Tema 4. Comercio electrónico.

4.1. Tienda virtual.

4.2. Firma digital y e-factura.

4.3. Seguridad técnica de e-pagos.

4.4. Internacionalización (soporte de múltiples lenguajes).

4.5. Herramientas para la creación de tiendas virtuales.

4.6. Marco legal del comercio electrónico.

Firma digital (1) (http://www.tuguialegal.com/firmadigital1.htm)

¿Qué es y para qué sirve la firma digital? (1)

Se puede definir la firma digital como una secuencia de datos electrónicos (bits) que se obtienen aplicando a un mensaje determinado un algoritmo de cifrado asimétrico o de clave pública, y que equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje. Desde un punto de vista material, la firma digital es una simple cadena o secuencia de caracteres que se adjunta al final del cuerpo del mensaje firmado digitalmente.

La aparición y desarrollo de las redes telemáticas, de las que internet es el ejemplo más notorio, ha supuesto la posibilidad de intercambiar entre personas distantes geográficamente mensajes de todo tipo, incluidos los mensajes de contenido contractual. Estos mensajes plantean el problema de acreditar tanto la autenticidad como la autoría de los mismos.

Referencia: http://www.tuguialegal.com/firmadigital1.htm

Firma digital (2) (http://www.tuguialegal.com/firmadigital1.htm)

¿Qué es y para qué sirve la firma digital? (2)

Concretamente, para que dos personas (ya sean dos empresarios o un empresario y un consumidor) puedan intercambiar entre ellos mensajes electrónicos de carácter comercial que sean mínimamente fiables y puedan, en consecuencia, dar a las partes contratantes la confianza y la seguridad que necesita el tráfico comercial, esos mensajes deben cumplir los siguientes **requisitos**:

1. **Identidad**, que implica poder atribuir de forma indubitada el mensaje electrónico recibido a una determinada persona como autora del mensaje.

2. **Integridad**, que implica la certeza de que el mensaje recibido por B (receptor) es exactamente el mismo mensaje emitido por A (emisor), sin que haya sufrido alteración alguna durante el proceso de transmisión de A hacia B.

3. **No repudiación** o no rechazo en origen, que implica que el emisor del mensaje (A) no pueda negar en ningún caso que el mensaje ha sido enviado por él.

Referencia: http://www.tuguialegal.com/firmadigital1.htm

Firma digital (3) (http://www.tuguialegal.com/firmadigital1.htm)

¿Qué es y para qué sirve la firma digital? (3)

La firma digital es un procedimiento técnico que basándose en técnicas criptográficas trata de dar respuesta a esa triple necesidad a fin de posibilitar el tráfico comercial electrónico.

Por otra parte, a los tres requisitos anteriores, se une un cuarto elemento, que es la **confidencialidad**, que no es un requisito esencial de la firma digital sino accesorio de la misma.

4. **Confidencialidad** implica que el mensaje no haya podido ser leído por terceras personas distintas del emisor y del receptor durante el proceso de transmisión del mismo.

Referencia: http://www.tuguialegal.com/firmadigital1.htm

Firma digital (4) (http://www.tuguialegal.com/firmadigital2.htm)

¿En qué se basa la firma digital? (1)

La criptografía como base de la firma digital (1)

La firma digital se basa en la **utilización combinada de dos técnicas** distintas, que son la **criptografía asimétrica o de clave pública** para cifrar mensajes y el uso de las llamadas **funciones hash** o funciones resumen.

El diccionario de la Real Academia Española de la Lengua define la **criptografía** como el arte de escribir con clave secreta o de forma enigmática. La criptografía es un conjunto de técnicas que mediante la utilización de algoritmos y métodos matemáticos sirven para cifrar y descifrar mensajes.

La criptografía ha venido siendo utilizada desde antiguo, fundamentalmente con fines militares. Tradicionalmente se ha hablado de **dos tipos** de sistemas criptográficos:

- los **simétricos** o de clave privada y
- los **asimétricos** o de clave pública.

Referencia: http://www.tuguialegal.com/firmadigital2.htm

Firma digital (5) (http://www.tuguialegal.com/firmadigital2.htm)

¿En qué se basa la firma digital? (2)

La criptografía como base de la firma digital (2)

En los **sistemas criptográficos simétricos** las dos personas (A y B) que van a intercambiarse mensajes entre sí utilizan la misma clave para cifrar y descifrar el mensaje. Así, el emisor del mensaje (A) lo cifra utilizando una determinada clave y, una vez cifrado, lo envía a B. Recibido el mensaje, B lo descifra utilizando la misma clave que usó A para cifrarlo. Los sistemas criptográficos simétricos más utilizados son los conocidos con los nombres de DES, TDES y AES.

Los principales **inconvenientes** del sistema simétrico son los siguientes:

- La necesidad de que A (emisor) y B (receptor) se intercambien previamente por un medio seguro la clave que ambos van a utilizar para cifrar y descifrar los mensajes.
- La necesidad de que exista una clave para cada par de personas que vayan a intercambiarse mensajes cifrados entre sí.

Referencia: http://www.tuguialegal.com/firmadigital2.htm

Firma digital (6) (http://www.tuguialegal.com/firmadigital2.htm)

¿En qué se basa la firma digital? (3)

La criptografía como base de la firma digital (3)

Las dos dificultades apuntadas determinan que los sistemas de cifrado simétricos **no sean aptos** para ser utilizados en redes abiertas como internet, en las que confluyen una pluralidad indeterminada de personas que se desconocen entre sí y que en la mayoría de los casos no podrán intercambiarse previamente claves de cifrado por ningún medio seguro.

