. Pases a prisión y comunicación de intervención
- c. Censo de letrados y pases a prisión

**Soluciones: en los anexos**

# ANEXOS

## SOLUCIONES AUTOEVALUACIÓN 1

1 b	2 a	3 a	4 a	5 c
6 c	7 a	8 c	9 b	10 a
11 c	12 b	13 c	14 a	15 a

## SOLUCIONES AUTOEVALUACIÓN 2

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

## SOLUCIONES AUTOEVALUACIÓN 3

1 c	2 a	3 a	4 b	5 c
6 a	7 c	8 b	9 a	10 a
11 a	12 b	13 a	14 c	15 a