Índice

PRIMERA SESIÓN

Regulación de las TI

1. Introducción

1.1. Presentación del módulo intermedio

En el módulo intermedio se tratará con mayor profundidad algunas de las cuestiones planteadas en el módulo básico como, por ejemplo, la regulación de las tecnologías de la información en nuestro ordenamiento o la seguridad de la información.

También se introducirán nuevos temas y se explicará con detalle una parte de los servicios telemáticos seguros para el ejercicio de la Abogacía que se prestan desde el portal RED Abogacía (http://www.redabogacia.org). El resto de los servicios se estudiarán en el módulo avanzado.

Una vez completado con éxito el módulo intermedio, el alumno obtendrá el título "Certificado de usuario avanzado de certificación electrónica".

1.2. Presentación de la 1ª sesión

Al finalizar esta sesión habrá adquirido una amplia visión de la regulación de las tecnologías de la información en nuestro ordenamiento, contemplando las siguientes materias:

- Firma electrónica.
- Servicios de la sociedad de la información.
- Protección de datos personales.
- Propiedad intelectual.
- Telecomunicaciones.

2. Régimen jurídico de las TI

2.1. 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 concurran 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:

http://www.mityc.es/DGDSI/Servicios/FirmaElectronica/Prestadores/

- 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 siguientes 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 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

1.º 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.

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

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

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

5.º 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.

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

7.º 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 Fé 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.»*

2.2. Práctica: verificación cumplimiento de requisitos en ACA

Duración aproximada de la práctica: 15 minutos

Contenido de la práctica. Verificar que ACA cumple con cada uno de los siguientes requisitos:

- La firma electrónica de ACA es firma electrónica reconocida: uso de dispositivo seguro de creación de firma y basada en certificado reconocido (arts. 3, 11 y 24)
- Contenido mínimo de un certificado reconocido: certificados ACA (art. 11)
- Obligaciones previas a la expedición de un certificado reconocido: explicación de la operativa de generación de certificados ACA (arts. 12 y 13)
- Obligaciones de los prestadores de servicios de certificación que emiten certificados digitales (art. 18)
- Declaración de prácticas de certificación (art. 19)
- Obligaciones de los prestadores de servicios de certificación que emiten certificados reconocidos (art. 20)
- Certificación de prestadores de servicios de certificación (art. 26)

2.3. 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 pr estadores 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 telemáticos.
- 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 al 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 atendrá 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 expresen 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:*
>
> *1.º La contratación de bienes o servicios por vía electrónica.*
>
> *2.º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.*
>
> *3.º La gestión de compras en la red por grupos de personas.*
>
> *4.º El envío de comunicaciones comerciales.*
>
> *5.º El suministro de información por vía telemática.*
>
> *6.º 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*
>
> *1.º Los servicios prestados por medio de telefonía vocal, fax o telex.*
>
> *2.º 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.*
>
> *3.º 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.*
>
> *4.º Los servicios de radiodifusión sonora, y*

5.º 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:

1.º 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

2.º 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 incluidos 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.»

2.4. Práctica: verificación cumplimiento de requisitos en RED Abogacía

Duración aproximada de la práctica: 15 minutos

Contenido de la práctica:

1. Comprobar en la página web wwwREDAbogacia.org el cumplimiento de la LSSICE: Restricciones a la prestación de servicios (art. 8)
2. Comprobar en la página web wwwREDAbogacia.org el cumplimiento de la LSSICE: Constancia registral del nombre de dominio (art. 9)
3. Comprobar en la página web wwwREDAbogacia.org el cumplimiento de la LSSICE: Información general (art. 10)
4. Comunicaciones comerciales por vía electrónica. Analizar el cumplimiento del deber de información (art. 20) en los supuestos facilitados al alumno.

2.5. 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 14/1999, 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 rectificados 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 negocial, 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 rectificados o cancelados, 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 rectificados o cancelados 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.

2.6. Práctica: verificación cumplimiento de requisitos en RED Abogacía

Duración aproximada de la práctica: 15 minutos

Contenido de la práctica:

1. Comprobar en la página web www.REDAbogacia.org el cumplimiento del deber de información en la recogida de datos (art. 5 LOPD).

2.7. 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.

2.8. 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 Titulo 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 arbítrales 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 arbítrales 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 aquélla 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 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, redes utilizadas para la 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.»

3. Despedida

3.1. Resumen

En esta sesión hemos recibido una amplia visión de la regulación de las tecnologías de la información en nuestro ordenamiento, contemplando las siguientes materias:

- Firma electrónica.
- Servicios de la sociedad de la información.
- Protección de datos personales.
- Propiedad intelectual.
- Telecomunicaciones.

3.2. En la próxima sesión

En la próxima sesión se tratarán los siguientes temas:

- Aproximación a la seguridad de la información.
- Problemas de seguridad que plantea el uso de las herramientas informáticas.
- Herramientas y técnicas de seguridad.
- Declaración de Prácticas de Certificación y Políticas de Certificación de ACA

SEGUNDA SESIÓN

Seguridad y servicios telemáticos

1. Introducción

1.1. Recordatorio de la 1ª sesión

En la sesión anterior se ofreció una amplia visión de la regulación de las tecnologías de la información en nuestro ordenamiento, contemplando las siguientes materias:

- Firma electrónica.
- Servicios de la sociedad de la información.
- Protección de datos personales.
- Propiedad intelectual.
- Telecomunicaciones.

1.2. Presentación de la 2ª sesión

Al finalizar esta sesión habrá adquirido los siguientes conocimientos:

- Aproximación a la seguridad de la información.
- Problemas de seguridad que plantea el uso de las herramientas informáticas.
- Herramientas y técnicas de seguridad.
- Declaración de Prácticas de Certificación y Políticas de Certificación de ACA.

2. Seguridad de la información

2.1. Concepto y aproximación a la seguridad de la información

Desde el punto de vista del usuario de los servicios telemáticos que venimos considerando, la seguridad de la información se concreta en las tres siguientes vertientes:

- **Integridad:** la información es segura si no ha sido alterada en el proceso de transmisión:
- **Confidencialidad:** la información sólo es accesible por el poseedor del certificado y la persona con quien interactúa.
- **Autenticación:** El emisor de la comunicación es quien dice ser. Dada la naturaleza cliente-servidor de los servicios telemáticos considerados, la autenticación es tanto de cliente como de servidor. El modo de autenticación es esencialmente el mismo, si bien en un caso se autentica a una máquina (servidor) y en el otro a una persona física (cliente).

Existe otra vertiente de la seguridad, la **disponibilidad**, si bien en el caso de los servicios telemáticos considerados recae sobre la plataforma de prestación de los servicios: RED Abogacía.

RED Abogacía 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.

3. Problemas de seguridad que se plantean en el uso de las herramientas informáticas

3.1. Programas maliciosos

No todos los programas informáticos realizan funciones legítimas. Existen programas informáticos que realizan operaciones perjudiciales para el usuario y lo hacen sin su conocimiento ni autorización.

El ejemplo más común de este tipo de programas lo constituyen los **virus informáticos**. Se trata de programas que realizan operaciones no consentidas de forma clandestina. Tales operaciones pueden consistir en la alteración de información, el envío de mensajes de correo electrónico, la propagación del virus a otros sistemas, etc.

Otro ejemplo de programa malicioso lo constituyen los **troyanos**. Son programas informáticos que, bajo una apariencia legítima, realizan de forma clandestina y no autorizada operaciones perjudiciales para el usuario. Un virus suele destruir y/o modificar archivos en la máquina infectada, mientras que con un troyano, es el usuario el que decide si se borra algo o no.

La diferencia fundamental entre un virus y un troyano es que un virus se reproduce, sea modificando ficheros, mandándose por Internet, etc. y un troyano no, ya que se trata de causar trastornos a quien se lo manda. Por otra parte, los troyanos tienen la capacidad de ejecutar programas externos, o incluso controlar el ordenador donde se instalan para tener acceso remoto a él.

Un último ejemplo de programa malicioso sería las **bombas lógicas.** Se trata de programas que, llegada una determinada fecha o verificadas unas determinadas condiciones, realizan operaciones destructivas para el sistema informático y/o para la información que almacena.

Un reciente caso que produjo una cierta alarma social fue el de los programas que cambiaban la configuración del acceso telefónico a Internet, sustituyendo el número establecido por otro con tarificación adicional. Estos programas se denominan *dialers*.

La propagación de los programas maliciosos se produce por varias vías, fundamentalmente:

- Mediante el correo electrónico.
- A través del uso de software de origen no fiable.
- Mediante el acceso a páginas web que ejecutan código malicioso.

3.2. Interceptación de comunicaciones

Cuando enviamos información a través de una red de ordenadores, la información se divide en pequeños trozos llamados paquetes. Los paquetes son enviados a su destino y para llegar a él pueden seguir varias rutas (siempre que la topología de red lo permita.), en función de parámetros tales como la saturación de determinados nodos de la red. No todos los paquetes siguen la misma ruta. En el caso de Internet, resulta muy difícil conocer la ruta exacta que seguirán, por ejemplo, los paquetes que componen un mensaje de correo electrónico.

Si tenemos el control de un nodo de la red por el que pasen los paquetes, podemos interceptarlos, no retransmitirlos y, en su lugar, transmitir otros paquetes falsificados (con una información distinta). Este tipo de ataques es difícil de detectar.

Una vez que todos los paquetes han llegado al destino, la información se recompone.

Si tenemos el control de un nodo por el cual pasen los paquetes podremos interceptarlos, vulnerando de este modo la confidencialidad de la comunicación.

3.3. Suplantación de identidad

Caben varias posibilidades de suplantación de identidad, siendo las más importantes las siguientes:

- Utilización de un remite falso en un mensaje de correo electrónico. Este fraude resulta muy fácil de cometer, aunque también es fácil de detectar.
- Utilización de un usuario y contraseña (datos de autenticación) ajenos. En este caso el titular de los datos de autenticación puede haber faltado a un deber de custodia diligente de esos datos.

3.4. Acceso ilícito a sistemas

El acceso ilícito a sistemas puede tener varios orígenes:

- Una suplantación de identidad, mediante el uso de datos de autenticación ajenos.
- La conexión a un programa que se ejecute legítimamente en el sistema.
- Un troyano que abra una puerta en nuestro sistema.

3.5. Robos de información

Los sistemas informáticos corporativos almacenan datos de gran interés para la competencia. No obstante, los sistemas personales también pueden resultar un objetivo atractivo, por cuanto contienen datos potencialmente útiles para el ladrón de información: números de cuentas bancarias, contraseñas, información personal y profesional, etc.

El robo de la información puede venir propiciado por:

- El acceso ilegítimo al sistema que la almacena.
- El empleo de un programa malicioso que, sin el conocimiento del usuario, accede a determinada información y la comunica a otro sistema informático o la envía por correo electrónico.
- La obtención de la información mediante engaño.

Un ejemplo de robo de información mediante el empleo de engaño, en este caso mediante suplantación de identidad, es el del *phishing*. Consiste en el envío de mensajes fraudulentos que simulan provenir de una entidad financiera y que solicitan al destinatario que acceda a una determinada página web (una maqueta con la apariencia de la página web de la entidad financiera) e introduzca allí sus datos de autenticación (usuario y contraseña). De este modo, el ladrón de información podrá suplantar la identidad de la víctima para acceder a la entidad financiera.

3.6. Recepción de correo publicitario no deseado

El correo no deseado se denomina ***spam***. Desafortunadamente, hoy en día es frecuente recibir mensajes no solicitados y de contenido publicitario o, en algunos casos, fraudulento. El *spam* se caracteriza porque frecuentemente se intenta ocultar el verdadero remitente del mensaje y porque se trata de mensajes enviados masivamente.

La recepción del mensaje se puede deber a una deficiente configuración de un servidor de correo y/o a que nuestra dirección de correo se encuentre en una base de datos empleada por el remitente del *spam*.

3.7. Denegación de servicio

La denegación de servicio se produce cuando se saturan los recursos de un sistema informático, de modo que éste ya no puede realizar las funciones encomendadas.

Estos recursos podrán ser:

- Capacidad de proceso.
- Memoria.
- Medios de almacenamiento.
- Capacidad de establecer nuevas conexiones de red.

Lo habitual es que se obtenga la saturación de un sistema informático mediante el ataque simultáneo desde varios otros. Estos ataques pueden ser realizados sin el conocimiento del dueño del sistema en caso de realizarse mediante un troyano.

Muchos sitios de internet han sido víctimas de ataques de denegación de servicio, entre otros, Yahoo, eBay y CNN.

4. Herramientas destinadas a solventar estos problemas

4.1. Formación de los usuarios

La formación de los usuarios permite evitar aquellos problemas de seguridad debidos al desconocimiento o al incorrecto uso de las herramientas informáticas.

4.2. Seguridad física

Empleando medidas físicas podemos evitar que personas no autorizadas manipulen los equipos informáticos.

4.3. Cifrado

El cifrado con certificado digital nos permite salvaguardar la confidencialidad de la información, aún en el caso de que ésta sea robada.

Mediante el cifrado transformamos la información de modo que ésta resulta ininteligible. Para devolver la información a su estado original (inteligible) es necesario realizar la transformación inversa, denominada descifrado.

Existen dos tipos de sistemas de cifrado:

- **Simétricos.** Se caracterizan porque la operación de descifrado es idéntica a la operación de cifrado. Emplean una sola clave.
- **Asimétricos o de clave pública.** Se caracterizan por el empleo de un par de claves: clave pública y clave privada. Ambas claves se encuentran relacionadas y resultan complementarias. Los algoritmos de clave pública emplean una clave para cifrar y la complementaria para descifrar. La clave pública se puede distribuir libremente, pero la clave privada ha de mantenerse en la más estricta confidencialidad.

4.4. Autenticación

La autenticación nos permite evitar la suplantación de identidad y algunas modalidades de acceso ilícito a sistemas.

La autenticación consiste en:

1. la identificación del usuario
2. la posterior comprobación de la autorización de acceso del usuario.

Existen diversas tecnologías que permiten la autenticación. La más extendida es la utilización de usuarios y contraseñas. Una de las tecnologías de autenticación más seguras existentes hoy en día es la basada en el uso de **certificados digitales**.

RED Abogacía ofrece un incomparable grado de seguridad en la autenticación de los usuarios, pues se basa en el uso de los certificados ACA (se trata de certificados reconocidos).