Referencia: http://www.tuguialegal.com/firmadigital2.htm

Firma digital (7) (http://www.tuguialegal.com/firmadigital2.htm)

¿En qué se basa la firma digital? (4)

La criptografía como base de la firma digital (4)

Los **sistemas criptográficos asimétricos o de clave pública** se basan en el cifrado de mensajes mediante la utilización de un par de claves diferentes (privada y pública), de ahí el nombre de asimétricos, que se atribuyen a una persona determinada y que tienen las siguientes características:

- Una de las claves, la privada, permanece secreta y es conocida únicamente por la persona a quien se ha atribuido el par de claves y que la va a utilizar para cifrar mensajes. La segunda clave, la pública, es, o puede ser, conocida por cualquiera.

- Ambas claves, privada y pública, sirven tanto para cifrar como para descifrar mensajes.

Referencia: http://www.tuguialegal.com/firmadigital2.htm

Firma digital (8) (http://www.tuguialegal.com/firmadigital2.htm)

¿En qué se basa la firma digital? (5)

La criptografía como base de la firma digital (5)

- A partir de la clave pública, que es conocida o puede ser conocida por cualquiera, no se puede deducir ni obtener matemáticamente la clave privada, ya que si partiendo de la clave pública, que es o puede ser conocida por cualquier persona, se pudiese obtener la clave privada, el sistema carecería de seguridad dado que cualquier podría utilizar la clave privada atribuida a otra persona pero obtenida ilícitamente por un tercero partiendo de la clave pública.

El criptosistema de clave pública más utilizado en la actualidad es el llamado RSA, creado en 1978 y que debe su nombre a sus tres creadores (Rivest, Shamir y Adleman).

Referencia: http://www.tuguialegal.com/firmadigital2.htm

Firma digital (9) (http://www.tuguialegal.com/firmadigital2.htm)

¿En qué se basa la firma digital? (6)

La criptografía como base de la firma digital (6)

La utilización del par de claves (privada y pública) implica que A (emisor) cifra un mensaje utilizando para ello su clave privada y, una vez cifrado, lo envía a B (receptor). B descifra el mensaje recibido utilizando la clave pública de A. Si el mensaje descifrado es legible e inteligible significa necesariamente que ese mensaje ha sido cifrado con la clave privada de A (es decir, que proviene de A) y que no ha sufrido ninguna alteración durante la transmisión de A hacia B, porque si hubiera sido alterado por un tercero, el mensaje descifrado por B con la clave pública de A no sería legible ni inteligible. Así se cumplen dos de los requisitos anteriormente apuntados, que son la integridad (certeza de que el mensaje no ha sido alterado) y no repudiación en origen (imposibilidad de que A niegue que el mensaje recibido por B ha sido cifrado por A con la clave privada de éste). El tercer requisito (identidad del emisor del mensaje) se obtiene mediante el uso de **certificados digitales**, que se analizan en otro apartado de esta guía.

Referencia: http://www.tuguialegal.com/firmadigital2.htm

Firma digital (10) (http://www.tuguialegal.com/firmadigital2.htm)

¿En qué se basa la firma digital? (7)

Funciones Hash

Los mensajes que se intercambian pueden tener un gran tamaño, hecho que dificulta el proceso de cifrado. Por ello no se cifra el mensaje entero, sino un resumen del mismo obtenido aplicando al mensaje una función hash.

Partiendo de un mensaje determinado que puede tener cualquier tamaño, dicho mensaje se convierte mediante la función hash en un mensaje con una dimensión fija (generalmente de 160 bits). Para ello, el mensaje originario se divide en varias partes cada una de las cuales tendrá ese tamaño de 160 bits, y una vez dividido se combinan elementos tomados de cada una de las partes resultantes de la división para formar el mensaje-resumen o hash, que también tendrá una dimensión fija y constante de 160 bits. Este resumen de dimensión fija es el que se cifrará utilizando la clave privada del emisor del mensaje.

Referencia: http://www.tuguialegal.com/firmadigital2.htm

Firma digital (11) (http://www.tuguialegal.com/firmadigital2.htm)

¿En qué se basa la firma digital? (8)

Sellos temporales

Finalmente, en el proceso de intercambio de mensajes electrónicos es importante que, además de los elementos o requisitos anteriormente analizados, pueda saberse y establecerse con certeza la fecha exacta en la que se han enviado los mensajes. Esta característica se consigue mediante los llamados **sellos temporales**, o "time stamping", que es una función atribuida generalmente a los Prestadores de Servicios de Certificación mediante la cual se fija la fecha de los mensajes electrónicos firmados digitalmente

Referencia: http://www.tuguialegal.com/firmadigital2.htm

Firma digital (12) (http://www.tuguialegal.com/firmadigital2.htm)

¿En qué se basa la firma digital? (9)

Confidencialidad de los mensajes

En ocasiones, además de garantizar la procedencia de los mensajes electrónicos que se intercambian por medio de internet y la autenticidad o integridad de los mismos, puede ser conveniente garantizar también su confidencialidad. Ello implica tener la certeza de que el mensaje enviado por A (emisor) únicamente será leído por B (receptor) y no por terceras personas ajenas a la relación que mantienen A y B.

En tales casos, también se acude al cifrado del mensaje con el par de claves, pero de manera diferente al mecanismo propio y característico de la firma digital. Para garantizar la confidencialidad del mensaje, el cuerpo del mismo (no el hash o resumen) se cifra utilizando la clave pública de B (receptor), quien al recibir el mensaje lo descifrará utilizando para ello su clave privada (la clave privada de B). De esta manera se garantiza que únicamente B pueda descifrar el cuerpo del mensaje y conocer su contenido.

Referencia: http://www.tuguialegal.com/firmadigital2.htm

Firma digital (13) (http://www.tuguialegal.com/firmadigital3.htm)

Obtención del par de claves y de los certificados digitales (1)

¿Dónde puede obtener una persona el par de claves?

