

Ciudadanos y Pruebas Digitales

Acceso a la Justicia con garantías de igualdad de armas

Guía 3

Consejos sobre cómo actuar y conservar información relevante de las transacciones por internet con fines legales



Esta guía editada por Aedel se encuentra bajo una Licencia Creative Commons Reconocimiento-NoComercial-SinObraDerivada 3.0 Unported.

Esta guía ha sido co-financiada por el Centro de Responsabilidad Social de la Abogacía (CRSA) del Ilustre Colegio de Abogados de Madrid (ICAM) dentro del programa de ayudas a proyectos en apoyo a iniciativas que tengan por objeto la mejora de acceso a la justicia y al mejor cumplimiento de los principios del Estado de Derecho entre colectivos desfavorecidos.



1. ¿Qué es el Centro de Responsabilidad Social de la Abogacía del Ilustre Colegio de Abogados de Madrid?


El Centro de Responsabilidad Social de la Abogacía tiene como objetivo atender a la responsabilidad social del Colegio y de los abogados, promoviendo la mejora, en las Comunidades más necesitadas, del acceso al derecho de defensa y de las condiciones en que éste ha de ejercerse, así como las actuaciones pro bono en servicio del bien común de abogados y despachos.

2. ¿Qué es AEDEL?

La Asociación Española para el Desarrollo de las Evidencias Electrónicas - AEDEL es una organización sin ánimo de lucro que tiene como finalidad estatutaria genérica la promoción, fomento e impulso de todas aquellas medidas que contribuyan al desarrollo del estudio, regulación, confiabilidad y apoyo a la normalización de las Evidencias Electrónicas y la certificación de profesionales.

3. ¿Cuál es el objetivo de esta guía?

En España, al igual que en el resto de Europa y en otras partes del mundo, desde hace varios años y con intensidad creciente, se está trabajando para la información, la sensibilización y la formación de la sociedad en su conjunto, en el uso sin riesgos de Internet y también, aunque con menor énfasis, de la telefonía móvil. La necesidad de esta labor de difusión de los riesgos, así como de los buenos hábitos y derechos, a la ciudadanía en general, y en particular a aquellos colectivos más necesitados de protección como son la infancia, la adolescencia y las víctimas de violencia de género, se hace evidente no sólo por los datos que arrojan los estudios que se realizan y publican al respecto, sino especialmente por el día a día que se vive en los ámbitos cotidianos de los hogares y las aulas.



No obstante todos los estudios publicados hasta la fecha, hacen especial hincapié en los peligros que nos acechan y en las recomendaciones que debemos seguir y casi nada en relación de cómo ejercer nuestros derechos de defensa y absolutamente nada en como presentar las pruebas para posibilitar dicha defensa con garantías de éxito. Pruebas que en gran medida estarán soportadas en los formatos electrónicos que los dispositivos que utilizamos para conectarnos a internet o a la red de telefonía móvil manejan. Las guías objeto de esta acción de Responsabilidad Social de la Abogacía del ICAM aporta información esencial, en este contexto, para el manejo de aquellas evidencias que puedan ser aportadas como prueba de la realización acciones en contra de nuestros derechos.

Así, mediante la coparticipación y cofinanciación del Centro de Responsabilidad Social de la Abogacía y AEDEL, se ha redactado un set de tres guía, del que forma parte la presente, con el objetivo de promover la igualdad de armas y dotar de una defensa real y efectiva a los consumidores y usuarios que efectúan sus transacciones telemáticamente o mediante comunicaciones móviles; menores con acceso a las nuevas tecnologías y herramientas de la Web 2.0; padres y tutores de menores con acceso con acceso a estas tecnologías preocupados por los abusos y robos de identidad de sus hijos; mujeres amenazadas y que sufren violencia de género; y los Abogados y Jueces y Magistrados obligados a enfrentarse a este nuevo reto tecnológico.

Así mismo, se ha desarrollado la herramienta Ad|Quiere, la primera distribución forense gratuita para la comunidad de habla hispana.




4. ¿Qué son las evidencias electrónicas?

En un mundo donde el uso de la redes de comunicaciones es cada vez es más intensivo (móviles, Internet, redes sociales y entornos 2.0 por poner algunos ejemplos) y, por lo tanto, donde las relaciones interpersonales se canalizan a través de medios electrónicos y telemáticos, es lógico que empiece a surgir la necesidad de probar o acreditar las actuaciones legítimas (transferencias bancarias, declaraciones de impuestos....) o las conductas ilícitas de las que somos víctimas (fraudes informáticos como el phishing, acosos a través de redes sociales, amenazas mediante sms) en el formato en que se producen: el electrónico.