4.5. Firma electrónica

La firma electrónica nos permite garantizar la integridad de la información e impedir la suplantación de identidad del firmante.

4.6. Filtros antispam

Gracias a los filtros *antispam* podemos detectar el correo no solicitado y eliminarlo o trasladarlo a una carpeta concreta.

Los servicios de correo electrónico alojados en RED Abogacía cuentan con protección *antispam*.

4.7. Antivirus

Permiten la detección, neutralización y eliminación de programas maliciosos.

Dado que continuamente aparecen nuevos programas maliciosos, se hace necesario mantener actualizada la base de datos del antivirus.

El funcionamiento del antivirus es el siguiente: rastrea los medios de almacenamiento, la memoria RAM y los mensajes de correo electrónico en busca de conjuntos de instrucciones que respondan a un determinado patrón. Estos patrones se extraen de la

base de datos del antivirus, donde se almacena información que permite la identificación de los programas maliciosos conocidos.

4.8. Cortafuegos

Los cortafuegos evitan la realización de conexiones no deseadas a nuestro ordenador, lo cual nos protege de intrusiones en el sistema y de ataques de denegación de servicio.

También pueden frustrar los intentos de conexión a red de programas maliciosos.

4.9. Sistemas de detección de intrusiones.

Los sistemas de detección de intrusiones monitorizan las conexiones de red en busca de patrones que les permitan detectar ataques contra el sistema.

Un sistema de detección de intrusiones nos protege frente a ataques de denegación de servicio y frente a intrusiones.

Una vez detectado el ataque, procede como un cortafuegos bloqueando el intento de conexión.

4.10. Actualizaciones

Es importante mantener el software al día, con los parches y actualizaciones de seguridad instaladas.

Muchas aplicaciones cuentan con mecanismos de actualización automática.

4.11. Copias de seguridad

La realización de copias de seguridad nos permite recuperar la información en caso de desastre, ya sea éste intencionado (por ejemplo, un virus) o accidental (por ejemplo, error del usuario).

4.12. Auditoría de registros de eventos

El sistema operativo y algunas aplicaciones (especialmente, las que ofrecen servicios de red) realizan un registro de determinadas operaciones (por ejemplo, accesos a recursos, autenticación de usuarios, etc.).

Auditar estos registros nos permite:

1. Conocer el uso que se hace de la aplicación.
2. En caso de incidente de seguridad, realizar un análisis forense.
3. Detectar tendencias que, en un futuro, podrían dar lugar a problemas de seguridad.

4.13. Securización de sistemas

Se refiere a un conjunto de prácticas que comprenden las herramientas mencionadas, así como otras, y que se destinan a reforzar la seguridad de un sistema informático.

5. Correo electrónico seguro

5.1. Los certificados digitales y el correo electrónico seguro

El correo electrónico se puede hacer seguro mediante el empleo de certificados digitales, que nos permitirán firmar y cifrar los mensajes, incluyendo los archivos adjuntos.

La firma de los mensajes nos ofrece las siguientes seguridades:

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 nos aporta confidencialidad. Únicamente los destinatarios del mensaje podrán descifrarlo.

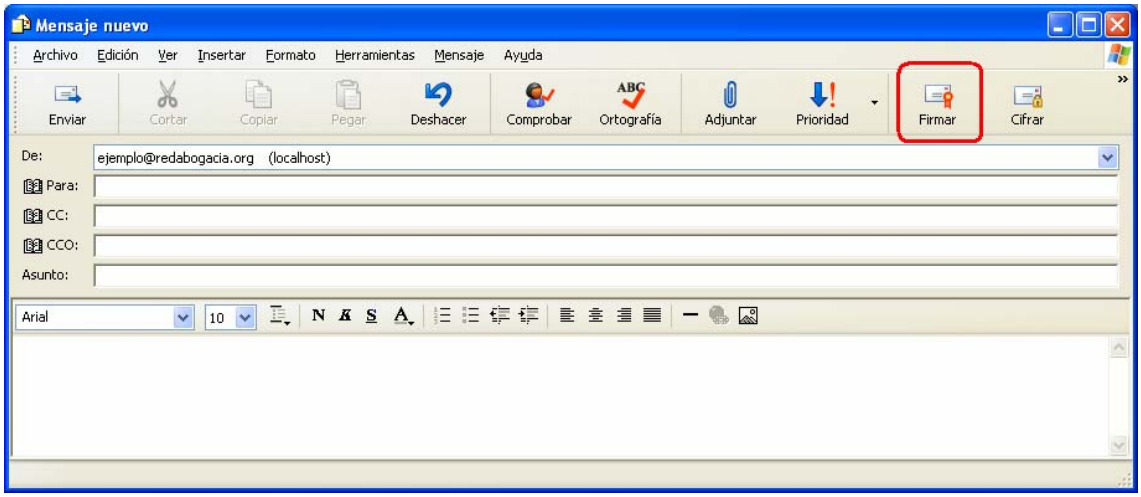
Adicionalmente, si se emplea un certificado reconocido y un dispositivo seguro de creación de firma tendremos firma electrónica reconocida y, por tanto, equivalencia de efectos con la firma manuscrita.

La firma electrónica de ACA es firma electrónica reconocida.

5.2. Firma de correo electrónico

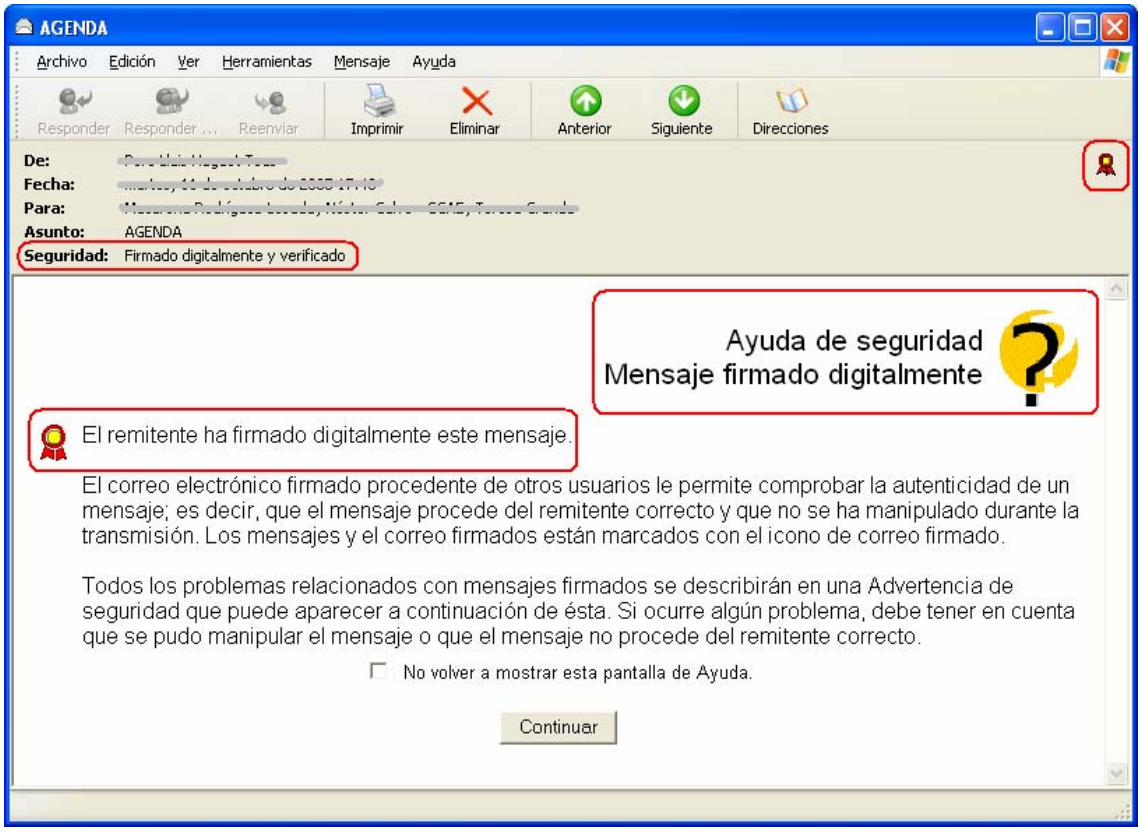
La firma y el cifrado de correo con Outlook Express y MS Outlook resultan muy sencillos.

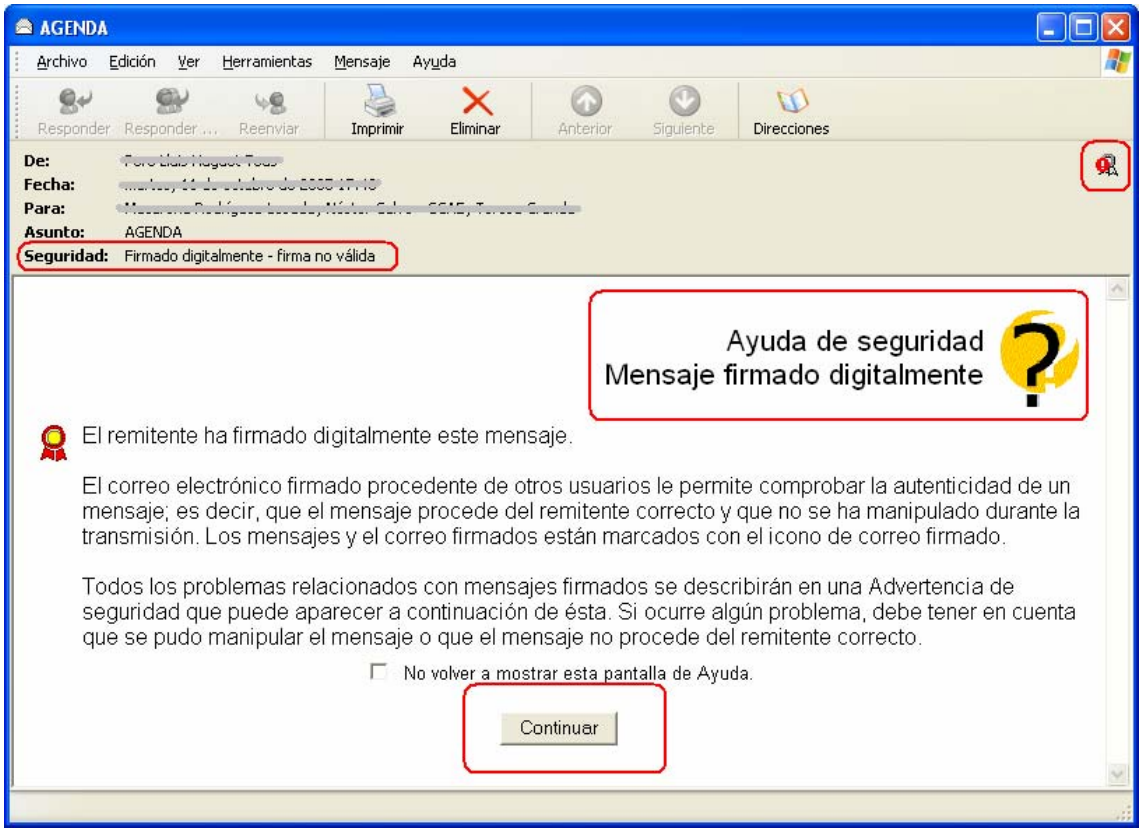
Para firmar un mensaje de correo electrónico pulsaremos el botón “Firmar” e introduciremos la tarjeta en el lector. Al pulsar el botón “Enviar”, se nos pedirá el PIN de la tarjeta para realizar la firma del correo.

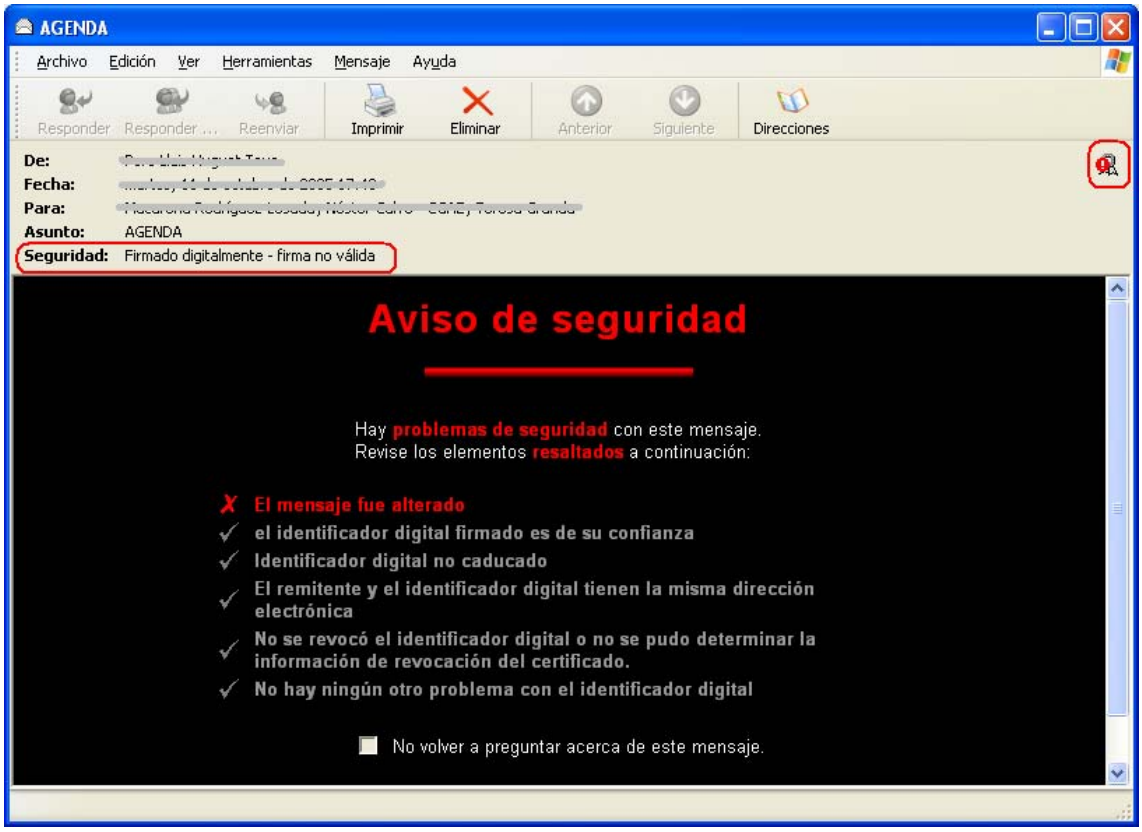


Hemos de tener presente que la cuenta de correo empleada para enviar el mensaje ha de coincidir con la incorporada en el certificado.