A diferencia de la firma autógrafa, que es de libre creación por cada individuo y no necesita ser autorizada por nadie ni registrada en ninguna parte para ser utilizada, la firma digital, y más concretamente el par de claves que se utilizan para firmar digitalmente los mensajes, no pueden ser creados libremente por cada individuo.

En principio, cualquier persona puede dirigirse a una empresa informática que cuente con los dispositivos necesarios para generar el par de claves y solicitar la creación de dicho par de claves. Posteriormente, con el par de claves creado para una persona determinada, ésta se dirigiría a un Prestador de Servicios de Certificación para obtener el certificado digital correspondiente a ese par de claves.

Sin embargo, en la práctica los Prestadores de Servicios de Certificación cumplen ambas funciones: crean el par de claves (pública y privada) para una persona y expiden el certificado digital correspondiente a ese par de claves.

Referencia: http://www.tuguialegal.com/firmadigital3.htm

Firma digital (14) (http://www.tuguialegal.com/firmadigital3.htm)

Obtención del par de claves y de los certificados digitales (2)

¿Qué son los certificados digitales? (1)

La utilización del par de claves (privada y pública) para cifrar y descifrar los mensajes permite tener la certeza de que el mensaje que B recibe de A y que descifra con la clave pública de A, no ha sido alterado y proviene necesariamente de A. Pero ¿quién es A?.

Para responder de la identidad de A (emisor) es necesario la intervención de un tercero, que son los llamados **Prestadores de Servicios de Certificación**, cuya misión es la de emitir los llamados certificados digitales o certificados de clave pública.

Un **certificado digital** es un archivo electrónico que tiene un tamaño máximo de 2 Kbytes y que contiene los datos de identificación personal de A (emisor de los mensajes), la clave pública de A y la firma privada del propio Prestador de Servicios de Certificación. Ese archivo electrónico es cifrado por la entidad Prestadora de Servicios de Certificación con la clave privada de ésta.

Referencia: http://www.tuguialegal.com/firmadigital3.htm

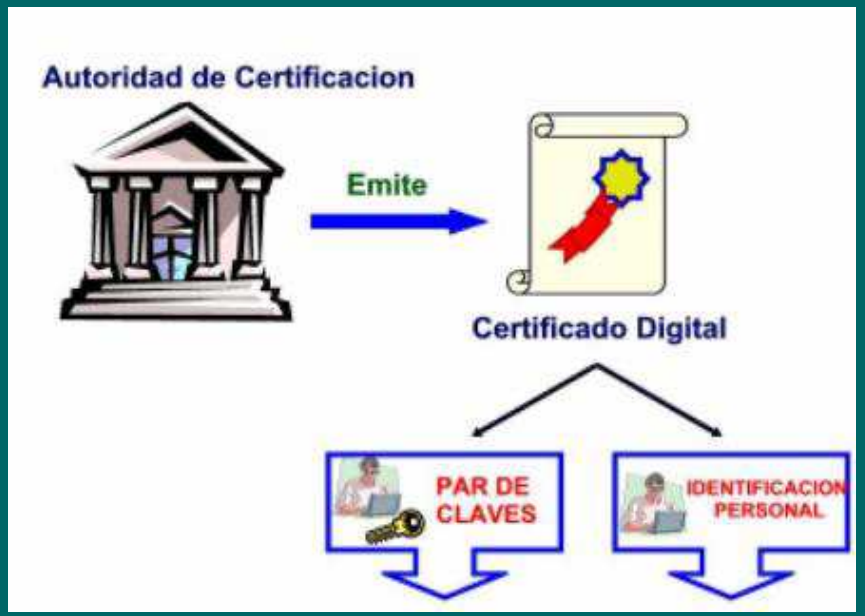
Firma digital (15) (http://www.tuguialegal.com/firmadigital3.htm)

Obtención del par de claves y de los certificados digitales (3)

¿Qué son los certificados digitales? (2)

Los certificados digitales tienen una **duración determinada**, transcurrida la cual deben ser renovados, y pueden ser revocados anticipadamente en ciertos supuestos (por ejemplo, en el caso de que la clave privada, que debe permanecer secreta, haya pasado a ser conocida por terceras personas no autorizadas para usarla).

Gracias al certificado digital, el par de claves obtenido por una persona estará siempre vinculado a una determinada identidad personal, y si sabemos que el mensaje ha sido cifrado con la clave privada de esa persona, sabremos también quién es la persona titular de esa clave privada.



Referencia: http://www.tuguialegal.com/firmadigital3.htm

Firma digital (16) (http://www.tuguialegal.com/firmadigital3.htm)

Obtención del par de claves y de los certificados digitales (4)

¿Cómo obtengo el dispositivo para firmar digitalmente un mensaje? (1)

El **proceso de obtención** de los elementos que necesito para firmar digitalmente mensajes (par de claves y certificado digital) es el siguiente:

1º).- Me dirijo a una empresa o entidad que tenga el carácter de Prestador de Servicios de Certificación y solicito de ellos el par de claves y el certificado digital correspondiente a las mismas. Generalmente, podré acudir a dicha entidad bien personalmente o por medio de internet utilizando la página web del Prestador de Servicios de Certificación.

2º).- El prestador de Servicios de Certificación comprobará mi identidad, bien directamente o por medio de entidades colaboradoras (Autoridades Locales de Registro), para lo cual deberé exhibirle mi D.N.I. y si soy el representante de una sociedad (administrador, apoderado, etc.) o de cualquier otra persona jurídica, deberé acreditar documentalmente mi cargo y mis facultades.

Referencia: http://www.tuguialegal.com/firmadigital3.htm

Firma digital (17) (http://www.tuguialegal.com/firmadigital3.htm)

Obtención del par de claves y de los certificados digitales (5)

¿Cómo obtengo el dispositivo para firmar digitalmente un mensaje? (2)

3º).- El prestador de Servicios de Certificación crea con los dispositivos técnicos adecuados el par de claves pública y privada y genera el certificado digital correspondiente a esas claves.