Si por evidencia entendemos cualquier dato o información que pueda ser utilizado para determinar o demostrar la veracidad, que prueba un hecho una vez realizado o bien que no ha sido realizado, por evidencia electrónica o prueba electrónica entendemos cualquier evidencia soportada en formato electrónico que permiten archivar y reproducir la palabra, el sonido, la imagen y datos de cualquier otra clase.

Ya no se amenaza mandando anónimos en papel de los que se pueden rastrear matasellos, huellas, papel, o tipo de letra. Ahora se recibe un mensaje en el chat o un sms en donde la componente electrónica generan varios problemas: la manipulación (¿puede un juez estar completamente seguro de que el sms que se le muestra no ha sido manipulado por el receptor?), la volatilidad (se puede borrar, perder, alterar) y cómo llevar ese sms a un proceso con garantías de que no ha sido manipulado ante la justicia o a la comisaría más cercana.

Así que cuando los particulares o las empresas se plantean acudir a la vía litigiosa para zanjar las diferencias que puedan presentarse, han de tener en cuenta que las relaciones presenciales e “inmediatas” están siendo sustituidas por relaciones “entre ausentes” y “mediatas”, donde la prueba de que determinado tipo de actividades han tenido lugar queda registrada en los sistemas informáticos de las compañías y de los particulares.




A la hora de sustanciar ante cualquier jurisdicción una cuestión litigiosa hay que tener presente que para que las pretensiones de las partes prosperen no basta con relatar los hechos acaecidos sino que también hay que desplegar la actividad probatoria necesaria que acredite la veracidad del relato fáctico que se expone.

Esta actividad que puede parecer sencilla es siempre compleja y, cuando intervienen relaciones electrónicas, nos encontramos con problemas específicos por la naturaleza del entorno electrónico. El primero, el ya mencionado de la integridad: quien tenga interés en presentar una prueba que le sea favorable puede aportar ficheros informáticos sobre los que puede recaer la sospecha de manipulación. Esto es así porque la información en formato electrónico no sólo es susceptible de manipulación, sino que esa posible manipulación no necesariamente deja rastro informático.

En un segundo plano, y esto es especialmente relevante cuando el cliente trata con su compañía telefónica o con su banco por Internet, la prueba electrónica es unilateral: la prueba de la existencia y circunstancias de esa relación queda almacenada en los sistemas informáticos a los que se ha accedido, esto es, del banco o administración en el que se acaba de realizar la transacción. Así, el que almacena, podría, a su conveniencia, borrar o alterar los mencionados ficheros según tenga interés en proteger su postura en el proceso judicial, sin que el cliente tenga un elemento de contraste, como sería un extracto bancario emitido por el banco en su propio papel, para demostrar que una determinada operación se ha producido.


Además, muchas veces es difícil, sino imposible, obtener una prueba electrónica de contraste sin una orden judicial que acredite los datos que nosotros como consumidores o víctimas guardamos para demostrar que los hechos que mantenemos se han producido. A nadie se le oculta que, para que ello ocurra, tiene que haber un juez que lo acuerde y que lo haga en un plazo suficientemente breve para que la prueba no haya sido borrada. Aquí nos enfrentamos con uno de los problemas que más afectan al derecho de defensa: por un lado la volatilidad de la prueba y por otra, la lentitud de la justicia. Excepto en macroprocesos, es extremadamente



complicado obtener una respuesta rápida en pleitos de escasa cuantía o de grooming o bullying, acoso entre menores a través de redes sociales sin consecuencias para la integridad física (pero si para la moral, para la que, en ocasiones, los órganos judiciales son poco receptivos).

Así pues, el problema de la complejidad de la verificación de la autenticidad y el riesgo de que el elemento electrónico probatorio esté sólo de una parte, es una de las primeras reflexiones que queremos traer a este texto. Qué ocurriría si, por ejemplo, nuestro banco quien, con la excusa por la protección del medio-ambiente y tras animarnos a que no recibamos los extractos en papel y que hagamos uso de la consulta por internet, pierde nuestros apuntes por un problema técnico o a cause de un desastre o los mismos son manipulados por una actuación malintencionada interna o externa ¿cómo podremos probar nuestras operaciones si nos las discuten? ¿Con una impresión de la web que he podido yo mismo modificar en mi casa con el ordenador personal? ¿Qué le llevo a un Juez?

