# Facturación electrónica

Josep Lluís Ferrer Gomila
Llorenç Huguet Rotger
M. Magdalena Payeras Capellà

PID_00199788

UOC
Universitat Oberta de Catalunya

# Índice

# Introducción

**Observación**

La factura electrónica tiene la misma validez legal que la factura emitida en papel.

La facturación electrónica se prevé, desde el 2007, como uno de los objetivos de la Ley de Medidas de Impulso de la Sociedad de la Información (LISI, 56/2007) y traslada a las empresas el reto de su implantación. Esta ley define la factura electrónica como: "un documento electrónico que cumple los requisitos exigibles legal y reglamentariamente a las facturas y que, además, garantiza la autenticidad del origen y la integridad del contenido de la factura, lo que impide que el emisor la rechace".

La empresa del siglo XXI se debe adaptar al desarrollo de las tecnologías de la información para situarse en el centro de la sociedad de la información; en ella, Internet les ofrece a las empresas muchos servicios que permiten trabajar telemáticamente y, gracias al impulso normativo que da cobertura jurídica, de una manera más profesional, flexible y dinámica; y, al mismo tiempo, les brinda un ahorro de tiempo y de costes de gestión documental bastante significativo.

Desde siempre, una factura es el justificante fiscal del pago de un producto o de la provisión de un servicio, que afecta al obligado tributario emisor (el vendedor) y al obligado tributario receptor (el comprador). Tradicionalmente es un documento en papel, cuyo original debe ser archivado por el receptor de la factura. Habitualmente, el emisor de la factura conserva una copia o la matriz, en la que se registra su emisión.

Este es un proceso basado en la manipulación de una gran cantidad de papeles que, junto con su proceso contable manual, suponen un lastre para la competitividad de la empresa.

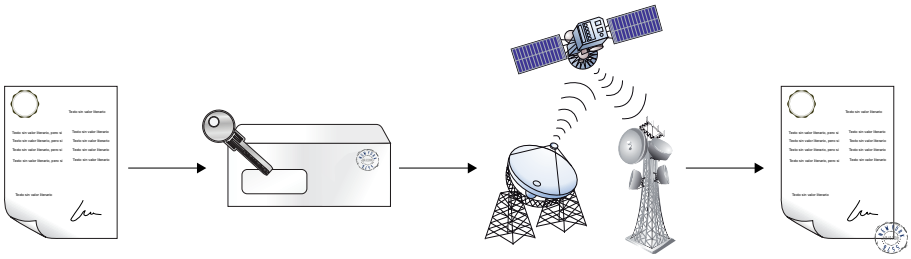
La factura electrónica es el equivalente digital de la factura en papel. La facturación electrónica (también nos referiremos a ella como **e-facturación**) consiste en la transmisión de las facturas, o documentos análogos, entre emisor y receptor por medios electrónicos (ficheros informáticos) y telemáticos (de un ordenador a otro), **firmados electrónicamente** con **certificados reconocidos**, lo que garantiza la **autenticidad** de su origen y la **integridad** de su contenido.

Los certificados reconocidos deben seguir los estándares del sector de normalización de la Unión Internacinal de Telecomunicaciones, UIT-T (antes, el Comité Consultivo Telefónico y Telegráfico, CCITT)), en particular, el protocolo X.509v3, o de una versión superior, que deben ser admitidos por una autoridad de certificación que participa en las relaciones tributarias por medios

electrónicos y telemáticos con la Agencia Estatal de Administración Tributaria (AEAT).

El gráfico siguiente muestra el proceso de facturación electrónica:

| Factura tradicional | Factura electrónica |
|---|---|
| Papel | Fichero electrónico |
| Firma normal | Firma electrónica + certificado electrónico reconocido |
| Envío postal | Transmisión telemática |




Se puede considerar la factura electrónica como un documento tributario generado por medios informáticos en formato electrónico, que reemplaza el documento físico en papel, pero que conserva el mismo valor legal con unas condiciones de seguridad (autenticidad e integridad) que no se dan en la factura en papel. Este valor legal permite atribuir a la factura electrónica la obligación tributaria del emisor.