Outlook Express nos informará sobre la validez de la firma cuando abramos el mensaje.




AGENDA
Archivo Edición Ver Herramientas Mensaje Ayuda
Responder Responder ... Reenviar Imprimir Eliminar Anterior Siguiente Direcciones
De:
Fecha:
Para:
Asunto: AGENDA
Seguridad: Firmado digitalmente - firma no válida
Ayuda de seguridad
Mensaje firmado digitalmente
El remitente ha firmado digitalmente este mensaje.
El correo electrónico firmado procedente de otros usuarios le permite comprobar la autenticidad de un mensaje; es decir, que el mensaje procede del remitente correcto y que no se ha manipulado durante la transmisión. Los mensajes y el correo firmados están marcados con el icono de correo firmado.
Todos los problemas relacionados con mensajes firmados se describirán en una Advertencia de seguridad que puede aparecer a continuación de ésta. Si ocurre algún problema, debe tener en cuenta que se pudo manipular el mensaje o que el mensaje no procede del remitente correcto.
No volver a mostrar esta pantalla de Ayuda.
Continuar


AGENDA
Archivo Edición Ver Herramientas Mensaje Ayuda
Responder Responder ... Reenviar Imprimir Eliminar Anterior Siguiente Direcciones
De:
Fecha:
Para:
Asunto: AGENDA
Seguridad: Firmado digitalmente - firma no válida
Aviso de seguridad
Hay problemas de seguridad con este mensaje.
Revise los elementos resaltados a continuación:
El mensaje fue alterado
el identificador digital firmado es de su confianza
Identificador digital no caducado
El remitente y el identificador digital tienen la misma dirección electrónica
No se revocó el identificador digital o no se pudo determinar la información de revocación del certificado.
No hay ningún otro problema con el identificador digital
No volver a preguntar acerca de este mensaje.

5.3. Cifrado de correo electrónico

Para cifrar un mensaje pulsaremos el botón “Cifrar”. En este caso es necesario disponer de la clave pública de los destinatarios para poder realizar el cifrado.

Cuando queramos leer un mensaje cifrado que hayamos recibido, necesitaremos introducir la tarjeta en el lector y se nos pedirá el PIN para poder descifrar el mensaje.

Si no disponemos de la clave privada correspondiente, no podremos descifrar el mensaje.

6. Firma de documentos

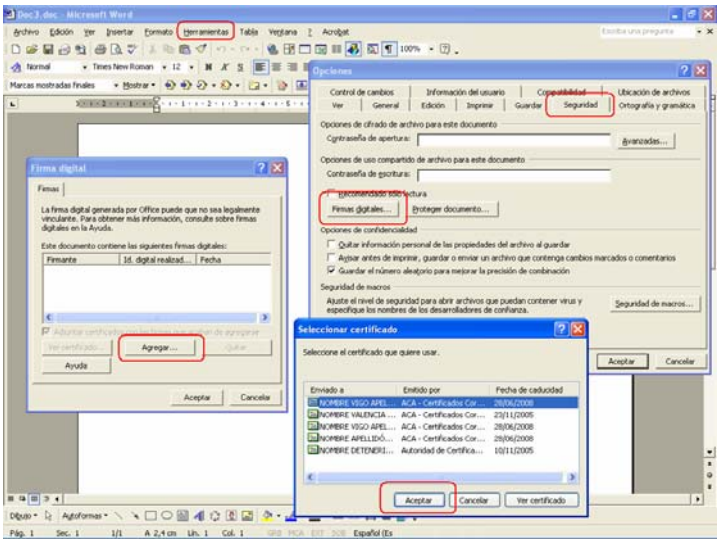
Firmar un documento con Word XP resulta muy sencillo. En primer lugar, necesitamos un documento por lo que abriremos o crearemos con Word el documento a firmar.

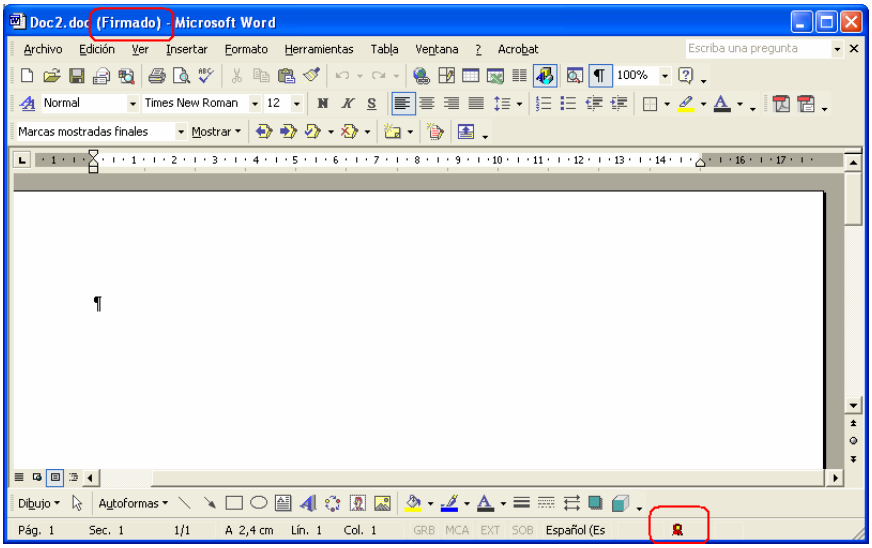
A continuación, insertamos la tarjeta en el lector y acudimos al menú desplegable: Herramientas → Opciones → Seguridad.

Pulsamos el botón “Firmas digitales”.

En la ventana obtenida pulsamos el botón “Agregar”.

Aparecerá una ventana en la que debemos elegir con qué certificado queremos firmar el documento. Una vez seleccionado el certificado e introducido el PIN de la tarjeta, se procede a la firma.





Para firmar documentos con Excel o Power Point, el procedimiento es análogo.

7. Práctica: técnicas y herramientas

7.1. Antivirus

Duración aproximada de la práctica: 10 min.

Contenido de la práctica:

1. Identificación del icono que representa el módulo residente en memoria del antivirus.
2. Acceso a la consola de administración del antivirus.
3. Análisis del sistema.
4. Análisis de un medio extraíble (CD-ROM).
5. Actualización de la base de datos de firmas del antivirus.
6. Configuración del nivel de protección permanente: sistema, correo electrónico.

7.2. Cortafuegos (Firewall)

Duración aproximada de la práctica: 10 min.

Contenido de la práctica:

1. Identificación del icono que representa al cortafuegos.
2. Acceso a la consola de administración del cortafuegos.
3. Configuración del cortafuegos según las instrucciones suministradas (dependerá de la aplicación utilizada).

7.3. Firma de documentos

Duración aproximada de la práctica: 10 minutos

Contenido de la práctica:

1. Firma de un documento con Word.

7.4. Verificación de la identidad de servidores seguros

Duración aproximada de la práctica: 10 minutos

Contenido de la práctica:

1. Cargar la página de la Agencia Española de Protección de Datos: www.agpd.es
2. Hacer doble clic sobre el candado que aparece en la barra de tareas.
3. Examinar el certificado presentado por el servidor.

8. Certificación digital para el abogado: ACA, la Autoridad de Certificación de la Abogacía

8.1. Presentación

Tal como se vio en el módulo básico, el Consejo General de la Abogacía Española se constituye en 2003 en Autoridad de Certificación de la Abogacía, con el objetivo de certificar la condición de abogado en el entorno digital.

La Autoridad de la Certificación de la Abogacía (en adelante, ACA), como órgano representativo, coordinador y ejecutivo superior de los Ilustres Colegios de Abogados de España, goza de la credibilidad y la confianza de los abogados, sus clientes o las Administraciones Públicas.

La actividad de ACA está regulada en una Declaración de prácticas de certificación, tal como explicamos a continuación.

8.2. Declaración de prácticas de certificación

El contenido de una Declaración de Prácticas de Certificación lo establece el art. 19 de Ley de Firma electrónica:

> *«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.*
> *[…]»*

La Declaración de Prácticas de Certificación de ACA se encuentra disponible en la siguiente URL:

https://documentacion.redabogacia.org/docushare/dsweb/View/Collection-1316

Su estructura es la siguiente:

- En el apartado “1.3 Comunidad y ámbito de aplicación” se establece quiénes son los agentes implicados en ámbito del documento: el prestador de servicios de certificación, la autoridad de certificación, las autoridades de registro, los suscriptores, los usuarios y los solicitantes. También se establecen los usos prohibidos de los certificados.
- En el apartado “2.1 Obligaciones” se establecen las obligaciones de los siguientes agentes: autoridad de certificación, autoridades de registro, suscriptores, usuarios y solicitantes.
- En los apartados “2.2 Responsabilidad” y “2.3 Responsabilidad financiera” se delimita la responsabilidad del prestador de servicios de certificación.
- En el apartado “2.6 Publicación y Registro de Certificados” se expone cómo se difunde la información relativa a los certificados. Recordemos que el art. 18 de la Ley de Firma impone la obligación de contar con un directorio de certificados.
- En el apartado “2.7 Auditorías” se delimita el alcance y frecuencia de las auditorías a las que se someten periódicamente la autoridad de certificación y las autoridades de registro.
- En el apartado “2.8 Confidencialidad y Protección de Datos Personales” se clasifica la información y se establece el tratamiento que merece en función de su naturaleza.
- El apartado “3 Identificación y Autenticación” establece qué se acepta como nombre de titular del certificado y cómo se verifica su identidad. También contempla la renovación y reemisión de los certificados. Este apartado presenta un contenido relativo a la operativa de las autoridades de registro.
- En el apartado “4 Requerimientos Operacionales” se establecen los procedimientos operativos que se refieren a la solicitud, emisión, suspensión y revocación de certificados. También se contemplan procedimientos operativos relacionados con la gestión de la seguridad por parte de la autoridad de certificación, tales como la gestión de logs, (archivos creado por el servidor donde se registran las acciones que los usuarios generan en la web), la recuperación de claves en caso de desastre y el cese de operaciones.
- En los apartados “5 Controles de Seguridad Física, Procedimental y de Personal” y “6 Controles de Seguridad Técnica” se establecen los controles que emplea la autoridad de certificación para la gestión del ciclo de la seguridad.
- En el apartado “7 Perfiles de Certificados y CRL” se establece la estructura de los certificados y de la lista de certificados revocados (CRL).

Además, cuenta con un anexo de protección de datos de carácter personal.

8.3. Políticas de certificación

La Autoridad de Certificación de la Abogacía cuenta con tres tipos de certificados reconocidos, existiendo una política por cada uno de ellos:

- Política de Certificado Reconocido Corporativo de Colegiado
- Política de Certificado Reconocido Corporativo de Personal Administrativo
- Política de Certificado Reconocido Corporativo de Persona jurídica

Las políticas recogen parte del contenido de la Declaración de Prácticas de Certificación, y se encuentran disponibles en la siguiente URL:

https://documentacion.redabogacia.org/docushare/dsweb/View/Collection-1317

En las políticas se establece las características de cada uno de los tipos de certificado, detallando:

- Quién y cómo puede solicitarlo.
- Procedimiento de identificación y autenticación.
- La estructura del certificado.

Lo habitual es que un prestador de servicios de certificación tenga una declaración de prácticas de certificación y tantas políticas como tipos de certificados emita.

9. Despedida

9.1. Resumen

En esta sesión hemos tratado los siguientes temas:

- Aproximación a la seguridad de la información.
- Problemas de seguridad que plantea el uso de las herramientas informáticas.
- Herramientas y técnicas de seguridad.
- Declaración de Prácticas de Certificación y Políticas de Certificación de ACA

9.2. En la próxima sesión

En la próxima sesión se tratarán los siguientes temas:

- RED Abogacía
- Servicios telemáticos seguros para el ejercicio de la abogacía:
    - Censo general de letrados
    - Pases a Prisión
    - Buromail

TERCERA SESIÓN

Servicios telemáticos para el ejercicio de la abogacía (I)

1. Introducción

1.1. Recordatorio de la 2ª sesión

En la sesión anterior se trataron los siguientes temas:

- Aproximación a la seguridad de la información.
- Problemas de seguridad que plantea el uso de las herramientas informáticas.
- Herramientas y técnicas de seguridad.
- Declaración de Prácticas de Certificación y Políticas de Certificación de ACA

1.2. Presentación de la 3ª sesión

Al finalizar esta sesión habrá adquirido los siguientes conocimientos:

- RED Abogacía
- Servicios telemáticos seguros para el ejercicio de la abogacía:
    - Censo general de letrados
    - Pases a Prisión
    - Buromail

2. Servicios telemáticos para el ejercicio de la Abogacía (Introducción)

2.1. Presentación

La página web RedAbogacia.org es una extranet dirigida a la Abogacía que comienza su desarrollo en 2004 como plataforma de servicios seguros que permite la interoperabilidad entre los distintos Colegios de Abogados y sus colegiados. Estos servicios ofrecen valor añadido para el abogado, permitiéndole, desde la zona privada de su colegio de abogados, comunicarse con su Colegio, con la Administración de Justicia, con otras Administraciones Públicas, y con otras entidades de forma más ágil, segura e identificada a través de su carné colegial que aloja el certificado digital ACA.

Las ventajas en términos de coste y valor añadido de los servicios de Redabogacia.org son considerables, ya que permiten reducir el consumo de tiempo, papel y franqueo al sustituir las formas tradicionales con el uso de las comunicaciones electrónicas, además de posibilitar la comunicación directa, en horario 24x7 y tiempo real.

2.2. Servicios de RED Abogacía

Aunque se han enunciado en apartados anteriores, pasamos a continuación a explicar brevemente cada uno de los servicios de RedAbogacía.

Servicios genéricos

1. **Noticias tecnológicas**
2. **Correo electrónico (Webmail):** permite consultar su correo electrónico desde cualquier parte con su certificado digital.
3. **Consulta del Censo General de Letrados:** permite la consulta del Censo General de colegiaciones de todo el territorio nacional desde cualquier lugar a través de Internet. Los datos ofrecidos son los suministrados por los Colegios conforme a lo exigido por la LOPD.