Para seguir centrado la cuestión, nuestro sistema legal distingue entre la fuentes de prueba (el hecho o situación que ha sucedido) y los medios de prueba, que algunos podrían pensar, en lenguaje informático, que se refiere a los formatos o soportes en que puede ser presentada la fuente de prueba en el proceso judicial. Pensar que, aunque la Ley de Enjuiciamiento Civil lo permita, cualquier formato electrónico es medio de prueba válido es una afirmación errónea. Pensemos, por ejemplo, en una conversación a través de telefonía IP –usando, por ejemplo, el conocido programa Skype- que hemos grabado en el disco duro de nuestro ordenador con una de las múltiples herramientas que permiten la grabación digital de conversaciones en tiempo real realizadas a través de ese programa. Este es un buen ejemplo de lo que es un formato de una evidencia (el fichero en mp3 de la conversación) pero de lo que no puede ser medio de prueba válido, ya que una conversación telefónica grabada sin el consentimiento expreso de ambas partes pueden vulnerar derechos fundamentales.



Por tanto, cuando nos referimos a medios de prueba electrónicos, hemos de considerar no sólo la admisibilidad del formato o soporte sino que la obtención de la prueba no se haya efectuado con infracción de derechos fundamentales. Una vez que la prueba ha llegado al procedimiento, la prueba se valora por el Juez según las normas de la sana crítica. Y aquí surge otro de los problemas de las pruebas electrónicas, la complejidad de su valoración. Las pruebas altamente tecnológicas, requiere del auxilio del perito, formación y cualificación, por cierto, de inexistente control en nuestro país. Mientras que para comprender lo que pone en un papel, el juez no requiere de un software de lectura para desentrañar su contenido, ya que lo lleva incorporado “de serie”, el documento electrónico -entendido en su acepción legal o considerado como un agregado de información electrónica- requiere de un número indeterminado de elementos que son para el juez tan ajenos como el propio documento electrónico: un hardware en el que corre un sistema operativo en el que, a su vez, se ejecuta un programa que permite la apertura y la lectura del documento, así como –en la mayor parte de los casos- su modificación.

Ante la vulnerabilidad y poca confiabilidad de las pruebas o evidencias en formato electrónico y los problemas que plantea una extracción segura y confiable – que requiere una capacitación técnica y unos medios que o bien no se encuentran al alcance de los particulares o bien no con la inmediatez que muchas veces se requiere- nace la necesidad de esta colección de guías sobre recomendaciones y buenas prácticas, destinadas a distintas situaciones y grupos, a la que acompaña un desarrollo informático gratuito para los destinatarios que permite la extracción segura de evidencias de manera sencilla, gratuita y con garantías. **Ad|Quiere**, que así se llama esta herramienta, es una distribución forense on-line completamente gratuita y colaborativa.

Existen muchas distribuciones gratuitas para realizar análisis forenses, pero todas acaban haciéndose de pago o no tienen herramientas suficientes para poder hacer, por ejemplo, adquisiciones en diferentes formatos. Por ello se ha desarrollado Ad|Quiere, la primera distribución forense para la comunidad de habla hispana, que podrá ser usada como complemento a esta guía. En la sección de “Algunas direcciones web que tener a mano” se encuentran todos los detalles de donde descargar esta herramienta y su tutorial.



5. ¿Qué tecnologías usamos? ¿Sabemos realmente como funcionan?

¿Qué pruebas generan?


Las tecnologías de la información nos ofrecen una gran variedad de dispositivos que pueden ser usados para la realización de este tipo de actividades. Recogemos a continuación los más comúnmente usados por los usuarios domésticos, que pueden, a su vez, dar lugar a la prueba electrónica a la que nos referiremos en esta guía.

5.1 Navegación web

Es el método de acceso por excelencia y está basado en el uso de un programa residente en el ordenador del cliente. Un navegador web es un programa de aplicación que te permite acceder a Internet, y en especial al sistema de información World Wide Web, de manera gráfica e intuitiva. Es la ventana que nos comunica con Internet y a través de la que no sólo accedemos a información sino a web transaccionales, de comercio electrónico o de gestiones ante diferentes administraciones.

A pesar de los avances en materia de antivirus, es un programa altamente vulnerable, sobre todo si quien lo usa tiene unos hábitos de navegación poco responsables, pudiendo sufrir todo tipo de ataques informáticos. Ello puede suponer acceder a una falsa página de nuestro banco. También, si se tiene el PC infectado con alguno de los miles de troyanos bancarios que hay en el “mercado” al abrir la página legítima de nuestro banco el troyano “inyectará” código en la página que nos puede hacer facilitar datos al pirata creyendo que se los facilitamos a nuestro banco.

El principal problema evidencial en la prueba generada mediante cualquier navegador es que resulta difícil conservar inalterada la página que queremos guardar como evidencia (la confirmación de una transferencia, de la compra de un billete de avión o de la presentación de una declaración fiscal). En muchos casos no po-



dremos guardar más que un “pantallazo”, la página web completa -que es fácilmente alterable al ser el HTML un estándar abierto-, o una impresión en papel. En algunos casos se genera un correo electrónico de confirmación y en otros un documento en .pdf con mayor o menor seguridad.