Entre las muchas ventajas de la facturación electrónica encontramos:

- **Ahorro de costes y mejora de la eficiencia. Control de acciones erróneas**. Aunque es difícil evaluar el coste global asociado a la facturación en papel, es evidente que en la facturación electrónica se reducen los costes del papel, de impresión, de manipulación (ensobrar y almacenar en ficheros y carpetas físicas) y de envío por correo postal, entre otros. Por otro lado, se puede considerar que la interacción electrónica y telemática durante todo el proceso ayudará a la mejora de la eficiencia y al control de errores. Dado que el proceso administrativo se puede automatizar, se reducen las tareas más reiterativas y así también se reducen los errores humanos.

- **Mayor seguridad en el resguardo de los documentos y menor probabilidad de falsificación**. El uso de certificados electrónicos reconocidos ofrece a las facturas las garantías de autenticidad del emisor y de integridad de la factura, que disminuyen enormemente las probabilidades de falsificación.

  La automatización del proceso de almacenamiento de las facturas provoca el aumento de la seguridad de los documentos guardados, al mismo tiempo que facilitará su recuperación.

**Mejora medioambiental**

La factura electrónica, al sustituir la factura emitida en papel, aporta unos beneficios medioambientales innegables: 1 tonelada de papel = 15 árboles + $250 m^3$ de agua.

- **Integración con las aplicaciones de gestión internas de la empresa. Facilidad en los procesos de auditoría.** El intercambio electrónico de facturas permite reducir el tiempo de gestión de las facturas de una manera considerable, sobre todo si se pueden integrar en los ERP (*enterprise resource planning*) del emisor para la generación de facturas e integrar las facturas en el ERP del receptor, para su gestión, mediante formatos estándar estructurados.

  La facturación electrónica permite una administración y contabilidad automatizadas, lo que supone una reducción de tiempo de gestión y aporta muchas facilidades a los procesos de auditoría, ya que permite, de manera rápida, verificar en qué estado se encuentra una factura y toda la información que está asociada a esta (albaranes, cobros, pagos, etc.).

**Enterprise resource planning (ERP)**

Los sistemas de planificación de recursos empresariales son sistemas de gestión de información que automatizan muchas de las prácticas de negocio asociadas a los aspectos operativos o productivos de una empresa.

- **Optimización de la tesorería. Uso eficaz de los recursos financieros.** La facturación electrónica permite acceder a los servicios avanzados de financiación y pago que ofrecen las entidades financieras, como el factoraje electrónico (*e-factoring*) o la confirmación electrónica (*e-confirming*).

**Factoraje electrónico**

Es una modalidad de factoraje (fórmula de financiación basada en la cesión de facturas a un tercero a cambio de unos costes derivados del adelanto del pago de las facturas antes de su vencimiento) en la que el documento cedido corresponde a una factura electrónica y las transacciones que se realizan entre el cliente, el deudor y el tercero (generalmente una entidad financiera) son totalmente en línea.

**Confirmación electrónica**

Es un servicio que ofrece una entidad financiera para facilitar a sus clientes la gestión del pago de las compras que realizan con la finalidad de que el proveedor pueda cobrar las facturas antes de la fecha de vencimiento. Realmente es un servicio de gestión de pagos y no de deuda.

- **Eliminación de espacios para almacenar documentos históricos. Agilidad en la localización de información.** Si antes nos hemos referido al ahorro de costes de papel, conviene recordar ahora que con la facturación electrónica se reduce sustancialmente la necesidad de espacio físico que se necesita para guardar las facturas en papel, al mismo tiempo que se mejora la localización de la factura y de toda la información a la que se hace referencia.

Para la realización de la factura electrónica es imprescindible considerar los requisitos siguientes:

**1)** Utilizar un formato electrónico de factura, que suele ser: EDIFACT, XML, PDF, HTML, DOC, XLS, TXT, etc.

**2)** Disponer de un sistema de transmisión telemática: la factura electrónica debe partir de un ordenador y ser recopilada, para su proceso, por otro ordenador. El medio telemático para el envío del fichero firmado, que es un único fichero que contiene la factura y la firma reconocida, es libre; es decir, se puede utilizar el correo electrónico, un FTP (*file tranfert protocol*), una página web desde la que se pueda descargar la factura o enviarla mediante un servicio web (*web service*).