Servicios vigentes desarrollados para comunicaciones y trámites con la Abogacía Institucional:

1. **Generación de Pases a Prisión**: permite la Generación de volantes para visitar centros penitenciarios de toda España desde cualquier lugar a través de Internet, informando a los Colegios de residencia y de destino, que pueden acceder a la base de datos de documentos firmados electrónicamente. Para generar un pase a prisión, el abogado debe utilizar su certificado digital, con el que firma su declaración responsable. El sistema almacena el documento firmado a fin de constituir una posible prueba y emite un pase que incorpora un código de seguridad inviolable. El servicio de pases a prisión incorpora además la posibilidad de verificar la autenticidad de los pases, pensado para que los funcionarios de prisiones puedan verificar su validez.

2. **Comunicaciones de Intervención Profesional**: Este servicio permite al abogado, a través de su certificado digital, informar al Colegio de Abogados de destino, al propio y a los consejos implicados, de cualquier actuación profesional en una zona distinta a la de su colegio de residencia. Las comunicaciones se pueden hacer desde cualquier lugar a través de Internet.

3. **BuroMail:** permite al colegiado el envío gratuito, a través de Redabogacía, de correos electrónicos (con o sin archivos adjuntos) con la máxima seguridad y fiabilidad a otros usuarios generando prueba de envío y de recepción por parte del destinatario. Tanto la prueba de envío, como la confirmación de apertura por el destinatario, son documentos digitales originales que incorporan sellado electrónico. Los avisos de que alguien nos ha enviado un BuroMail o de que el destinatario a quien se lo enviamos lo ha recibido, pueden enviarse a una cuenta de correo electrónico convencional o a un número de teléfono móvil en forma de mensaje de texto. Redabogacía da acceso, en pocos segundos, al envío y recepción de documentos remitidos de manera electrónica entre las partes, generándose una prueba que garantiza la autenticidad e integridad de la transmisión, así como la fecha y hora del envío.

4. **SecuriWeb** (disponible bajo solicitud del Colegio) Para los colegios de Abogados que dispongan de una zona de acceso restringido en su web colegial, este servicio permite el acceso a abogados que se identifiquen con su certificado digital de ACA.

Servicios web seguros en colaboración con las Administraciones Públicas y otros organismos:

1. **Presentación de Escritos en los Juzgados: Lexnet.** Es una plataforma de comunicaciones desarrollada por el Ministerio de Justicia y pensada específicamente para la presentación de escritos a los juzgados. Esta plataforma se ha integrado en RedAbogacía junto con otros servicios exclusivos para Abogados para facilitar el ejercicio de la profesión a través de Internet. LexNet es una iniciativa que supone un importante hito para todos los profesionales del Derecho, por la que la Administración de Justicia ofrecerá la posibilidad de desarrollar una importante parte de la actividad profesional de forma telemática, con los beneficios en cuanto a rapidez, claridad y transparencia que ello puede reportar tanto al abogado como a la sociedad en general. **LexNet**, actualmente en fase de implantación en los juzgados, contempla la posibilidad de actuar de forma telemática ante los órganos judiciales participantes tanto para los abogados como para los procuradores, respetando cuidadosamente la actual Ley de Enjuiciamiento Civil.

   La integración de las plataformas LexNet y RedAbogacia permite al abogado, directamente o a través de procurador, la presentación de escritos judiciales ante un órgano judicial y recibir de éste las correspondientes comunicaciones. Además, la integración de LexNet con los servicios de Avisos que dispone RedAbogacía, permite que los Abogados reciban avisos en su teléfono móvil o en su cuenta de correo electrónico (según la modalidad de confirmación deseada) en el momento en que tenga pendiente una notificación en la plataforma LexNet del Ministerio de Justicia.

2. **Acceso a la plataforma Hermes web del Registro:** este servicio, actualmente en desarrollo, proporciona acceso seguro a consultas informativas, anotaciones marginales, presentación de cuentas anuales en su nombre y/o en nombre de terceros en los Registros Mercantil y de la Propiedad.

3. **Oficina virtual del Catastro:** esta aplicación, actualmente operativa, permite a los usuarios darse de alta en el servicio mediante certificado digital y realizar consultas catastrales sobre bienes de su titularidad, a nivel nacional.

Servicios en colaboración con terceros.

1. **Consulta de Jurisprudencia y legislación en RedAbogacia (Iuris et Legis).** A través del Convenio alcanzado con la Editorial La Ley, desde Redabogacia, utilizando el nuevo carné colegial con certificado de ACA, los colegiados pueden consultar los contenidos gratuitos ofrecidos por la editorial en su base de datos de jurisprudencia Colex Data. Además, gracias al Convenio, los colegiados que se suscriban a Colex Data utilizando su nuevo carné colegial, obtendrán un importante descuento.

2. **Oficina Virtual de Correos en RedAbogacia:** Gracias al convenio firmado con Correos, se ha abierto una Oficina Postal Virtual en Redabogacía. De esta forma el abogado con su nuevo carné colegial con certificado digital de ACA, puede enviar cartas o telegramas online desde su despacho, evitando desplazamientos innecesarios a la oficina de Correos. Además, a través de Redabogacía, el colegiado puede conocer el momento y circunstancias de la entrega del mensaje, localizar sus envíos e identificar certificados, entre otros A estos servicios, en breve se añadirá la posibilidad de enviar BuroFaxes.

3. **SIGA:** Este programa de gestión se encuentra en fase de implantación en algunos Colegios de Abogados. Una vez culminado, su acceso se configurará a través de Redabogacía, y facilitará al colegio de abogados la optimización de recursos, aumentando la eficiencia de sus comunicaciones con los letrados y la Administración.

Servicios telemáticos de la Administración Pública:

El certificado digital ACA está reconocido por muchas Administraciones Públicas a nivel nacional, autónomo y local. El Consejo General de la Abogacía Española continúa trabajando para que los abogados puedan realizar trámites telemáticos con los distintos Ministerios y Administraciones locales y regionales. El listado actualizado de entidades que acreditan el certificado digital ACA está disponible en www.acabogacia.org/zona institucional/acreditaciones y convenios.

Cabe destacar aquí el valor añadido que para el abogado supone la Oficina Virtual de la AEAT, a la que se puede acceder a través de www.aeat.es. El abogado puede, con su certificado digital ACA, acceder vía Internet a diversos servicios de la Agencia Tributaria a título personal y de terceros, como por ejemplo:

- Presentación de la declaración del IRPF.
- Consulta online de notificaciones administrativas

- Presentación del modelo 190 en nombre de terceros. (Impreso que se presenta por las Empresas a la AEAT en el cual aparece el resumen anual de retenciones e ingresos a cuenta del IRPF de su trabajadores)
- Consulta de los propios datos fiscales
- Presentación de facturas electrónicas con plena validez mercantil y solicitud online de etiquetas tributarias

2.3. Práctica: Oficina virtual de Correos: mandar un telegrama

Duración aproximada de la práctica: 15 min.

Contenido de la práctica:

1. Acceder a la zona privada en RED Abogacía.
2. Acceder a la oficina virtual de Correos.
3. Darse de alta como usuario
4. Enviar un telegrama a la dirección facilitada por el profesor.

3. Servicios telemáticos para el ejercicio de la abogacía (I)

3.1. Censo

A continuación se dan unas breves indicaciones a modo de introducción al servicio. Podrá encontrar información más detallada en el manual del servicio, accesible en el gestor documental de RED Abogacía en la siguiente ubicación:

https://documentacion.redabogacia.org/docushare/dsweb/View/Collection-1013

3.1.1. Descripción del servicio

El Censo de Letrados contiene los datos profesionales (dirección profesional, nº de teléfono, nº de colegiado, Colegio de pertenencia, tipo de colegiación, etc.) de los colegiados de los Colegios de Abogados de España. Estos datos son siempre suministrados por los Colegios de Abogados, por lo que cualquier corrección que se desee en los datos deberá comunicarse al Colegio de Abogados.

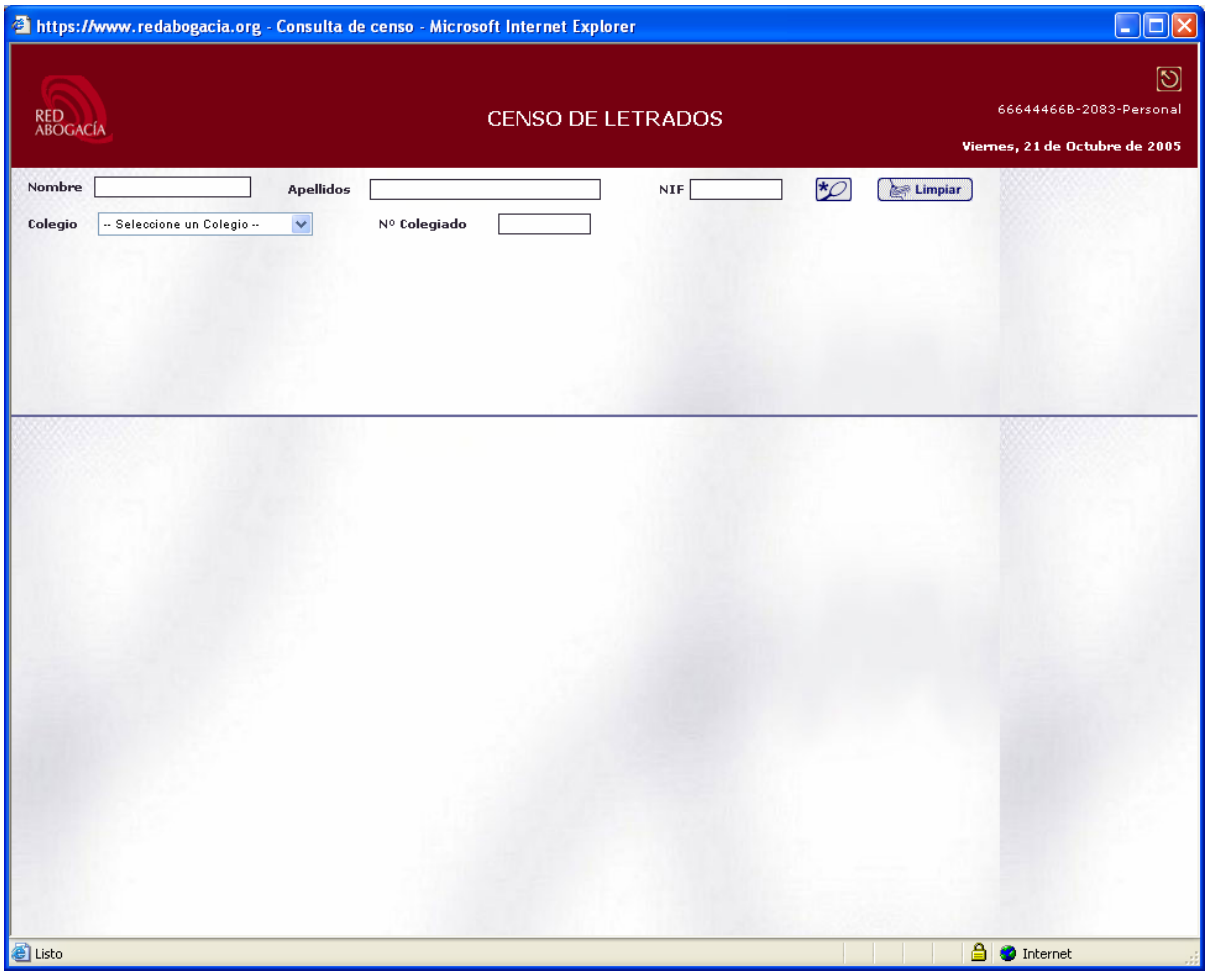
3.1.2. Usuarios

Cualquier usuario de Internet.

3.1.3. Acceso

El acceso se puede hacer desde la parte pública de Redabogacia (www.redabogacia.org) o desde alguna zona privada de Colegio en Redabogacia.

Una vez se haya accedido a la aplicación, aparecerá la siguiente pantalla:



3.1.4. Utilización del servicio

Se trata de un sistema de búsqueda a través de un filtro con diversos criterios de búsqueda (nombre, NIF, Colegio, etc.)

Estos criterios se pueden combinar a fin de refinar la búsqueda.

Una vez rellenado alguno de estos datos, es necesario hacer clic en el botón con el dibujo de una lupa para que se realice la búsqueda.

Una vez realizada la búsqueda se muestra el resultado en la misma ventana.

La ventana se divide en dos partes: superior e inferior.

En la parte superior se indica el número de registros encontrados (lado izquierdo) y las páginas para acceder a ellos (lado derecho). Justo debajo aparecen dos columnas: “Nombre” y “Apellidos”.

Si hacemos clic en algún registro se muestra la información correspondiente a ese colegiado en la parte inferior de la ventana.

Los datos que se muestran son:

- Nombre / Apellidos
- Dirección Profesional /Código Postal /Población /Teléfono
- Colegios en el que reside o ejerce.
- Número de Colegiado.
- Fecha de alta de la Colegiación.
- Si es residente o no residente en ese Colegio.
- Si es ejerciente o no ejerciente en ese Colegio.
- Fecha de actualización de los datos.

Para ver los datos de otro colegiado obtenido como resultado de la búsqueda, basta con hacer clic sobre el registro correspondiente.

Para realizar una nueva búsqueda, haremos clic sobre el botón “Limpiar”, situado en la parte superior de la ventana, para que se borre el formulario de búsqueda y desaparezcan los datos mostrados.

Para salir de la aplicación pulsaremos el botón “Desconectar”, situado en la esquina superior derecha de la ventana.

3.2. Práctica: Censo

Duración aproximada de la práctica: 5 minutos

Contenido de la práctica:

1. El alumno se buscará a sí mismo en el Censo.

3.3. Pases a Prisión

A continuación se dan unas breves indicaciones a modo de introducción al servicio. Podrá encontrar información más detallada en el manual del servicio, accesible en el gestor documental de RED Abogacía en la siguiente ubicación:

https://documentacion.redabogacia.org/docushare/dsweb/View/Collection-1013

3.3.1. Descripción del servicio

Es el servicio del Portal Redabogacia que da la posibilidad al Letrado de solicitar de forma telemática a su Colegio de Abogados de residencia un pase a prisión para poder tener acceso a un Centro Penitenciario y así poder visitar a los internos.
Este servicio se agiliza al verificarse la condición de abogado de ese letrado cada vez que accede a este servicio (garantizando deontología profesional) ya que cada solicitud es firmada con su Certificado Digital de abogado.
Cuando se produce dicho trámite, se manda automáticamente una comunicación informativa en formato digital al Colegio de Abogados de la demarcación a la que pertenece este Centro Penitenciario.