4º).- El prestador de Servicios de Certificación me entrega una tarjeta semejante a una tarjeta de crédito que tiene una banda magnética en la que están grabados tanto el par de claves como el certificado digital. El acceso al par de claves y al certificado digital grabados en la tarjeta está protegido mediante una clave como las que se utilizan en las tarjetas de crédito o en las tarjetas de cajero automático. En otras ocasiones, en lugar de la tarjeta el Prestador de Servicios de Certificación deja almacenado el certificado digital en su propia página web, a fin de que el destinatario copie el archivo y lo instale en su ordenador.

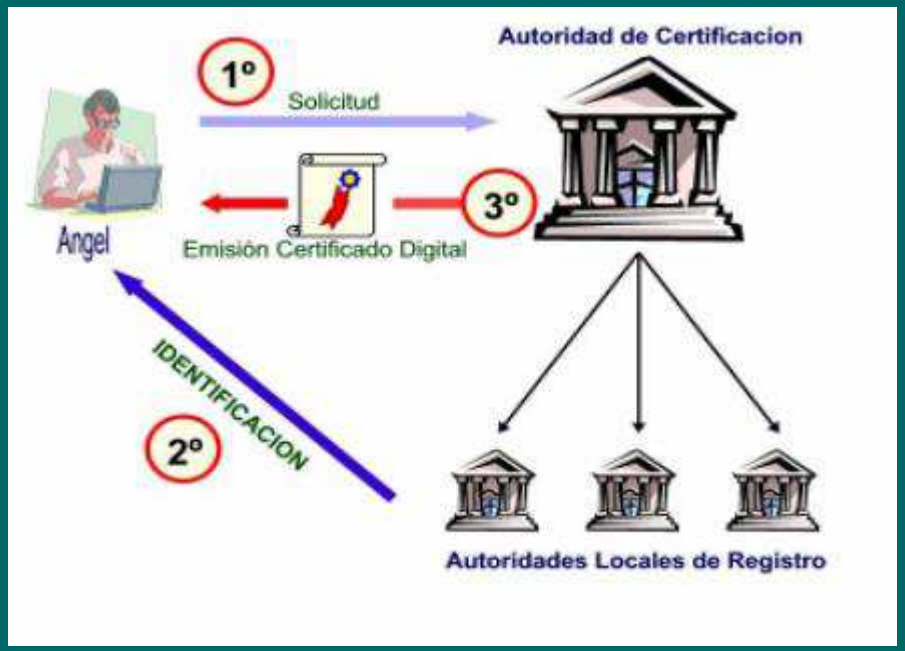
Referencia: http://www.tuguialegal.com/firmadigital3.htm

Firma digital (18) (http://www.tuguialegal.com/firmadigital3.htm)

Obtención del par de claves y de los certificados digitales (6)

¿Cómo obtengo el dispositivo para firmar digitalmente un mensaje? (3)

5º).- Con esa tarjeta magnética y un lector de bandas magnéticas adecuado conectado a mi ordenador personal, podré leer y utilizar la información grabada en la tarjeta para firmar digitalmente los mensajes electrónicos que envíe a otras personas.



Referencia: http://www.tuguialegal.com/firmadigital3.htm

Firma digital (19) (http://www.tuguialegal.com/firmadigital4.htm)

¿Cómo funciona la firma digital? (1)

El proceso de firma digital de un mensaje electrónico comprende en realidad dos procesos sucesivos:

- la firma del mensaje por el emisor del mismo, y
- la verificación de la firma por el receptor del mensaje.

Esos dos procesos tienen lugar de la manera que se expresa a continuación, en la que el emisor del mensaje es designado como **Ángel** y el receptor del mensaje es designado como **Blanca**

Referencia: http://www.tuguialegal.com/firmadigital4.htm

Firma digital (20) (http://www.tuguialegal.com/firmadigital4.htm)

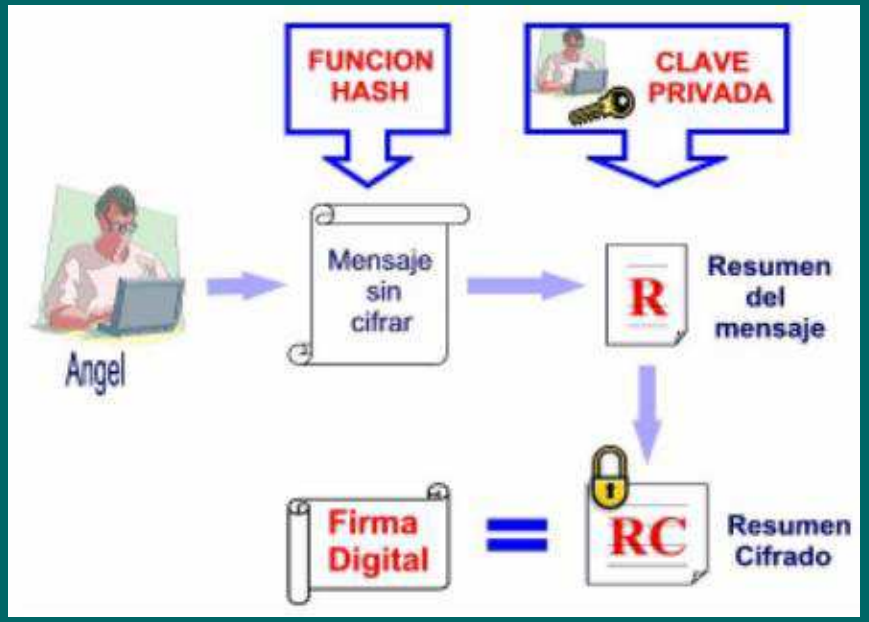
¿Cómo funciona la firma digital? (2)

Firma digital de un mensaje electrónico (1)

1º.- Ángel (emisor) crea o **redacta un mensaje** electrónico determinado (por ejemplo, una propuesta comercial).