5.2 Correo electrónico

Quizás este sea el mecanismo más tradicional y a la vez más cercano a nosotros debido a su uso cotidiano. Hoy por hoy el email es el servicio más popular para comunicarse.

Existen dos formas de lo que comúnmente ha dado en llamarse ‘leer el correo’:

- Mediante un navegador web y acceso a la dirección web del proveedor de correo. También denominado correo web. Los más populares son: Gmail, Hotmail, etc.
- Con un programa de correo que se conecta con el servidor de correo y realiza la descarga de los mensajes a nuestro ordenador. En este modo existen dos modos de funcionamiento:
 - Cada vez que el usuario se conecta, para ver si tiene correo nuevo, se realiza una descarga hacia el ordenador desde donde se conecta, pero en el servidor de correo se sigue almacenando una copia.
 - En la segunda variante, es funcionalmente idéntica a la anterior, salvo que no se guarda copia en el servidor

Los correos electrónicos contienen, junto con el texto del mensaje, la cabecera, el/los documentos adjuntos, otra información no visible relativa a los servidores del remitente, receptor, etc. Esta información se pierde al imprimir el correo electrónico, por lo que resulta recomendable guardar el correo en su formato electrónico para permitir una investigación más exhaustiva.



5.3 Llamadas telefónicas: telefonía móvil, geolocalización, etc

Las llamadas telefónicas se encuentran amparadas por el derecho fundamental al secreto de las comunicaciones y sólo pueden ser grabadas legítimamente si se cuenta con el consentimiento expreso de los participantes, o sin él, mediando orden judicial. En la contratación de servicios o en la presentación de quejas, el ejercicio de derechos ARCO (acceso, rectificación, cancelación y oposición) o la portabilidad del número de teléfono de una compañía a otra, se suelen grabar las conversaciones como prueba de la transacción queja. Tal grabación ha de ser realizada con el consentimiento del cliente o usuario.

5.4 Teléfono móvil / SmartPhone /PDA

El teléfono móvil es un dispositivo inalámbrico electrónico que permite tener acceso a la red de telefonía celular o móvil. Se denomina celular debido a las antenas repetidoras que conforman la red, cada una de las cuales es una célula, si bien existen redes telefónicas móviles satelitales. Su principal característica es su portabilidad, que permite comunicarse desde casi cualquier lugar.

Aunque su principal función es la comunicación de voz, como el teléfono convencional, su rápido desarrollo ha incorporado otras funciones como son cámara fotográfica, agenda, acceso a Internet, reproducción de vídeo e incluso GPS y reproductor mp3.

Un SmartPhone es un dispositivo que reúne las prestaciones de un teléfono móvil y una PDA (ordenador de mano). Por tanto, nos ofrece todas las capacidades multimedia de un móvil asociadas a la posibilidad de trabajar con unos documentos, hojas de cálculo o navegar por Internet.



5.5 Mensajes SMS

SMS (Short Messaging Service) puede ser traducido por servicio de mensajes cortos, o en otras palabras, un mensaje de texto enviado o recibido de o desde un teléfono móvil. Los mensajes son cortos, hasta 160 caracteres, y un teléfono móvil fuera de cobertura o apagado, puede guardar el mensaje hasta que el teléfono esté operativo de nuevo.

El manejo de los SMS es realmente sencillo y esto ha provocado su gran popularidad. Únicamente hay que seleccionar el destinatario por su número de teléfono y teclear el mensaje que le queremos enviar. Después el destinatario recibe un aviso de que ha recibido un mensaje y procede a leerlo.

Normalmente los SMS se originan desde teléfonos móviles, aunque también pueden mandarse desde sitios de Internet o programas de telefonía como Skype.

Los SMS son entregados desde un SMSC (Short Messaging Center) en donde, por obligación legal, se guardan los diversos datos del mensaje pero no el mensaje mismo, lo que supone que el SMS sólo queda en el teléfono del remitente y del receptor, lo que, en caso de disputa sobre su contenido, supone no tener una prueba de tercero que sirva para autenticar el mensaje enviado/recibido.

Dependiendo del tipo de terminal, es posible acceder a los mensajes guardados en la SIM o en la memoria del teléfono, modificarlos y volverlos a mandar.

5.6 Mensajes MMS

MMS quiere decir Servicio de Mensajería Multimedia (Multimedia Messaging Service). Se trata de una versión avanzada del conocido SMS, servicio de mensajes cortos.



La principal diferencia está en que también permite incorporar al texto: imágenes, animaciones y secuencias de vídeo o voz. Además, nos ofrece la posibilidad elegir uno solo de sus elementos o una combinación de ellos.

A diferencia del correo electrónico, las fotos y las secuencias de vídeo no aparecerán como datos adjuntos cuando se envíen a otro teléfono compatible con capacidad para MMS, sino que estarán incorporados en un solo mensaje.