3.3.2. Usuarios

A este servicio sólo pueden acceder los usuarios con perfil de abogado que tengan el Certificado Digital ACA.

3.3.3. Acceso al servicio

1. Entrar a la zona privada de su Colegio de residencia, bien desde la página principal de RED Abogacía o bien desde el enlace habilitado en la página web de su Colegio.
2. Hacer clic en el enlace de la aplicación “Pases a Prisión”.

3.3.4. Utilización del servicio

Solicitar pase

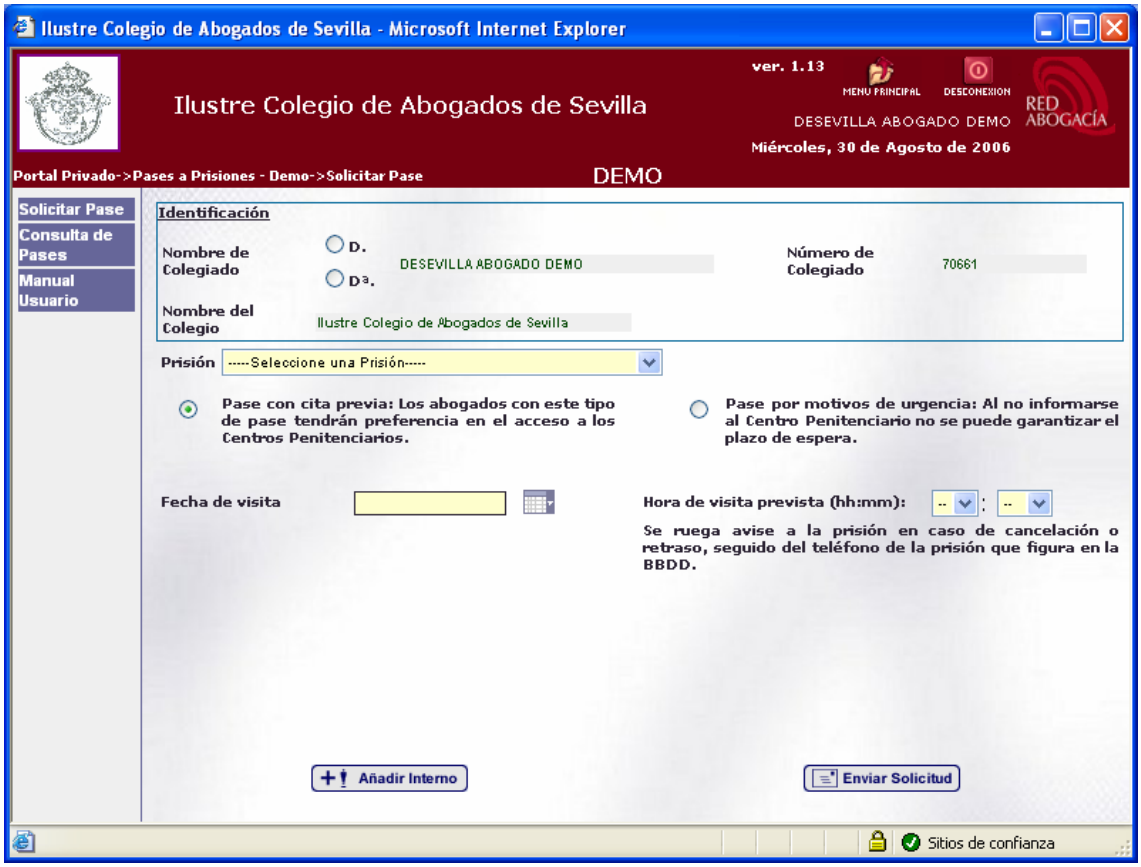
Este módulo funcional permite a un Usuario con rol de Abogado solicitar el pase a una prisión para visitar a un interno.

Para acceder a este módulo hay que hacer clic en el enlace “Solicitar Pase” que aparece en el menú de Pases a Prisiones.

NOTA: Para poder realizar la firma digital del Pase a Prisión, el sistema necesita que el PC del usuario tenga instalado un componente llamado SAMIS. El sistema verificará si su PC tiene dicho componente instalado. Si el componente SAMIS no está instalado en su PC, el sistema instalará el componente, previa autorización del usuario. Debe permitir la instalación del mismo para poder firmar la solicitud del pase.

La pantalla principal de solicitud consta de los siguientes elementos:

- Identificación. En la parte superior de la pantalla se identifica al emisor del Pase a Prisión. Estos datos se toman automáticamente de su Certificado Digital (Nombre del Colegiado, Número de Colegiado y Nombre del Colegio de residencia). Estos datos no pueden ser modificados por el usuario.
- Prisión para la que se solicita el pase. Lista desplegable con todas las prisiones para las que se podrá solicitar un pase.
- Elección del tipo de visita:
    - Visita con cita previa. Se informará a la prisión de la fecha y hora de visita.
    - Visita por motivos de urgencia. En esta opción no será necesario introducir la fecha y hora de visita.
- Fecha de visita, ésta debe ser posterior o igual a la fecha actual. Si se pide para el día actual, la hora de visita debe ser posterior al momento de solicitud. La fecha se puede seleccionar usando el calendario.
- Hora de visita. Se expresa en horas y minutos. Dependiendo de la prisión seleccionada se mostrarán horarios diferentes, puesto que cada prisión tiene sus propios horarios de visita.



Si la solicitud del pase es mediante “visita previa” en la pantalla aparecerán los campos Fecha de visita y Hora de visita.

En caso de seleccionar “visita por motivos de urgencia” los campos Fecha de visita y Hora de visita se ocultarán.

A continuación es necesario introducir el interno a visitar y los motivos de visita:

- Para introducir el interno a visitar basta con hacer clic en el botón “Añadir Interno”, que al ser pulsado abre la ventana para la introducción del Nombre del interno y el Motivo de visita.
- Motivos de visita:
    - Llamado por el interno. No será necesario introducir ningún dato más.
    - Como defensor del mismo. Se deberá introducir la causa y el tribunal.
    - Llamado por los familiares. Será obligatorio introducir el nombre de la persona que ha realizado dicha petición.
    - Turno de oficio. Indicando la causa y el tribunal.

Una vez introducido el nombre y el motivo se pulsará sobre el botón “Aceptar”.

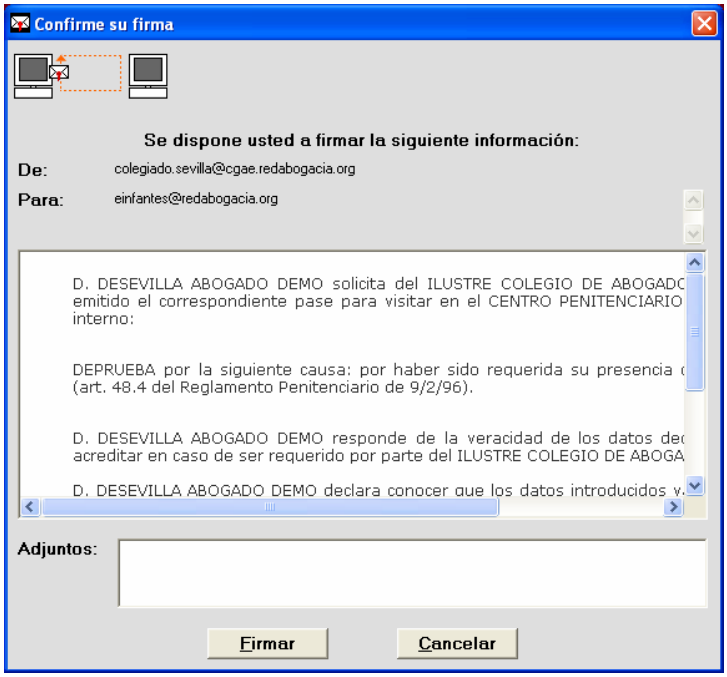
Para eliminar el interno de un pase, se pulsara sobre él, en la tabla de la pantalla principal para que aparezca la Ventana Gestión de Internos.

Sólo se podrá crear un pase a prisiones para un interno.

Cuando se hayan rellenado todos los datos del pase a prisiones se elegirá la opción “Enviar Solicitud” que abrirá la ventana que muestra las implicaciones de la firma y da la posibilidad de firmar digitalmente la solicitud.

En el caso de seleccionar ‘Visita con cita previa’ y elegir una fecha y una hora fuera de margen (no es posible enviar el correo a la prisión a tiempo) al intentar enviar la solicitud, se mostrará una pantalla de aviso.

Si los datos de la solicitud son correctos, al pulsar sobre ‘Enviar Solicitud’ aparece la pantalla para aceptar el proceso de firma a través de SAMIS.



La ventana de firma muestra el texto que el usuario se dispone a firmar.

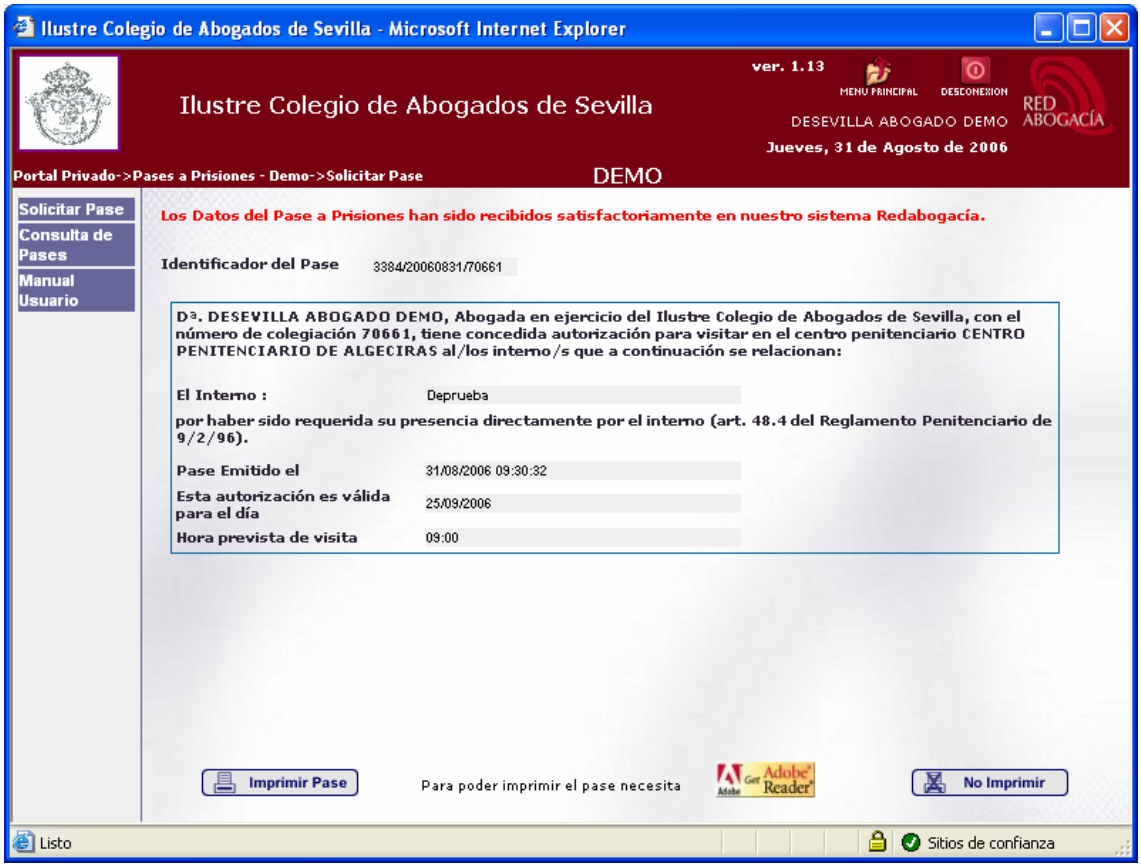
Para proseguir con el envío del pase a prisión, es necesario hacer clic en el botón “Firmar”.

En el caso de que se realice un pase a prisiones para una prisión que no pertenece a la zona Geográfica del Colegio se enviará un correo al Colegio o Colegios de la zona geográfica correspondiente.

En el caso en el cual una prisión corresponda a la zona geográfica de dos colegios, no enviará correo a ninguno de ellos si el abogado corresponde a alguno de estos colegios, en caso contrario, enviará correo a ambos colegios.

Una vez completado el proceso de firma digital de la solicitud aparece una pantalla en la que hay un resumen de toda la información contenida en dicho pase.

Una vez firmado el pase se muestra la ventana que se reproduce en la siguiente ilustración.



En la parte inferior de la pantalla están los botones de “Impresión” (el pase sólo se podrá imprimir una vez), para imprimir el pase solicitado y de “No Impresión”, si no se quiere imprimir el pase en ese momento (el pase se podrá imprimir más tarde).