2º.- El emisor (Ángel) aplica a ese mensaje electrónico una **función hash** (algoritmo), mediante la cual obtiene un resumen de ese mensaje.

3º.- El emisor (Angel) **cifra ese mensaje-resumen** utilizando su clave privada.



Referencia: http://www.tuguialegal.com/firmadigital4.htm

Firma digital (21) (http://www.tuguialegal.com/firmadigital4.htm)

¿Cómo funciona la firma digital? (3)

Firma digital de un mensaje electrónico (2)

4º.- Ángel envía a **Blanca** (receptor) un correo electrónico que contiene los siguientes elementos:

- El **cuerpo** del mensaje, que es el mensaje en claro (es decir, sin cifrar). Si se desea mantener la confidencialidad del mensaje, éste se cifra también pero utilizando la clave pública de Blanca (receptor).

- La **firma** del mensaje, que a su vez se compone de dos elementos:

  1. El **hash** o mensaje-resumen cifrado con la clave privada de Angel.

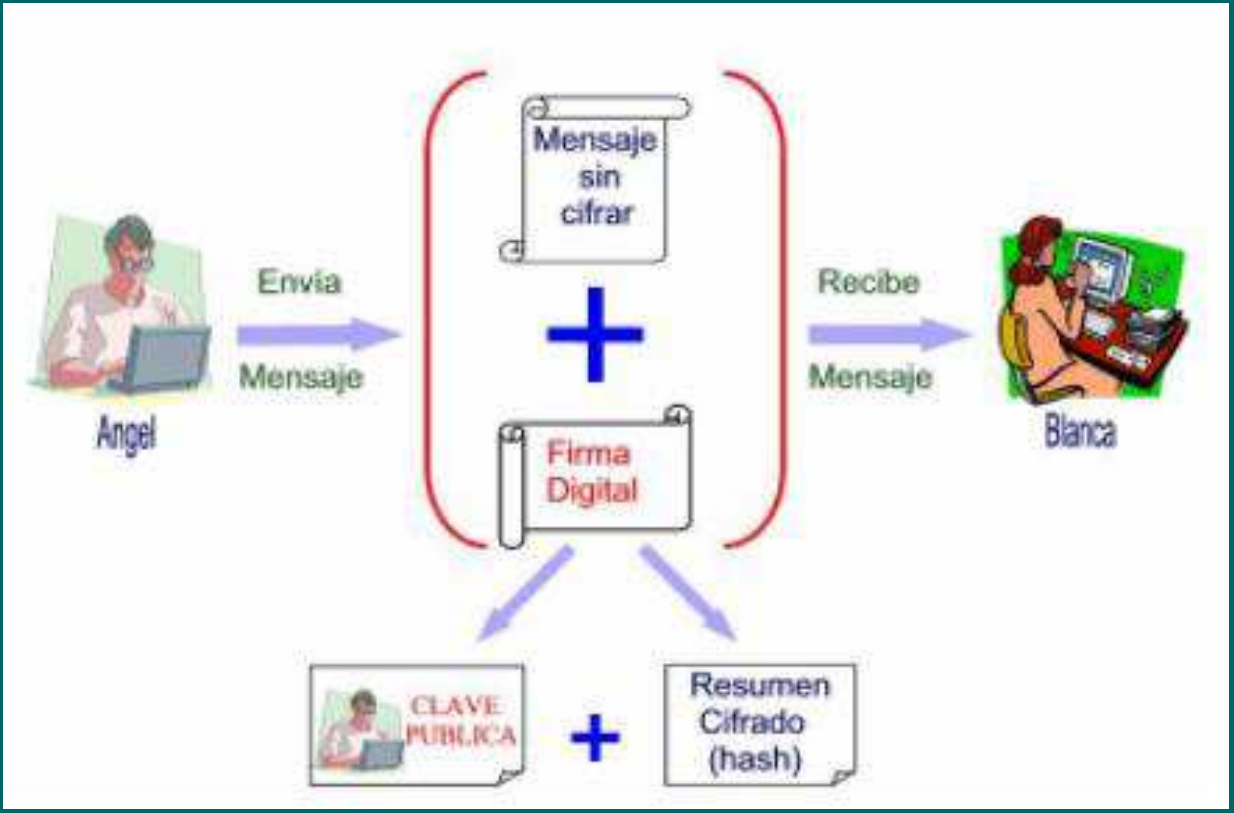
  2. El **certificado digital** de Angel, que contiene sus datos personales y su clave pública, y que está cifrado con la clave privada del Prestador de Servicios de Certificación.

Referencia: http://www.tuguialegal.com/firmadigital4.htm

Firma digital (22) (http://www.tuguialegal.com/firmadigital4.htm)

¿Cómo funciona la firma digital? (4)

Firma digital de un mensaje electrónico (3)



Referencia: http://www.tuguialegal.com/firmadigital4.htm

Firma digital (23) (http://www.tuguialegal.com/firmadigital4.htm)

¿Cómo funciona la firma digital? (5)

Verificación por el receptor de la firma digital del mensaje (1)

1º.- Blanca (receptor) recibe el correo electrónico que contiene todos los elementos mencionados anteriormente.

2º.- Blanca en primer lugar **descifra el certificado digital** de Ángel incluido en el correo electrónico, utilizando para ello la clave pública del Prestador de Servicios de Certificación que ha expedido dicho certificado. Esa clave pública la tomará Blanca, por ejemplo de la página web del Prestador de Servicios de Certificación en la que existirá depositada dicha clave pública a disposición de todos los interesados.

3º.- Una vez descifrado el certificado, Blanca podrá acceder a la clave pública de Ángel, que era uno de los elementos contenidos en dicho certificado. Además podrá saber a quién corresponde dicha clave pública, dado que los datos personales del titular de la clave (Ángel) constan también en el certificado.