5.7 Documentos .pdf

Pdf un formato de almacenamiento de documentos, desarrollado por la empresa Adobe Systems. Este formato es de tipo compuesto (imagen vectorial, mapa de bits y texto) y está especialmente ideado para documentos susceptibles de ser impresos, ya que especifica toda la información necesaria para la presentación final del documento, determinando todos los detalles de cómo va a quedar, no requiriéndose procesos anteriores de ajuste ni de maquetación.

Es multiplataforma, es decir, puede ser presentado por los principales sistemas operativos (Windows, Unix/Linux o Mac), sin que se modifiquen ni el aspecto ni la estructura del documento original, puede integrar cualquier combinación de texto, elementos multimedia como vídeos o sonido, elementos de hipertexto como vínculos y marcadores, enlaces y miniaturas de páginas, y es uno de los formatos más extendidos en Internet para el intercambio de documentos. Por ello es muy utilizado por empresas, gobiernos e instituciones educativas.

Es una especificación abierta, para la que se han generado herramientas de software libre que permiten crear, visualizar o modificar documentos en formato PDF.

Puede cifrarse para proteger su contenido e incluso firmarlo digitalmente.



El archivo PDF puede crearse desde varias aplicaciones exportando el archivo o generándose desde cualquier aplicación mediante la instalación de una impresora virtual en el sistema operativo, en caso de usar aplicaciones sin esa funcionalidad embebida.

Es el estándar ISO (ISO 19005-1:2005) para ficheros contenedores de documentos electrónicos con vistas a su preservación de larga duración.

Los ficheros PDF son independientes del dispositivo, el mismo archivo puede imprimirse en una impresora de inyección de tinta o una filmadora.



6. Problemas específicos en el ámbito de esta guía

6.1 Relaciones electrónicas con prestadores de servicios de la sociedad de la información y su prueba

La Ley de Servicios de la Sociedad de la Información asegura la validez y eficacia de los contratos que se celebren por vía electrónica, aunque no consten en soporte papel. Se equipara la forma electrónica a la forma escrita y se refuerza la eficacia de los documentos electrónicos como prueba ante los Tribunales, resultando también éstos admisibles en juicio como prueba documental.

Pueden celebrarse por vía electrónica todo tipo de contratos, salvo los relativos al Derecho de familia y sucesiones, por ejemplo adopciones, matrimonio o testamento. Si los contratos deben ir seguidos del cumplimiento de ciertos requisitos formales, como su elevación a escritura pública o su inscripción en algún Registro, dichos requisitos seguirán siendo exigibles para que el contrato sea plenamente válido o eficaz.

El prestador de servicios de la sociedad de la información que lleve a cabo un proceso de contratación electrónica tendrá, en síntesis, las siguientes obligaciones:

1) Antes de iniciar el procedimiento de contratación, deberá poner a disposición del usuario, mediante técnicas adecuadas al medio de comunicación utilizado, de forma permanente, fácil y gratuita, información clara, comprensible e inequívoca sobre:

- Los trámites o pasos que debe seguir para celebrar el contrato.
- Si va a archivar el documento electrónico del contrato y si va ser accesible.
- Los medios técnicos que pone a su disposición para identificar y corregir los errores en la introducción de los datos, antes de confirmarlos.
- La lengua o lenguas en las que puede formalizarse el contrato.
- Las condiciones generales de contratación que, en su caso, rijan el contrato.



La obligación de poner a disposición la información anterior se dará por cumplida si el prestador la incluye en su página o sitio web.

Cuando a los servicios se acceda mediante dispositivos que cuenten con pantallas de formato reducido (ej. móviles) se dará por cumplida la obligación si se facilita la dirección de Internet donde se encuentre dicha información.

2) Celebrado el contrato, el prestador debe:

- Confirmar la recepción de la aceptación, ya sea por medio de un acuse de recibo por correo electrónico u otro medio de comunicación equivalente, ya sea a través de un medio equivalente al utilizado en el procedimiento de contratación.

Las anteriores obligaciones quedan exceptuadas en dos supuestos:

- Cuando hubiera un acuerdo entre las partes en tal sentido y ninguna de ellas tuviera la condición de consumidor
- Cuando el contrato se haya celebrado exclusivamente mediante el intercambio de correo electrónico u otro medio de comunicación electrónica equivalente.

Las obligaciones de los prestadores de servicios que realicen actividades económicas a través de Internet se concretan en dos grupos:

- Obligaciones de información
- Obligaciones en relación con la contratación on-line.