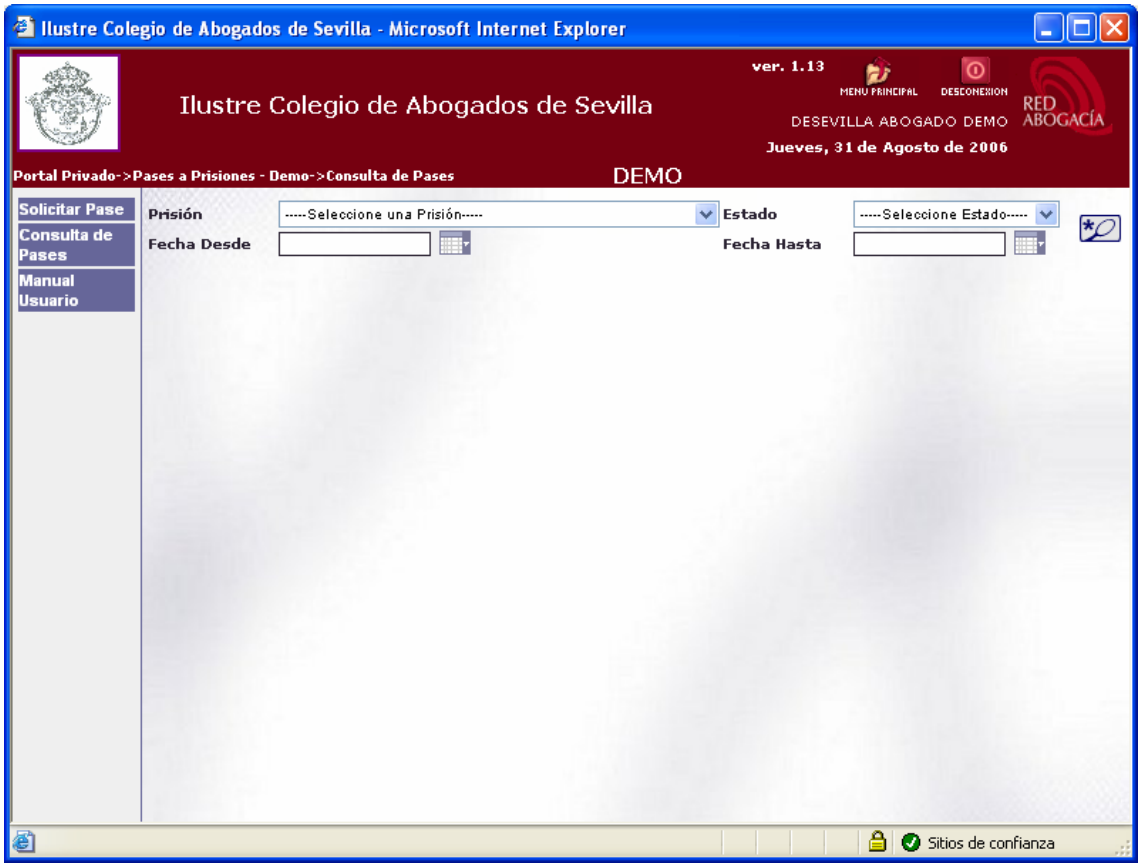
Para la impresión de los pases es necesario tener instalado en local la aplicación ACROBAT READER. En caso de que no se tenga instalada puede ser descargada pulsando en el link de ACROBAT que se encuentra en la parte inferior de la pantalla.

Si la impresión ha sido correcta aparecerá el siguiente mensaje: “El pase ha sido enviado a su impresora. Pulse aceptar cuando termine la impresión”.

Si el proceso se ha realizado correctamente le aparecerá el siguiente mensaje: “Proceso finalizado con éxito”.

Consulta de pases

Este módulo, permite a cada Usuario con rol de Abogado consultar todos los pases que él mismo ha solicitado. Para acceder a este módulo hay que hacer clic sobre el enlace “Consulta de Pases”.

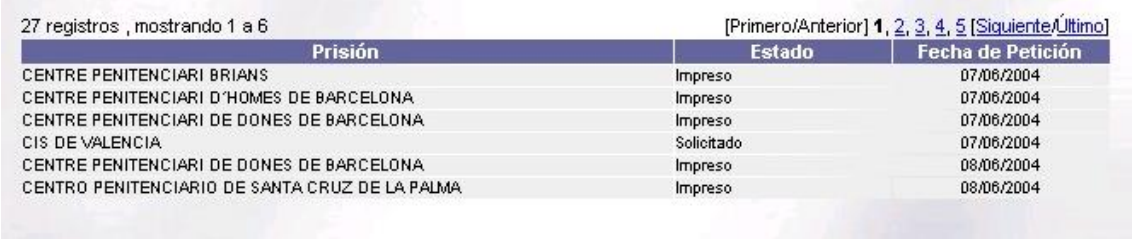


Pulsando el botón “Buscar” se realiza un filtro sobre el listado. Si se han dejado en blanco los campos del formulario, se obtendrá el listado entero.

Los campos por los que se podrá realizar el filtro son:

- Prisión. Es la prisión para la que se ha solicitado el pase.
- Estado. Estado en el que se encuentra el pase.
- Fecha Desde / Fecha Hasta. Permite definir el intervalo de fechas en el que se ha solicitado el pase.

El listado de Pases contendrá los siguientes datos: la Prisión, el Estado y la Fecha de petición.


27 registros , mostrando 1 a 6 [Primero/Anterior] 1, 2, 3, 4, 5 [Siguiente/Último]

Prisión	Estado	Fecha de Petición
CENTRE PENITENCIARI BRIANS	Impreso	07/06/2004
CENTRE PENITENCIARI D'HOMES DE BARCELONA	Impreso	07/06/2004
CENTRE PENITENCIARI DE DONES DE BARCELONA	Impreso	07/06/2004
CIS DE VALENCIA	Solicitado	07/06/2004
CENTRE PENITENCIARI DE DONES DE BARCELONA	Impreso	08/06/2004
CENTRO PENITENCIARIO DE SANTA CRUZ DE LA PALMA	Impreso	08/06/2004

Si el número de elementos resultantes de la búsqueda es mayor que la dimensión de la tabla los resultados se presentarán paginados. En la parte superior izquierda aparece en número de registros obtenidos en la búsqueda. En la parte superior derecha aparecen elementos que permiten navegar por las diferentes páginas de resultados (Primera página, Página Anterior, Nº de página, Página siguiente y Última página)

Pulsando sobre uno de los pases de la tabla se mostrará el detalle del mismo.

Manual de Usuario

Este módulo, permite a cada Usuario con rol de Abogado consultar y descargar el Manual de Usuario.

Para acceder a este módulo hay que pinchar sobre el enlace “Manual Usuario” que aparece en el menú de Pases a Prisiones.

3.4. Práctica: Pases a Prisión

Duración aproximada de la práctica: 15 minutos

Contenido de la práctica:

1. Emitir un pase a prisión a la prisión indicada por el profesor.
2. Consultar el listado de pases a prisión generados por el usuario.

3.5. Buromail

A continuación se presenta unas breves indicaciones a modo de introducción al servicio. Podrá encontrar información más detallada en el manual del servicio, accesible en el gestor documental de RED Abogacía en la siguiente ubicación:

https://documentacion.redabogacia.org/docushare/dsweb/View/Collection-1013

3.5.1. Descripción del servicio

BuroMail es un servicio para la práctica de notificaciones fehacientes entre Usuarios con certificado ACA y otros Usuarios (Abogados, Colegios de Abogados y otras Instituciones del colectivo de la Abogacía) que se proporciona a través de *RedAbogacia.*

La característica esencial de esta nueva herramienta de comunicación es la posibilidad de enviar correos electrónicos a otros usuarios generando prueba de envío y de recepción por parte del destinatario, de forma similar al servicio **Burofax,** por todos conocido, con la ventaja añadida del envío telemático. Tanto la prueba de envío, como la confirmación de apertura por el destinatario, son documentos digitales originales que incorporan sellado electrónico. Es un servicio de fácil acceso, rápido y de calidad basado en un sistema de correo electrónico que proporciona máxima seguridad y fiabilidad en la comunicación.

A través de este servicio se reducen a escasos segundos las operaciones de envío y recepción de documentos remitidos de manera electrónica entre las partes generándose prueba que garantiza la autenticidad e integridad de la transmisión, así como la fecha y hora del envío.

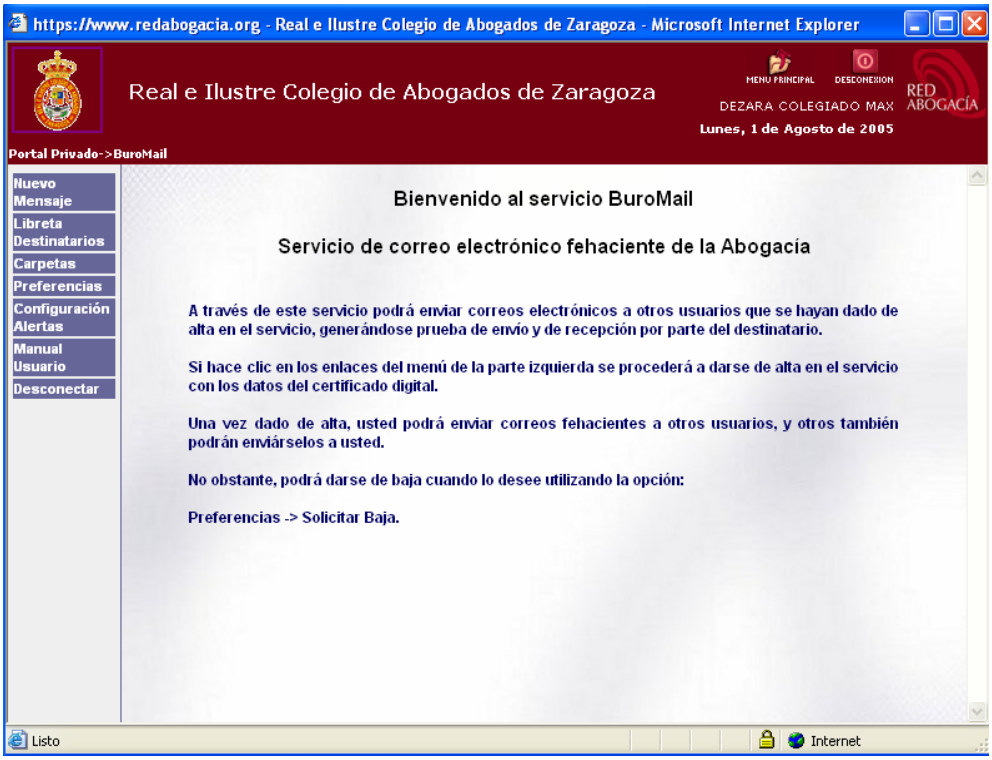
3.5.2. Usuarios

A este servicio sólo pueden acceder los usuarios con perfil de abogado, que tengan el certificado digital ACA.

3.5.3. Acceso al servicio

1. Entrar a la zona privada de su Colegio de residencia, bien desde la página principal de RED Abogacía o bien desde el enlace habilitado en la página web de su Colegio.
2. Hacer clic en el enlace de la aplicación “Buromail”.

Una vez producido el acceso a la aplicación, aparecerá la siguiente pantalla:



3.5.4. Utilización del servicio

Los Abogados, al acceder al servicio BuroMail por medio de su certificado digital ACA, quedan registrados como usuarios del servicio, pudiéndose dar de baja cuando lo deseen.

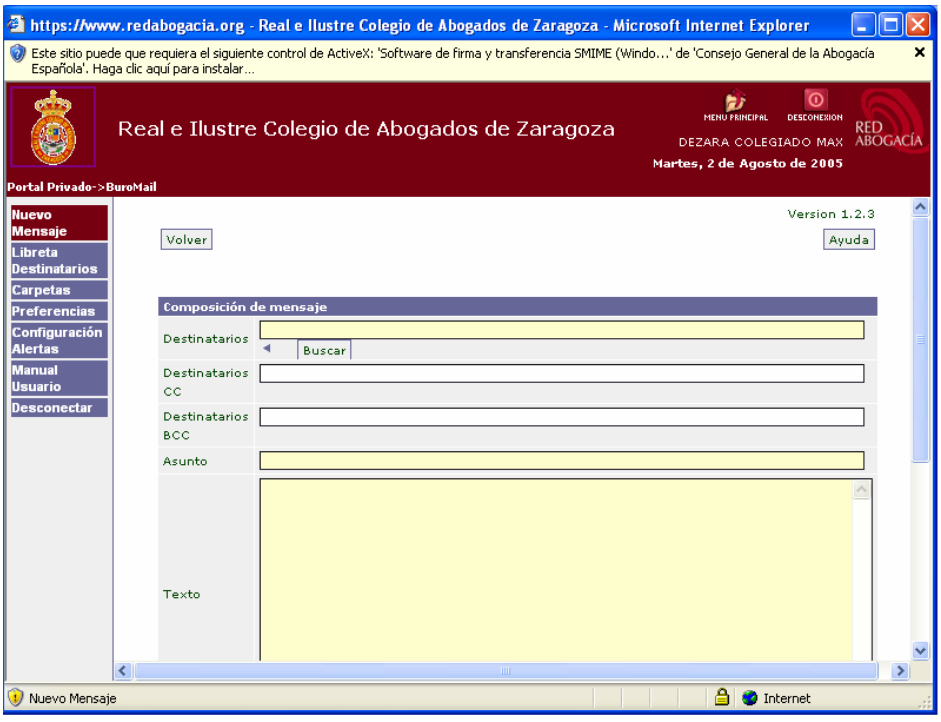
El usuario podrá enviar notificaciones fehacientes y electrónicas a otros usuarios que se hayan dado de alta en el servicio, es decir, a todos aquellos usuarios que dispongan de un certificado digital ACA y que hayan accedido alguna vez a la aplicación “Buromail”.

Las opciones disponibles en BuroMail son las siguientes:

1. Nuevo Mensaje
2. Libreta de Destinatarios
3. Carpetas
4. Preferencias
5. Configuración de Alertas
6. Manual de Usuario
7. Desconectar

Nuevo mensaje

Mediante la función de **Nuevo Mensaje** se podrá componer un nuevo mensaje. Para ello dispondrá de un formulario con los campos que se muestran en la siguiente ilustración.



Descripción de los campos a rellenar:

- Destinatarios
    - Destinatarios BuroMail o Internos. Son aquellos usuarios que se han dado de alta en este servicio BuroMail con anterioridad. El alta se realiza de forma automática en el momento de seleccionar cualquiera de las opciones del menú izquierdo de este servicio. Pueden optar por darse de baja en cualquier momento, solicitándolo en la función situada en la sección de “Preferencias”. Los envíos realizados a estos destinatarios contarán con la funcionalidad de “Confirmación de Lectura”, es decir, garantiza la apertura del mensaje por el receptor.
    - Destinatarios externos. Son aquellos usuarios que no están dados de alta en el servicio. Permite introducir en el formulario cualquier tipo de cuenta de correo electrónico. El envío a estos usuarios no permite utilizar la funcionalidad de recepción de “Confirmación de Lectura”. Por otro lado se garantiza mediante firma digital el envío pero no la recepción del documento.

- Destinatarios CC
    - Destinatarios internos y 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 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.

Para rellenar los campos "Destinatario", "Destinatario CC" y "Destinatario BCC" pulsaremos sobre el botón “Buscar” y podremos seleccionar los destinatarios de cuatro formas diferentes:

1. Libreta personal
2. Grupos
3. Por nombre
4. Por zona.

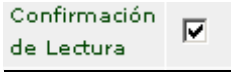
- Asunto. Es el título del mensaje.