Referencia: http://www.tuguialegal.com/firmadigital4.htm

Firma digital (24) (http://www.tuguialegal.com/firmadigital4.htm)

¿Cómo funciona la firma digital? (6)

Verificación por el receptor de la firma digital del mensaje (2)

4º.- Blanca utilizará la clave pública del emisor (Ángel) obtenida del certificado digital para **descifrar el hash** o mensaje-resumen creado por **Ángel**.

5º.- Blanca **aplicará al cuerpo del mensaje**, que aparece en claro o no cifrado, que también figura en el correo electrónico recibido, la misma **función hash** que utilizó **Ángel** con anterioridad, obteniendo igualmente **Blanca** un mensaje-resumen. Si el cuerpo del mensaje también ha sido cifrado para garantizar la confidencialidad del mismo, previamente **Blanca** deberá descifrarlo utilizando para ello su propia clave privada (recordemos que el cuerpo del mensaje había sido cifrado con la clave pública de **Blanca**)

Referencia: http://www.tuguialegal.com/firmadigital4.htm

Firma digital (25) (http://www.tuguialegal.com/firmadigital4.htm)

¿Cómo funciona la firma digital? (7)

Verificación por el receptor de la firma digital del mensaje (3)

6º.- Blanca comparará el mensaje-resumen o hash recibido de **Ángel** con el mensaje-resumen o hash obtenido por ella misma. Si ambos mensajes-resumen o hash coinciden totalmente significa lo siguiente:

- El mensaje no ha sufrido alteración durante su transmisión, es decir, es íntegro o auténtico.
- El mensaje-resumen descifrado por Blanca con la clave pública de Ángel ha sido necesariamente cifrado con la clave privada de Ángel y, por tanto, proviene necesariamente de Ángel.
- Como el certificado digital nos dice quién es Ángel, podemos concluir que el mensaje ha sido firmado digitalmente por Ángel, siendo Ángel una persona con identidad determinada y conocida.

Referencia: http://www.tuguialegal.com/firmadigital4.htm

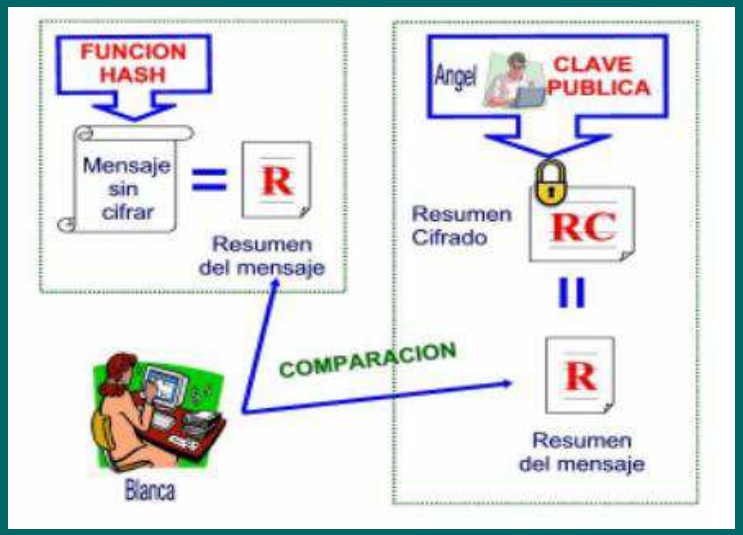
Firma digital (26) (http://www.tuguialegal.com/firmadigital4.htm)

¿Cómo funciona la firma digital? (8)

Verificación por el receptor de la firma digital del mensaje (4)

6º (continuación)**.-** Por el contrario, si los mensajes-resumen no coinciden quiere decir que el mensaje ha sido alterado por un tercero durante el proceso de transmisión, y si el mensaje-resumen descifrado por Blanca es ininteligible quiere decir que no ha sido cifrado con la clave privada de Ángel. En resumen, que el mensaje no es auténtico o que el mensaje no ha sido firmado por Ángel sino por otra persona.

Finalmente, hay que tener en cuenta que las distintas fases del proceso de firma y verificación de una firma digital que han sido descritas no se producen de manera manual sino automática e instantánea, por el simple hecho de introducir la correspondiente tarjeta magnética en el lector de tarjetas de nuestro ordenador y activar el procedimiento.



Referencia: http://www.tuguialegal.com/firmadigital4.htm

Firma digital (27) (http://www.ugr.es/pages/administracion/registro/normativa/normativa_aplicable

Normativa General aplicable (1)

Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (BOE nº 285 de 27 de Noviembre de 1.992).

Ley 4/1999 de 13 de enero de modificación de la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica (B.O.E. de 18 de septiembre de 1999).

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. de 14 de diciembre de 1999).

Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos (B.O.E. de 28 de febrero de 2003).

Referencia: http://www.ugr.es/pages/administracion/registro/normativa/normativa_aplicable

Firma digital (28) (http://www.ugr.es/pages/administracion/registro/normativa/normativa_aplicable

Normativa General aplicable (2)

Orden PRE/1551/2003, de 10 de junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos (B.O.E. de 13 de junio de 2003).

Decreto 183/2003, de 24 de junio, por el que se regula la información y atención al ciudadano y la tramitación de procedimientos administrativos por medios electrónicos.

Ley 59/2003, de 19 de diciembre, de firma electrónica (B.O.E. de 20 de diciembre de 2003).

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (B.O.E. de 23 de junio de 2007).

Referencia: http://www.ugr.es/pages/administracion/registro/normativa/normativa_aplicable

Firma digital (29)

Más información:

http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/FirmaElectronica.aspx#contenido

e-Factura (1) (http://www.facturae.es/es-ES/Aspectos/Paginas/Index.aspx)

¿Qué es la factura electrónica? (1)

La facturación electrónica es un equivalente funcional de la factura en papel y consiste en la transmisión de las facturas o documentos análogos entre emisor y receptor por medios electrónicos (ficheros informáticos) y telemáticos (de un ordenador a otro), firmados digitalmente con certificados reconocidos.