**3)** Disponer de software para llevar a cabo la firma electrónica reconocida, o avanzada, para garantizar la integridad y la autenticidad, tanto del documento electrónico como de la transmisión telemática.

**FTP**

Se trata de un protocolo de red para la transferencia de archivos que se basa en la arquitectura cliente-servidor, permitiendo que desde el equipo de un usuario se pueda conectar a un servidor de otro (por ejemplo, el de un proveedor) para bajarse archivos o para subirlos, independientemente del sistema operativo utilizado en cada equipo.

# 1. Requisitos legales

Para que el uso de Internet sea seguro, especialmente en las transacciones que tienen o pueden tener contenido económico, se deben poder garantizar los requisitos siguientes:

- **Identidad**: Tener la seguridad de que se está realizando la transacción con la persona/entidad deseada.
- **Legitimación**: Conocer si el interlocutor está capacitado profesional o legalmente para llevar a cabo la gestión o la transacción que está intentando realizar.
- **Confidencialidad**: Tener la seguridad de que solo la empresa/administración y la persona/entidad con la que se está realizando la transacción pueden acceder a la información.
- **Integridad**: Tener la seguridad de que los documentos que son motivo de la transacción sean los originales; es decir, que los documentos no han sido manipulados.
- **Autenticidad**: Tener la evidencia de la realización de un convenio, contrato, transacción, etc., con los requisitos suficientes para su validez.
- **Autenticación**: Tener la seguridad de que el interlocutor es realmente quien dice ser.
- **Disponibilidad**: Tener garantías de poder acceder al documento electrónico durante todo el tiempo y que este continúe teniendo validez jurídica.

Hoy en día existen las herramientas necesarias y las garantías jurídicas suficientes para poder garantizar la confianza en las relaciones a través de la Red. Para justificar el cuadro legislativo que da amparo a la facturación electrónica, desde el punto de vista jurídico, podéis considerar las publicaciones siguientes tanto de ámbito español como comunitario.

**Normativa española**

En España, se aplica de manera general la Directiva de la Unión Europea 2001/115/CE (20/12/2001), donde se definen los aspectos técnicos precisos para que sea válido, legal y fiscalmente, el uso de las facturas en soportes electrónicos.

También marca el deber de garantizar la autenticidad en origen (del emisor) y la integridad del contenido de la factura (datos). Esta Directiva está adaptada al ordenamiento nacional, principalmente en estas normas:

- Orden HAC/3134/2002 del Ministerio de Hacienda y Administración (publicada en el BOE, 13-12-2002), que desarrolla el régimen de facturación telemática, en la que se autoriza directamente a los sistemas que utilizan la firma electrónica basada en certificados reconocidos (derogada por la Orden EHA 962/2007).

**Facturación telemática**

Este es el término que se utiliza en estas normativas para referirse a la facturación electrónica. Por tanto, en este apartado hemos respetado esta sintaxis.

- Resolución de la AEAT 2/2003 (BOE 28-02-2003), de la Dirección general de la Agencia Estatal de Administración Tributaria (AEAT), sobre determinados aspectos relacionados con la facturación telemática. En particular, admite, entre otros, los certificados reconocidos por la Fábrica Nacional de Moneda y Timbre (FNMT).

- Orden HAC 1181/2003 del Ministerio de Hacienda y Administración (publicada en el BOE, 15-05-2003), por la cual se establecen normas específicas sobre el uso de la firma electrónica en les relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria.

- Real Decreto 1496/2003 (BOE, 29-11-2003), por el que se aprueba el Reglamento que regula las obligaciones de facturación y se modifica el Reglamento del impuesto sobre el valor añadido. En particular, se regula la prestación de los servicios de emisión y de conservación de las facturas por parte de terceros.