- Texto. Consiste en texto libre a introducir por el usuario. Es el contenido del mensaje.

- Ficheros Adjuntos. Este enlace permite adjuntar los archivos que considere oportunos. Antes de ser adjuntados, los archivos son analizados por el sistema en busca de virus.

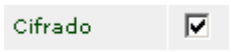
  Los pasos a seguir para adjuntar los ficheros son:
  1. El escrito que se quiere adjuntar deberá estar previamente redactado y guardado en su PC.
  2. Haremos clic en “Examinar” y buscaremos el escrito.
  3. Una vez seleccionado, haremos clic en “Añadir” para adjuntarlo.
  4. Si en algún momento se desea eliminar del mensaje un archivo de la lista de ficheros adjuntos basta seleccionarlo y seleccionar “Quitar”.

- Confirmación de Lectura: al marcar esta opción se garantiza que el texto del BuroMail enviado ha sido leído por su destinatario principal.



- Idioma: El Idioma del envío por defecto estará marcado el idioma del que envía el mensaje. Este campo se utilizará para seleccionar el idioma de la plantilla "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.



Proceso del mensaje

Una vez completado el “Nuevo Mensaje” podrá:

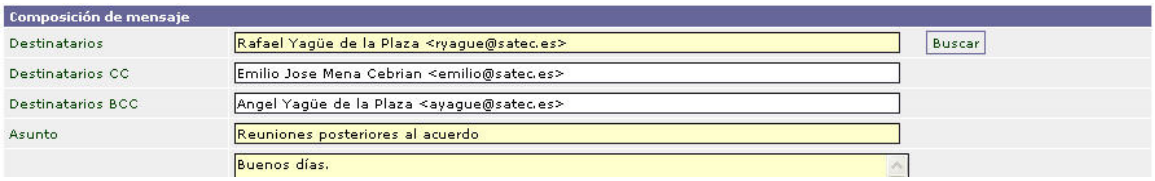
- Enviar el BuroMail haciendo clic en el botón ”Enviar”.

- Guardar los datos que se han completado en el formulario. Para guardar los datos hacer clic en el botón “Guardar como borrador”. De esta forma, se puede guardar el Borrador pudiendo realizar el envío en un momento posterior, si así se desea.

  Si se quiere guardar el Borrador después de hacer el envío, debe hacer clic en:

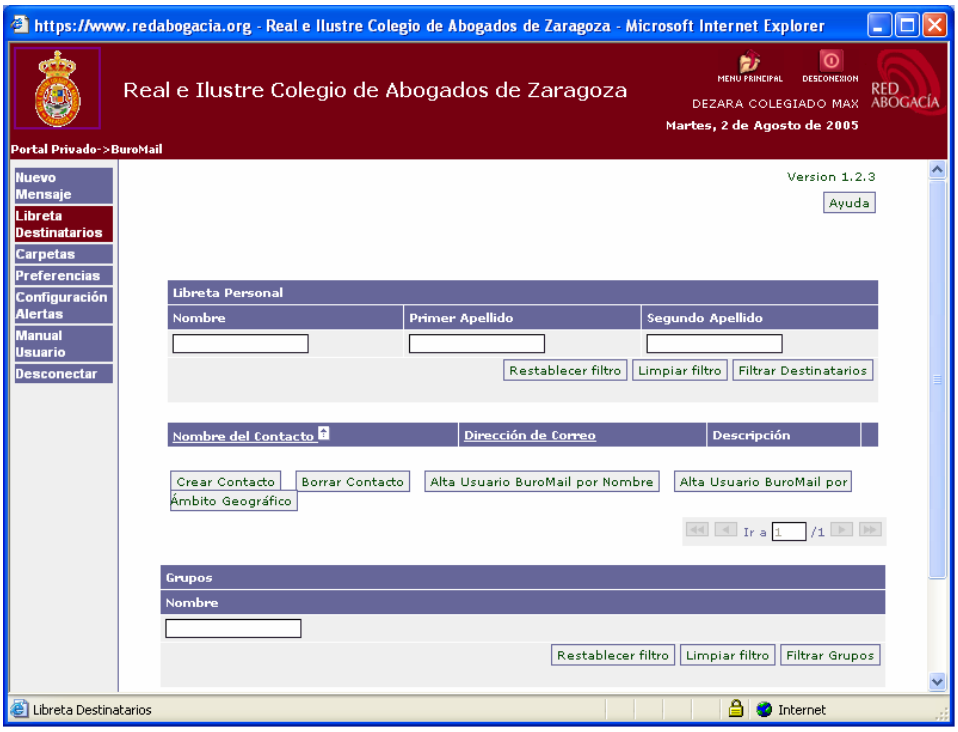
  Si el Borrador no se guarda, se perderá.

  Para visualizar al detalle el borrador basta con acudir al enlace del margen izquierdo: Carpetas → Borradores y hacer doble clic con el botón izquierdo del ratón en el borrador que queramos visualizar.



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.



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

A continuación explicamos cada una de estas funciones:

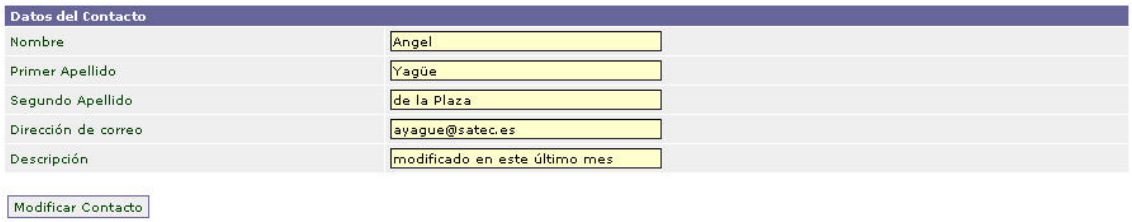
- Crear contacto. Para la creación de un contacto debemos rellenar todos los campos de la pantalla, como son nombre, apellidos, dirección de correo y una descripción, y validarlo pulsando “Crear contacto”.

- Borrar contacto. Para borrar algún contacto, lo seleccionaremos y pulsaremos sobre 'Borrar Contacto'. Podemos borrar varios contactos a la vez, seleccionaremos todos los que deseamos eliminar.

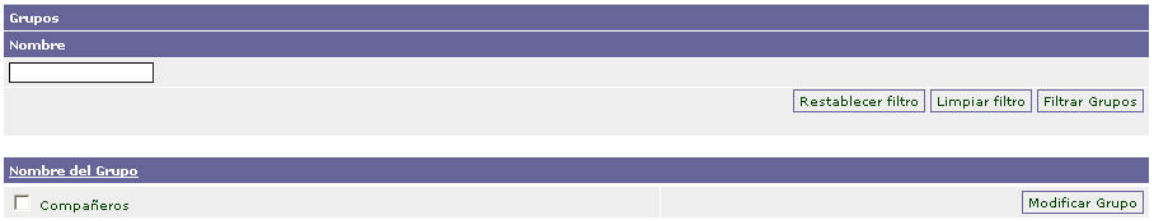
- Alta abogado por Nombre. Para dar de alta a un abogado haciendo una búsqueda por nombre, accedemos a una pantalla que nos permite una búsqueda por el nombre de todos los abogados inscritos. Tal búsqueda puede ser filtrada por el nombre o apellidos.
  Con solo pulsar sobre el abogado, se añadirá a la libreta de direcciones y se podrá elegir otro, hasta que no se desee insertar más con lo que habrá que cerrar la ventana.

- Alta abogado por Ámbito regional. Al igual que 'Alta Abogado por Nombre' pero la búsqueda se realiza por comunidad autónoma.

- Modificar contacto. Al modificar un contacto nos aparecerán los campos de dicho contacto, los cuales podremos editar y aceptar los cambios pulsando 'Modificar Contacto'.



- Grupos. También se muestran los grupos que tiene el usuario creados, dando el nombre de dichos grupos y dándonos la posibilidad de modificarlo.



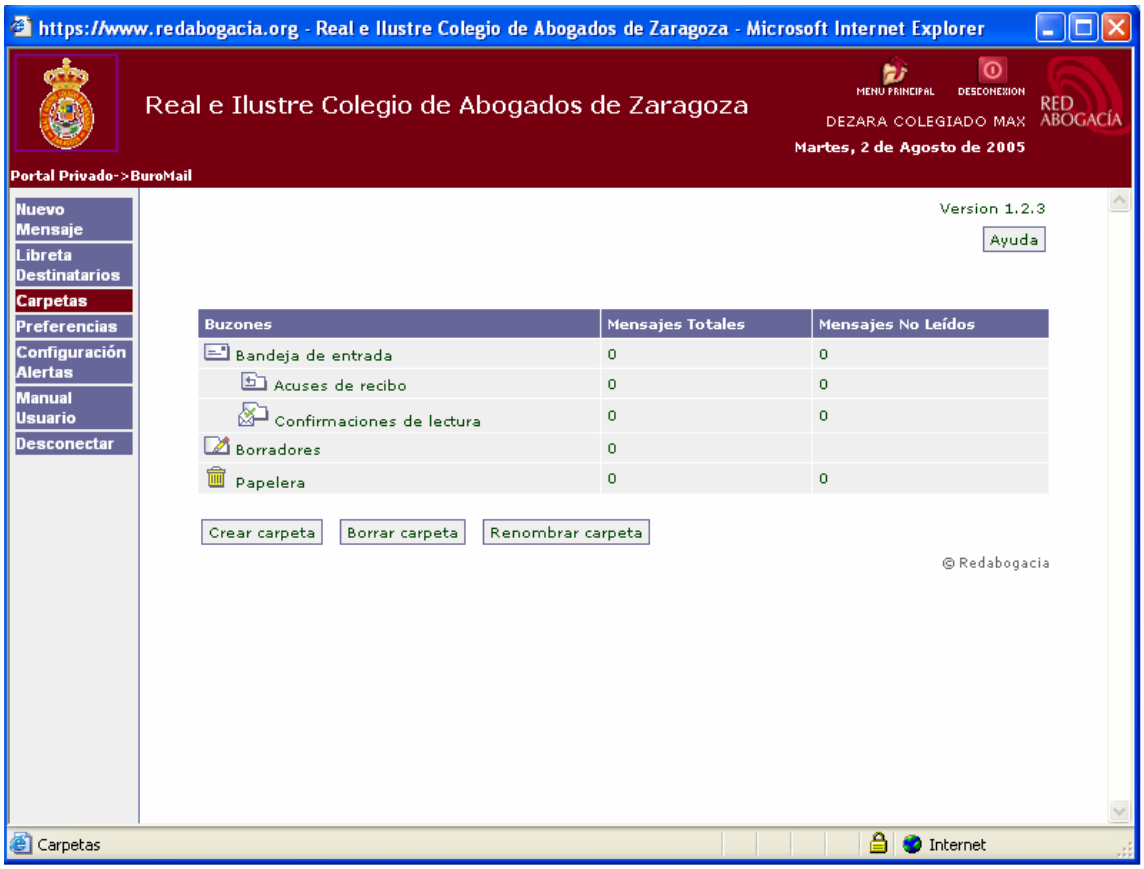
- Crear grupo. Al crear un grupo, deberemos introducir el nombre de dicho grupo y pulsar sobre 'Crear Grupo'. Para añadir contactos al grupo se hará en la parte de 'Modificar Grupo'.

- Borrar grupo. Para borrar un grupo solo habrá que seleccionarlo y pulsar 'Borrar Grupo'. Se borrarán tantos grupos a la vez como se hayan seleccionado.

- Modificar grupo. Apartado en el que se puede modificar el nombre del grupo, validándolo con 'Modificar Grupo'. Aquí, también se podrá agregar y borrar contactos pertenecientes al grupo, por medio de los botones 'Agregar Contacto' y 'Borrar Contacto'.
  Para agregar un contacto nos aparecerá un listado de todos los contactos a los que podremos aplicar un filtro de búsqueda por nombre y apellidos, y con solo pulsar sobre el que deseamos lo añadiremos al grupo. Una vez que hayamos introducido todos acabaremos dicha operación cerrando la ventana.
  Para borrar algún contacto, se seleccionará y se pulsará sobre 'Borrar Contacto'.

Carpetas

Esta función proporciona acceso a los mensajes disponibles, de manera organizada en Carpetas:



Por otra parte, los mensajes se muestran divididos en varias Carpetas: Bandeja de entrada, Acuses de recibo Confirmación de lectura, Borradores y Papelera.

Algunas de estas carpetas son fijas y no modificables, como es el caso de 'Bandeja de Entrada', 'Acuses de recibo', 'Confirmaciones de Lectura', 'Borradores' y 'Papelera' (carpetas del sistema). Otras carpetas podrán ser modificadas por el usuario, que las podrá crear, borrar y renombrar, accionando los botones destinados para realizar dichas operaciones.

Las carpetas no modificables son:

- Bandeja de entrada: a través de esta carpeta el sistema muestran los mensajes de correo recibidos por el usuario, dando la información del número total de mensajes y, también, del número de ellos no leídos.
- Acuses de recibo: a través de esta carpeta el sistema informa al Abogado del envío del mensaje quedando registrado en la Plataforma Redabogacia la fecha y la hora de la presentación del escrito. Si esta operación se ha finalizado correctamente, se recibe el acuse de recibo con el contenido íntegro del escrito enviado (Documento Principal y Documentos Anexos (si se han adjuntado).
- 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 Destinatario.
- Borradores: a través de esta carpeta el sistema almacena los mensajes que el usuario ha decidido guardar una vez enviado o ha decidido guardar para enviar en un momento posterior.
- Papelera: a través de esta carpeta el sistema almacena los mensajes eliminados.

Para ver más detalladamente las opciones de: “Borradores”, “Crear carpeta”, “Borrar carpeta” “Renombrar carpeta” basta con acudir al acceso directo de “Ayuda” (margen superior derecho de cada pantalla) en la que se explica todo las operaciones que se pueden hacer en cada enlace.

Mensajes

Abriendo cada una de las distintas carpetas se muestra el listado de los mensajes que contiene, dando las siguientes opciones: ver el mensaje de forma de detallada, mover el mensaje a otra carpeta o borrar el mensaje.

Visualización de los mensajes: 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.