Por lo que se refiere a las obligaciones de información, la empresa debe incluir en su página web información



básica que permita a los usuarios identificar quién es el titular de dicha página. La información básica que se debe facilitar es, en síntesis, la siguiente:

- a)** Su denominación social, NIF, domicilio y dirección de correo electrónico, así como cualquier otro dato que permita una comunicación directa y efectiva, como por ejemplo un teléfono o un número de fax.
- b)** Datos de inscripción, en el caso de que la empresa esté registrada en el Registro Mercantil o en cualquier otro registro público.
- c)** Información sobre el precio de los productos, indicando si incluye o no los impuestos aplicables, gastos de envío y cualquier otro dato que deba incluirse en cumplimiento de normas autonómicas aplicables.
- d)** Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.
- e)** En los casos de que su actividad esté sujeta a autorización previa o ejerza una profesión regulada, deberá informar a los usuarios sobre los siguientes aspectos:
 - Si ejerce alguna profesión regulada (abogado, médico, arquitecto, ingeniero), los datos básicos que acrediten su derecho a ejercer dicha profesión (colegio profesional al que pertenece, número de colegiado, título académico, Estado de la Unión Europea en que se expidió el título académico y, en su caso, la correspondiente homologación).
 - Si su actividad estuviera sujeta a autorización administrativa, los datos de la autorización de que disponga y los identificativos del órgano encargado de su supervisión.
 - Los proveedores de acceso a Internet deben: Informar a sus usuarios sobre los medios técnicos que permitan la protección frente a las amenazas de seguridad en Internet (virus informáticos, programas espías, spam) y sobre las herramientas para el filtrado de contenidos no deseados.
 - Informar a sus clientes sobre las medidas de seguridad que apliquen en la provisión de sus servicios.
 - Informar a sus clientes sobre las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos.

- 
- Los prestadores de servicios de correo electrónico deben: Informar a sus clientes sobre las medidas de seguridad que apliquen en la provisión de sus servicios.

Los prestadores de servicios de intermediación:

- No tienen obligación de supervisar los contenidos que alojan, transmiten o clasifican en un directorio de enlaces, pero deben colaborar con las autoridades públicas cuando se les requiera para interrumpir la prestación de un servicio de la sociedad de la información o para retirar un contenido de la Red.
- No son, en principio, responsables por los contenidos ajenos que transmiten, alojan o a los que facilitan acceso, pero pueden incurrir en responsabilidad si toman una participación activa en su elaboración o si, conociendo la ilegalidad de un determinado material, no actúan con rapidez para retirarlo o impedir el acceso al mismo.

6.2 Relaciones electrónicas con la Administración y su prueba

La Ley 30/1992 de 26 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJAP-PAC), ya en su primera versión recogió (artículo 45) el impulso al empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, por parte de la Administración al objeto de desarrollar su actividad y el ejercicio de sus competencias y de permitir a los ciudadanos relacionarse con las Administraciones cuando fuese compatible con los medios técnicos de que dispongan.

Esa previsión, junto con la de la informatización de registros y archivos del artículo 38 de la misma Ley en su versión originaria y, especialmente, en la redacción que le dio la Ley 24/2001 de 27 de diciembre al permitir el establecimiento de registros telemáticos para la recepción o salida de solicitudes, escritos y comunicaciones por medios telemáticos, abrió el paso a la utilización de tales medios para relacionarse con la Administración.




Simultáneamente, la misma Ley 24/2001 modificó el artículo 59 permitiendo la notificación por medios telemáticos si el interesado hubiera señalado dicho medio como preferente o consentido expresamente.

En el mismo sentido destacan las modificaciones realizadas en la Ley General Tributaria para permitir también las notificaciones telemáticas así como el artículo 96 de la nueva Ley General Tributaria de 2003 que prevé expresamente la actuación administrativa automatizada o la imagen electrónica de los documentos.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos reconoce el derecho de los ciudadanos de acceder electrónicamente a las Administraciones Públicas. Ello genera una serie de problemas, no sólo los derivados de la generación de los expedientes en formato original electrónico, sino el evidencial y probatorio de las gestiones realizadas ante la Administración: dicho expediente debe poder permitir el acceso en línea a los interesados para verificar la situación del expediente, sin mengua de todas las garantías de la privacidad y de prueba.

El hecho de reconocer el derecho de los ciudadanos a comunicarse electrónicamente con la Administración ha planteado la necesidad de definir claramente la sede administrativa electrónica con la que se establecen las relaciones, lo que ha llevado a una reciente marea de publicaciones en el BOE relativa a la constitución de sedes electrónicas de Agencias, Ministerios y demás organismos. Estas sedes se dotan de servicios de seguridad en materia de identificación (firma electrónica, DNI-e), autenticación, contenido mínimo, protección jurídica, accesibilidad, disponibilidad y responsabilidad.