Colaboran

Fundetec · AECOC · AMETIC · centro de cooperación interbancaria · OASIS · UBL

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/Index.aspx

e-Factura (2) (http://www.facturae.es/es-ES/Aspectos/Paginas/Index.aspx)

¿Qué es la factura electrónica? (2)

El Anteproyecto de Ley de Medidas de Impulso de la Sociedad de la Información define la factura electrónica como "**un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la autenticidad de su origen y la integridad de su contenido, lo que permite atribuir la factura a su obligado tributario emisor**".

De esta definición extendida en todo el mercado, se transmite tres condicionantes para la realización de e-Factura:

- Se necesita un **formato electrónico** de factura de mayor o menor complejidad (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg o txt, entre otros).
- Es necesario una **transmisión telemática** (tiene que partir de un ordenador, y ser recogida por otro ordenador).
- Este formato electrónico y transmisión telemática, deben **garantizar su integridad y autenticidad a través de una firma electrónica reconocida**.

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/Index.aspx

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

e-Factura (3) (http://www.facturae.es/es-ES/Aspectos/Paginas/Index.aspx)

¿Qué es la factura electrónica? (3)

El artículo 3.3 de la Ley 59/2003 de 19 de diciembre define la firma electrónica reconocida como:

"la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma".

Es decir, se tienen que dar tres condicionantes para que se de la firma electrónica reconocida:

1. Que sea una firma electrónica avanzada.
2. Que esté basada en un certificado reconocido, siendo certificado reconocido aquél que "cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes".
3. Que sea generada mediante un dispositivo seguro de creación de firma, es decir aquel que ofrece, al menos, las siguientes garantías:

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/Index.aspx

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

e-Factura (4) (http://www.facturae.es/es-ES/Aspectos/Paginas/Index.aspx)

¿Qué es la factura electrónica? (4)

- Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.
- 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.
- Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.
- 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." (Art. 24.3)

Por último y para que tuviera la facturación electrónica la misma validez legal que una factura en papel, se necesita el consentimiento de ambas partes (emisor y receptor).

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/Index.aspx

e-Factura (5) (http://www.facturae.es/es-ES/Aspectos/Paginas/Requisitos.aspx)

Requisitos de todas las facturas (1)

Adicionalmente, y como requisito de todas las facturas independientemente de cómo se transmitan, en papel o en formato electrónico, el artículo 6 del RD 1496/2003 que regula el contenido de una factura establece que **los campos obligatorios de una factura** son:

- Núm. Factura
- Fecha expedición
- Razón Social emisor y receptor
- NIF emisor y "receptor"
- Domicilio emisor y receptor
- Descripción de las operaciones (base imponible)
- Tipo impositivo
- Cuota tributaria
- Fecha prestación del servicio (si distinta a expedición)

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/Requisitos.aspx

e-Factura (6) (http://www.facturae.es/es-ES/Aspectos/Paginas/Requisitos.aspx)

Requisitos de todas las facturas (2)

Para cumplir con la norma y que una factura electrónica tenga la misma validez legal que una emitida en papel, el documento electrónico que la representa debe contener los campos obligatorios exigibles a toda factura, estar firmado mediante una firma electrónica avanzada basado en certificado reconocido y ser transmitido de un ordenador a otro recogiendo el consentimiento de ambas partes.

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/Requisitos.aspx

e-Factura (7) (http://www.facturae.es/es-ES/Aspectos/Paginas/ObligacionesExpedidor.aspx)

Reglamento sobre Facturación Electrónica

Obligaciones legales para el expedidor (1)

1. **Consentimiento verbal o escrito del destinatario.-** La Orden 962/2007, de 10 de abril, desarrolla determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas, contenidas en el Real Decreto 1496/2003, que es el Reglamento de Facturación. Al respecto del consentimiento del destinatario, se encuentra recogido en el Artículo 2 de la citada Orden, donde dice que el consentimiento podrá formularse de forma expresa por cualquier medio, verbal o escrito.

2. **Creación de la factura.- Mediante una aplicación informática**, con los contenidos obligatorios mínimos requeridos.

3. **Firma electrónica reconocida**

4. **Remisión telemática**

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/ObligacionesExpedidor.aspx

e-Factura (8) (http://www.facturae.es/es-ES/Aspectos/Paginas/ObligacionesExpedidor.aspx)

Obligaciones legales para el expedidor (2)

5. **Conservación de copia o matriz de la Factura.-** Esta obligación se regula en el artículo 1 del RD 1496/2003, donde se especifica la obligación de expedir, entregar y conservar facturas.

   También han existido dudas sobre si las facturas electrónicas pueden emitirse en copia o sólo se debe guardar la matriz. Al respecto la Agencia Tributaria lo ha aclarado en el borrador antes citado (Art. 5) con la siguiente definición:

   "**Se entiende por Matriz de una factura (...) un conjunto de datos, tablas, base de datos o sistemas de ficheros que contienen todos los datos reflejados en las facturas junto a los programas que permitieron la generación de las facturas....**

6. **Contabilización y anotación en registros de IVA**

7. **Conservación durante el período de prescripción**

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/ObligacionesExpedidor.aspx

e-Factura (9) (http://www.facturae.es/es-ES/Aspectos/Paginas/ObligacionesExpedidor.aspx)

Obligaciones legales para el expedidor (3)

8. **Garantía de accesibilidad completa.-** Deber de gestionar las facturas de modo que se garantice una accesibilidad completa:

   - visualización,
   - búsqueda selectiva,
   - copia o
   - descarga en línea e impresión.