A continuación se muestra un ejemplo de los campos que se pueden visualizar dentro de la Carpeta: “Confirmación de Lectura”.

Datos del Mensaje

Mediante esta función se podrá leer los mensajes de su buzón. Si el mensaje no está cifrado el contenido del mensaje se presentará en una página Web con la siguiente información, dividida en tres partes:

1. Primera parte: Aparecerá como Remitente el "Servicios Avanzados Telemáticos". Además dispondrá de las opciones 'Borrar', 'Responder', 'Responder a todos', 'Reenviar' e 'Imprimir mensaje'.

2. Segunda parte: se garantiza el registro correcto del mensaje por la Plataforma RED Abogacía, su remitente (Colegiado o Empleado) y la fecha.

3. Tercera parte: Aparecerá como Remitente el "Servicios Avanzados Telemáticos".

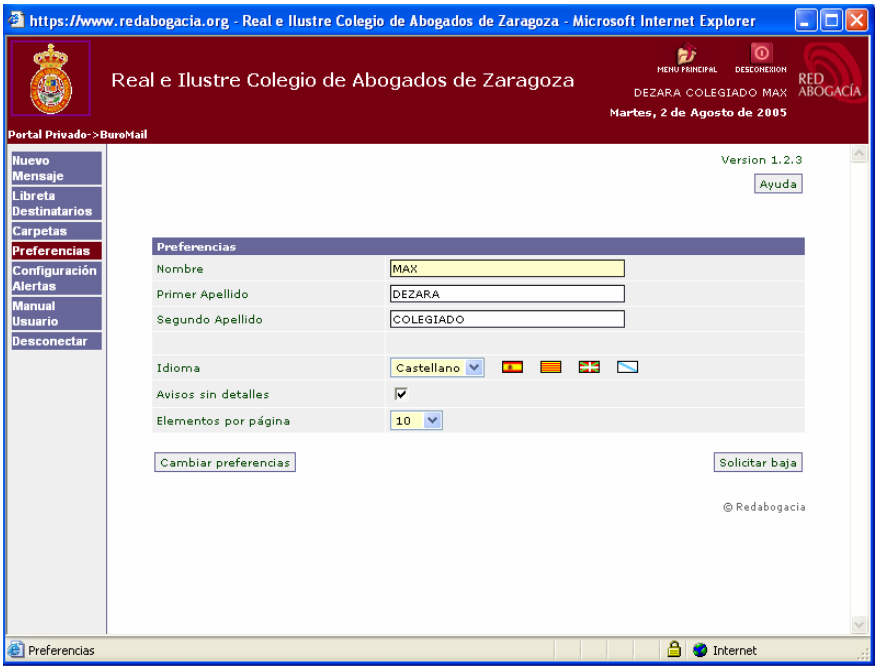
Visualización en detalle del mensaje

En esta página se dispondrá de las opciones de descarga del mensaje completo y de los ficheros adjuntos.

Si el mensaje está cifrado, se realizará una descarga del mensaje para que se pueda visualizar con el cliente de correo Outlook Express.

Preferencias

La función “Preferencias” se utiliza para seleccionar e introducir y aspectos referidos al perfil del usuario.



Los elementos que se pueden configurar son:

- Cambio de idioma
  Este campo indica el idioma en el que se desea recibir los avisos de Redabogacia, dando a elegir al usuario entre varios idiomas.

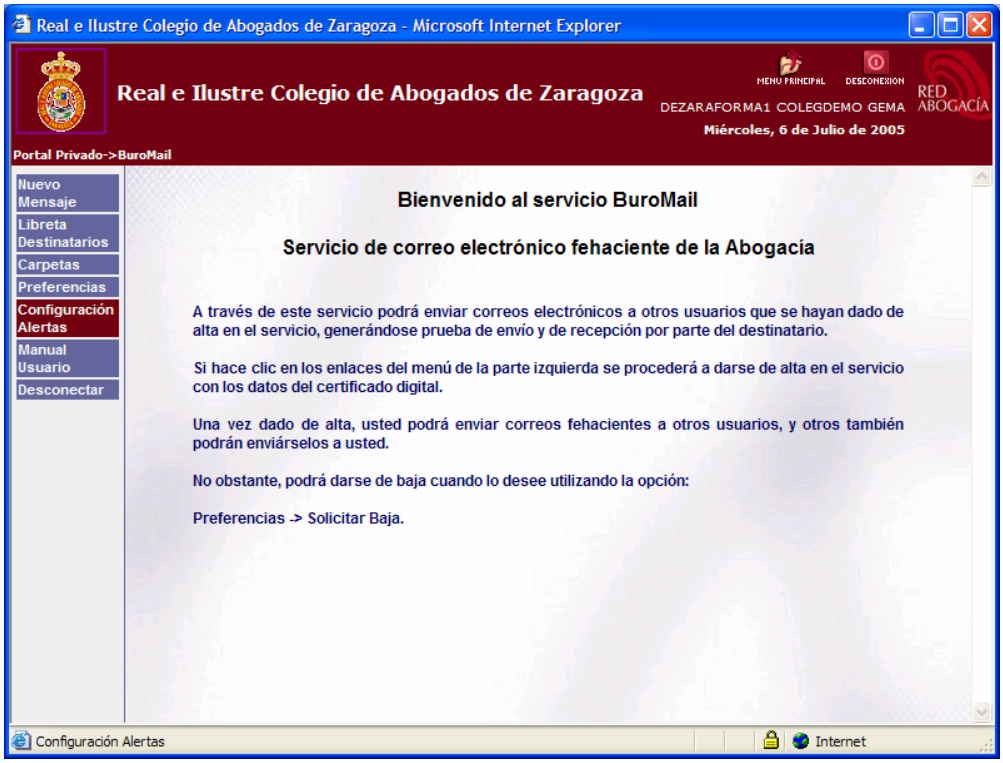
- Avisos confidenciales
  Si se activa esta opción, los avisos recibidos solo pdrán ser abiertos por el interesado con su certificado. Los avisos de recepción por e-mail y SMS no podrán incluir información del contenido.

- Elementos por página
  Con este dato indicaremos el número de avisos a mostrar por página.

- Dispositivos
  En esta sección de la página se mostrarán los diferentes dispositivos de aviso a utilizar, mostrando la información de cada uno.
  En esta pantalla aparece un acceso directo “Ayuda” en la que se explica todo el funcionamiento de esta opción.

Configuración de Alertas

Desde la opción de “Configuración Alertas” del menú izquierdo, es posible la configuración de avisos tanto a su móvil como a cualquier correo electrónico, a fin de avisarle de la recepción de un nuevo mensaje.



Cómo configurar un aviso SMS

Se escoge “Nuevo destino mensaje corto” y se completa la información en el formulario que se no presenta.

En la introducción del número de teléfono ya aparece el prefijo de España (+34) y también el primer dígito del número de móvil (6), por lo tanto sólo sería necesario añadir las últimas 8 cifras de dicho número móvil.

El campo descripción, es para anotar un comentario a este número, por ejemplo: Número del despacho, etc.

Con respecto al tipo de mensaje, lo más usual es tener marcado el segundo tipo, que hace que se reciba una alerta en cuanto entre un nuevo mensaje en nuestra carpeta de “bandeja de entrada”.

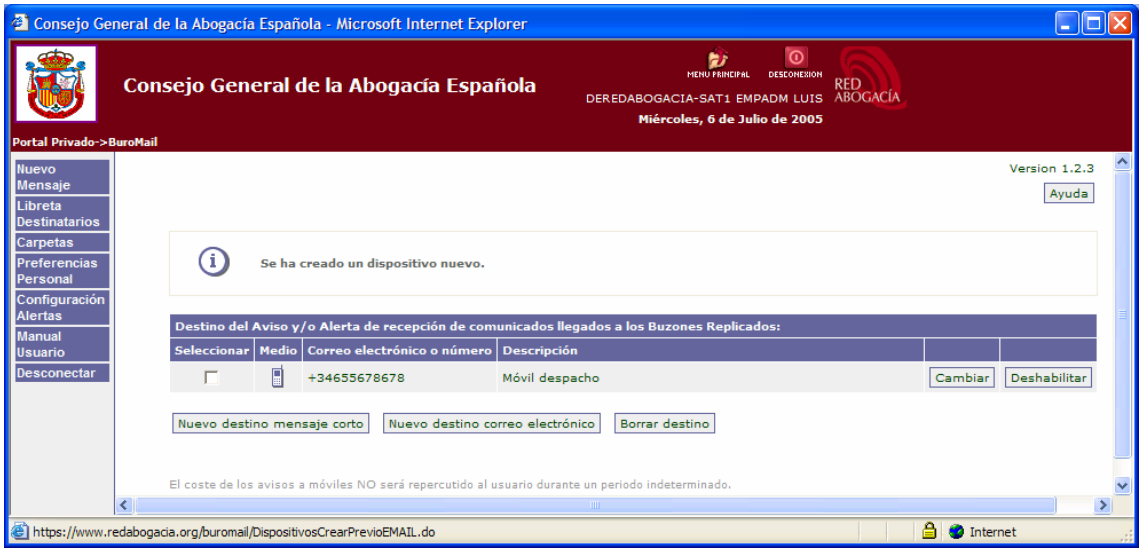
El último campo denominado “Palabras de búsqueda”, se utiliza para filtrar los mensajes por el contenido del ‘Asunto’ del mensaje, y su finalidad es que recibamos sólo las alertas de aquellos mensajes que contengan los caracteres introducidos.

Por último, hacer clic en ‘Crear destino’ concluye el proceso de creación de una alerta SMS.

El proceso se finaliza con la pantalla que se muestra a continuación.

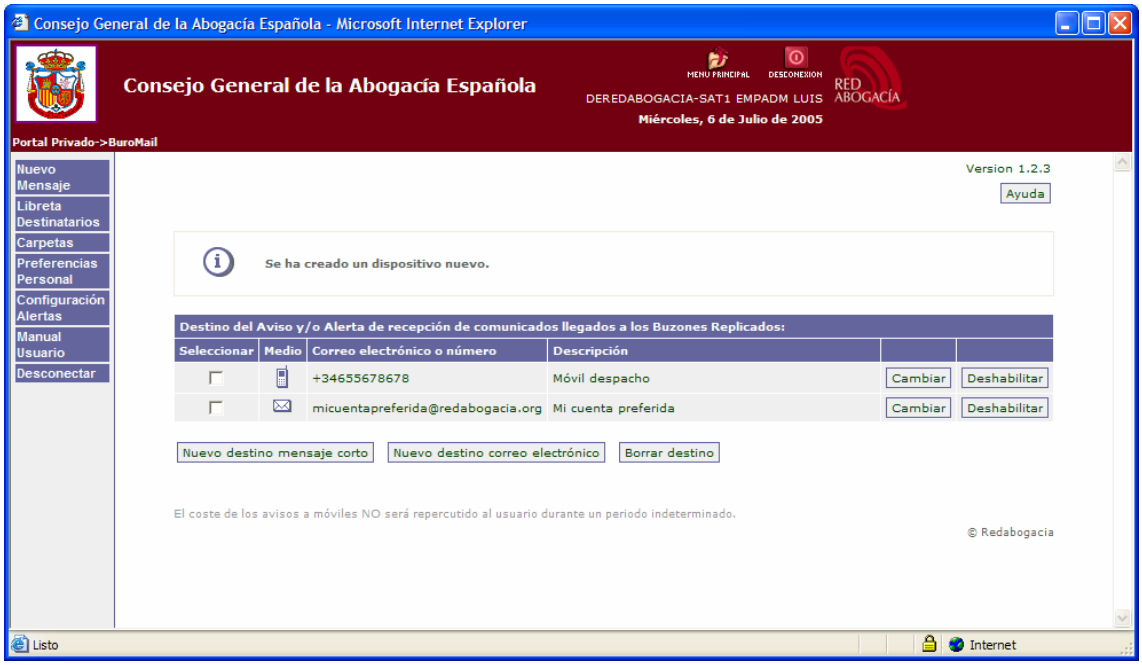
Cómo configurar un aviso al correo electrónico

El procedimiento de la configuración de una alerta en un buzón de correo electrónico sigue un procedimiento similar, en esta ocasión, se hace clic en 'Nuevo destino correo electrónico'.



Se completan los campos de forma similar a como se describe en el procedimiento de crear destino SMS.

Una vez completados los campos, debemos de hacer clic en 'Crear destino' para completar el proceso.



En este momento, ya dispondría de recepción de Alertas tanto por SMS, como por correo electrónico.

Manual de Usuario

Para hacer más fácil la utilización del servicio telemático BuroMail se ha creado un Manual de Usuario en donde se explica paso a paso toda su funcionalidad.

Desconectar

La opción “Desconectar” permite al usuario abandonar el sistema.

Para volver al menú principal basta con hacer clic en el logo del Colegio que se encuentra en la parte superior derecha de la pantalla.

3.6. Práctica: Buromail

Contenido de la práctica:

1. Darse de alta en la aplicación.
2. Enviar una comunicación a otro alumno.
3. Recibir una comunicación de otro alumno.

4. Despedida

4.1. Resumen

En esta sesión habrá hemos tratado los siguientes temas:

- Servicios telemáticos para el ejercicio de la abogacía.
  - Censo general de letrados
  - Pases a Prisión
  - Buromail
- Servicios telemáticos de la Administración Pública.

4.2. Recapitulación módulo

En el módulo intermedio hemos profundizado en algunas de las cuestiones tratadas en el módulo básico y se han introducido temas nuevos. En particular, se han estudiado con detalle algunos servicios telemáticos seguros para el ejercicio de la abogacía.

En este momento, el alumno se encuentra en condiciones de obtener el título "Certificado de usuario avanzado de certificación electrónica".

4.3. En el próximo módulo

En el módulo avanzado continuaremos estudiando nuevos servicios telemáticos seguros para el ejercicio de la abogacía. También trataremos el e-goverment o e-administración y realizaremos un supuesto práctico que integrará los conocimientos adquiridos en los tres módulos.

El módulo avanzado nos permitirá obtener el título "Certificado de Experto en el ejercicio telemático de la Abogacía y servicios de E-Administración".

4.4. Realización telemática del siguiente módulo

En caso de haber solicitado la modalidad online para la realización de los siguientes módulos, deberá acceder al Campus Virtual que se encuentra en la zona privada de su Colegio en el portal Redabogacia.