La Ley también ha traído la definición de expediente electrónico y de documento electrónico, de los registros electrónicos y de las notificaciones electrónicas y del alcance y sistemas de sellados de tiempo.



El uso de medios electrónicos no puede significar merma alguna del derecho del interesado en un expediente a acceder al mismo en la forma tradicional, así como tampoco puede suponer un freno o un retraso para que la Administración internamente adopte los mecanismos más adecuados, en este caso medios electrónicos, que le permitan mejorar procesos y reducir el gasto público.

Mediante el Reglamento de desarrollo de esta Ley, se regulan la validez de los documentos y sus copias y la forma de que el documento electrónico opera con plena validez en modo convencional y, en su caso, la forma en que los documentos convencionales se transformen en documentos electrónicos.

Otra cuestión que la Ley aborda es la de las plataformas que pueden utilizar los ciudadanos o las propias Administraciones para establecer tales comunicaciones electrónicas. El ordenador e Internet puede ser una vía, pero no es desde luego la única; las comunicaciones vía SMS pueden ser otra forma de actuación que en algunas Administraciones están siendo ya utilizadas. La Televisión Digital Terrestre, por ejemplo, abre también posibilidades con las que hay también que contar.

La Ley, en todo caso, establece el principio de libertad de los ciudadanos en la elección de la vía o canal por el que quieren comunicarse con la Administración, si bien cada tecnología puede ser apta para una función en razón de sus características y de la fiabilidad y seguridad de sus comunicaciones.

7. ¿Cómo obtener las evidencias electrónicas más habituales?

7.1. Copia en disco de la página visualizada

Una de las formas más fáciles, será sencillamente la de pulsar la opción de imprimir desde el navegador y obtener una copia impresa.

La gran mayoría de los navegadores aporta la impresión y tanto en la cabecera como en el pie de página aportan tanto la fecha y la hora como la url completa del site.

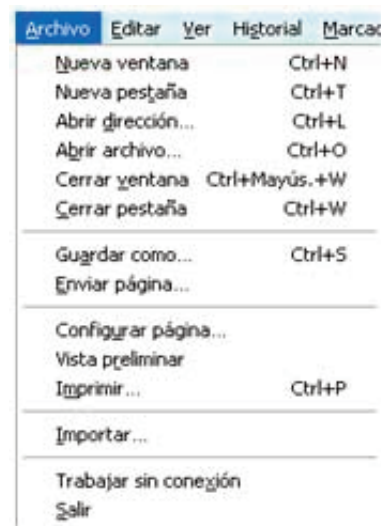
Explorer

Desplegar el menú archivo y Seleccionar la opción Imprimir



Firefox

Desplegar el menú archivo y seleccionar la opción Imprimir



El principal problema de esta obtención la facilidad de alterar el contenido y generar una nueva impresión con el mismo aspecto y contenido.

Otra forma será la de proceder al guardado de la pagina/s visualizada en el navegador, mediante la opción de guardar como disponible tanto en Microsoft Internet Explorer, Firefox, Safari, y etc.

También en este caso la alteración posterior es bastante sencilla.

Explorer

Desplegar el menú archivo y seleccionar la opción Guardar como..., aquí elegiremos como pagina html completa.



FireFox

Desplegar el menú archivo y seleccionar la opción Guardar como..., aquí elegiremos como pagina html completa.





7.2. Obtención de las cabeceras de un correo electrónico en los servicios de correo más populares

¿Qué son esas cabeceras y donde se encuentran?

Al recibir un correo en nuestro buzón lo identificamos mediante los campos De, Asunto y recibido (from, subject y date en el protocolo de correo). Lamentablemente, esta información es fácilmente falsificable y por ello, en ocasiones, se le concede poca fiabilidad, salvo que incorpore algún mecanismo que garantice la identidad del remitente como, por ejemplo, una firma digital. Por ello es conveniente guardar el correo en formato electrónico e intentar aportar otras pruebas que ratifiquen el contenido del correo.

Un mensaje de correo electrónico se compone de una cabecera (header) con los datos identificativos del mensaje y el texto del mensaje denominado cuerpo (body).

Las cabeceras de las que hablamos son líneas de texto insertadas automáticamente por el programa que envía el correo y por cada uno de los servidores de correo por los que va pasando hasta llegar a nuestro buzón. Si no han sido manipuladas, son simplemente una lista de los ordenadores por los que el mensaje ha pasado hasta llegar a ti.

Aunque puedan manipularse con cierta facilidad, el remitente nunca puede falsificar los datos que se insertan automáticamente después de su envío, luego siguiendo la cadena hacia atrás, hasta el momento de la falsificación, siempre se podrá obtener datos muy útiles.

Las cabeceras de mail no son visualizadas por los programas de correo, y por ello para verlas hay que ejecutar determinadas funciones, cada programa/servicio lo visualiza de una forma distinta.