   Esta es una obligación inherente a la conservación de las facturas por medios electrónicos que el legislador denomina acceso completo a datos, tratando de facilitar la auditoria e inspección de las facturas electrónicas. (Articulo 9 del RD 1496/2003)

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/ObligacionesExpedidor.aspx

e-Factura (10) (http://www.facturae.es/es-ES/Aspectos/Paginas/ObligacionesExpedidor.aspx)

Obligaciones legales para el expedidor (4)

9. **Subcontratación a un tercero.-** Todas las fases anteriores pueden ser subcontratadas a un tercero, sin perder su responsabilidad.

   Regulado en el artículo 5.1 del RD 1496/2003 el legislador deja claro en ese mismo párrafo que, aunque se permite la subfacturación a terceros, es el obligado tributario el responsable de cumplir todas estas obligaciones.

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/ObligacionesExpedidor.aspx

e-Factura (11) (http://www.facturae.es/es-ES/Aspectos/Paginas/ObligacionesDestinatario.aspx)

Obligaciones legales para el destinatario (1)

1. Recepción de la factura por medio electrónico.-

- Verificación de los contenidos mínimos exigibles y
- Verificación segura de la firma electrónica.

Regulado en el artículo 21 e inherente a las obligaciones de la conservación de las facturas electrónicas se indica que:

"el destinatario se debe asegurar de la legibilidad en el formato original en el que se haya recibido, así como, en su caso, de los datos asociados y mecanismo de verificación de firma".

A diferencia del emisor, al que se permite construir la factura desde la matriz, el destinatario debe conservar los originales firmados.

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/ObligacionesDestinatario.aspx

e-Factura (12) (http://www.facturae.es/es-ES/Aspectos/Paginas/ObligacionesDestinatario.aspx)

Obligaciones legales para el destinatario (2)

2. **Contabilización y anotación en registros de IVA**

3. **Conservación durante el período de prescripción**

4. **Deber de gestionar las facturas de modo que se garantice una accesibilidad completa**

   - visualización,
   - búsqueda selectiva,
   - copia o
   - descarga en línea e impresión.

5. **Todas las fases anteriores puede subcontratarlas a un tercero, sin perder su responsabilidad**

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/ObligacionesDestinatario.aspx

e-Factura (13) (http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx)

Enlaces de interés

- Ministerio de Industria, Energía y Turismo
- La e-factura de la Agencia Tributaria
- Asociación Centro de Cooperación Interbancaria (CCI)
- Congreso de Factura Electrónica y Digitalización Certificada
- Northern European Subset
- UNeDocs internacional document set

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx

e-Factura (14) (**http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx**)

Documentación (1) (http://www.facturae.es/es-ES/Documentacion/Paginas/index.aspx)

1. Esquema Formato Facturae
2. Políticas de Firma
3. Normativa
4. Análisis y Estudios

1.- Esquema Formato Facturae
(http://www.facturae.es/es-ES/Documentacion/EsquemaFormato/Paginas/Index.aspx)

Versión 3.2

- Esquema v 3.2 [XSD] [172,94 KB]
- Tabla de campos en español [PDF] [146,52 KB]
- Tabla de campos en inglés [PDF] [152,45 KB]

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx

e-Factura (15) (**http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx**)

Documentación (2) (http://www.facturae.es/es-ES/Documentacion/Paginas/index.aspx)

2.- Políticas de Firma
(http://www.facturae.es/es-ES/Documentacion/Politicas/Paginas/Index.aspx)

Versión 3.1.

- Política Firma v3.1 [PDF] [39,93 KB]
- Política Firma_v3_1_sha1 Formato [< 1 Kb] [TXT] [28 Bytes]
- Política Firma_v3_1_sha2 Formato [< 1 Kb] [TXT] [44 Bytes]
- Política Firma_v3_1_md5 Formato [< 1 Kb] [TXT] [24 Bytes]

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx

e-Factura (16) (**http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx**)

Documentación (3) (http://www.facturae.es/es-ES/Documentacion/Paginas/index.aspx)

3.- Normativa (1)
(http://www.facturae.es/es-ES/Documentacion/Normativa/Paginas/Leyes.aspx)

- Leyes
- Proyectos de Ley
- Factura Electrónica
- Firma Electrónica

Esquema del ámbito de aplicación y plazos de entrada en vigor [PDF] [26 Kb]

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx

e-Factura (17) (**http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx**)

Documentación (4) (http://www.facturae.es/es-ES/Documentacion/Paginas/index.aspx)

3.- Normativa (2)
(http://www.facturae.es/es-ES/Documentacion/Normativa/Paginas/Leyes.aspx)

Otras Leyes

- Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público (BOE 16-11-2011) [ZIP [815,96 KB]
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso a la Sociedad de la Información [PDF] [527,26 KB]
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos [PDF] [532,58 KB]
- Ley 30/2007, de 30 de octubre, de Contratos del Sector Público [PDF] [735,71 KB]

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx

e-Factura (18) (**http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx**)

Documentación (5) (http://www.facturae.es/es-ES/Documentacion/Paginas/index.aspx)

4.- Análisis y Estudios
(http://www.facturae.es/es-ES/Documentacion/Paginas/Analisis.aspx)

- Estudio de la facturación electrónica [PDF] [1,14 MB]
- Análisis y Estudio del Formato Normalizado de la eFactura [PDF] [429,99 KB]

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx

e-Factura (18) (http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx)

Descargas (http://www.facturae.es/ES-ES/DESCARGAS/Paginas/index.aspx)

En esta página puede acceder a la información sobre **descargas de aplicaciones, utilidades y componentes de la Factura Electrónica**.

- Utilidades Facturae
- Aplicación de Gestión de Facturación Electrónica
- Desarrollo

GOBIERNO DE ESPAÑA | MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Referencia: http://www.facturae.es/es-ES/Aspectos/Paginas/Enlaces.aspx