A continuación veremos los más populares.

Outlook 2007:

1. Abra Outlook.
2. Abra el mensaje afectado.
3. En la pestaña Mensaje, en Opciones, haga clic en la imagen de icono Iniciar > cuadro de diálogo.
4. En el cuadro de dialogo Opciones del mensaje, las cabeceras aparecen en el cuadro Cabeceras de Internet.

Para versiones anteriores de Outlook:

1. Abra Outlook.
2. Abra el mensaje cuyas cabeceras desea visualizar.
3. Haga clic en el menú Ver y seleccione Opciones Aparecerán las cabeceras completas en una ventana nueva.

Outlook Express:

1. Abra Outlook Express.
2. Desde la carpeta "Recibidos", localice el mensaje cuyas cabeceras desee visualizar.
3. Haga clic con el botón derecho del ratón en el mensaje y seleccione Propiedades.
4. Abra la pestaña Detalles del cuadro de diálogo. Aparecerán las cabeceras completas en el cuadro de diálogo.

Correo Yahoo

1. Acceda a su cuenta de Correo Yahoo!
2. Abra el mensaje cuyas cabeceras desea visualizar.
3. Haga clic en Encabezado completo en la parte superior de su mensaje. Aparecerán las cabeceras completas sobre el texto del mensaje.

GMail

1. Acceda a su cuenta de Gmail.
2. Abra el mensaje cuyas cabeceras desea visualizar.
3. Haga clic en la flecha ubicada junto a Responder en la parte superior derecha del panel de mensajes.
4. Seleccione Mostrar original. Aparecerán las cabeceras completas en una ventana nueva.

Hotmail

1. Acceda a su cuenta de Hotmail.
2. Haga clic en Opciones junto a las pestañas.
3. Seleccione Correo en el menú izquierdo.
4. Haga clic en Configuración de pantalla de correo.
5. En Encabezados de mensajes, seleccione Avanzado.
6. Haga clic en Aceptar.

Microsoft Internet Mail

1. Acceda a su cuenta de Microsoft Internet Mail.
2. Abra el mensaje cuyas cabeceras desea visualizar.
3. Haga clic en el menú Archivo y seleccione Propiedades.
4. Seleccione la pestaña Detalles para mostrar las cabeceras completas. Aparecerán las cabeceras completas sobre el texto del mensaje.



7.3. Navegación y grabación de las páginas visionadas

Sin ser un método perfecto, se puede optar por guardar un pantallazo, por imprimir la página o por generar un .pdf (para lo que se requiere un programa más avanzado que el mero lector de Acrobat reader).

Hay algunos programas, como ScreenToaster, que es un servicio web que permite generar un vídeo con todas las acciones que se realicen en la pantalla del ordenador, incluida la navegación Web. Aunque no hay versión en español, es muy intuitivo y fácil de manejar.

8. Recomendaciones

Para la obtención de pruebas electrónicas, tan importante es que se generen en un entorno seguro, como que se extraigan y conserven en iguales condiciones. Por eso es importante seguir estas reglas antes y después de que el incidente o hecho a probar se haya producido.

1. Piense antes de actuar: cualquier cosa por pequeña que sea puede servirle.
2. Haga un uso responsable de la tecnología y transmítalo a su entorno.
3. Supervise el uso que de la tecnología se realiza en su nombre.
4. Mantenga siempre evidencia de sus actuaciones (volcado de pantallas, teléfonos móviles, mensajes, etc.)
5. A pesar de la obligación de remitir por escrito los contratos de algunos servicios (los de telecomunicaciones, por ejemplo), cuando realice una transacción, guarde las condiciones generales y particulares que aparecen en la página (normalmente bajo "aviso legal") siguiendo las instrucciones indicadas en la sección 7, para que quede constancia de las que eran de aplicación en el momento de realizar la transacción o firmar el contrato. Los prestadores pueden cambiar las condiciones de contratación sin previo aviso.



6. Guarde los contratos, la documentación acreditativa de la realización de las gestiones ante la administración, los correos electrónicos de confirmación en su formato nativo: pdf, html, etc.
7. Haga copia de seguridad de los documentos referidos en la recomendación anterior
8. En el caso de la factura electrónica, recuerde que las obligaciones incluyen guardar el programa de lectura y que una factura en papel escaneada o impresa en pdf no tiene validez a efectos fiscales.

9. Algunas direcciones que tener a mano

Ad|Quiere. Información general y descarga

<http://aedel.es/2010/04/25/aedel-lanza-con-la-colaboracion-de-blueliv-adquiere>

Privacidad y protección de datos

Agencia de Protección de Datos

www.aepd.es

aedel
asociación española
de evidencias electrónicas