- Ley General Tributaria 58/2003 (BOE, 18-12-2003), que constituye el eje central del ordenamiento tributario y en la que se recogen sus principios esenciales y se regulan las relaciones entre la Administración tributaria y los contribuyentes.

- Ley 59/2003 (BOE, 20-12-2003) de **firma electrónica**, en la que se regulan los diferentes sistemas de firma electrónica y otros servicios, así como su nivel de valor legal. Es un texto mejor adaptado a las necesidades de los prestadores y de los usuarios que transpone la directiva europea. Además, da un tratamiento especial al DNI electrónico y a los certificados de personas jurídicas.

- Real Decreto 87/2005 (BOE, 01-02-2005), por el que se modifican el Reglamento del impuesto sobre el valor añadido, aprobado por el Real Decreto 1624/1992, el Reglamento de los impuestos especiales, aprobado por el Real Decreto 1165/1995 y el Reglamento por el que se regulan las obligaciones de facturación, aprobado por el Real Decreto 1496/2003, en particular respecto a las facturas o documentos sustitutivos rectificativos.

- Orden EHA 962/2007 del Ministro de Economía y Hacienda (BOE, 14-04-2007), por el que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas, contenidas en el Real Decreto 1496/2003, por el que se aprueba el reglamento que regula las obligaciones de facturación (deroga la Orden HAC/3134/2002).

- Resolución AEAT (BOE, 24-10-2007) de la Agencia Estatal de Administración Tributaria, sobre procedimiento para la homologación de software de digitalización previsto en la Orden EHA 962/2007.

- Ley 11/2007 (BOE, 23-06-2007) de Acceso Electrónico de los Ciudadanos a los Servicios Públicos. En la ley se explicita que es necesario que las administraciones públicas garanticen: la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad, la conservación de los datos, informaciones y servicios; bajo los principios de seguridad en la implantación y utilización de medios electrónicos y del de proporcionalidad en relación con las medidas de seguridad exigidas y en relación con los datos que se requieren a los ciudadanos.

  De esta ley destacan los 46 artículos que hacen referencia a identidad digital, firma electrónica, seguridad jurídica, indicando la importancia que da el legislador a estos aspectos.

  Se hace referencia a esta ley mediante el acrónimo LAECSP.

- Orden PRE 2971/2007 (BOE, 15-10-2007) sobre la expedición de facturas por medios electrónicos cuyo destinatario sea la Administración General del Estado, u organismos públicos vinculados que son dependientes de esta y sobre la presentación ante la Administración General del Estado, o de sus organismos públicos vinculados o dependientes, de facturas expedidas entre particulares.

- Ley 30/2007 (BOE, 31-10-2007) de Contratos del Sector Público. Esta ley tiene como objeto regular la contratación del sector público. Hace continuas referencias a la utilización de los medios electrónicos, informáticos y telemáticos en el ámbito de la contratación pública, y siempre haciendo referencia a conseguir como finalidad hacer más fluidas y transparentes las relaciones entre los órganos de contratación y las empresas licitadoras. En esta ley se pone de relieve la importancia de la firma electrónica, del sellado de tiempo y del documento electrónico. Además, se ve muy claro el motivo y la voluntad del legislador de que las administraciones públicas impulsen la utilización de estos medios.

  Se hace referencia a esta ley mediante el acrónimo LCSP.

- Ley 56/2007 (BOE, 29-12-2007) de Medidas de Impulso de la Sociedad de la Información, que define la factura electrónica como un documento electrónico que cumple los requisitos legal y reglamentariamente exigibles a las facturas. Esta ley es de alguna manera la LAESCP del sector privado, en la que se establece la obligación para un conjunto de empresas de admitir los medios telemáticos con garantías jurídicas en las relaciones con sus clientes.

Se hace referencia a esta ley con el acrónimo LISI.

- Orden PRE 2794/2011 (BOE, 18-10-2011), por la que se determina el marco de ejercicio de las competencias estatales en materia de factura electrónica, se crea el Foro Nacional Multilateral sobre facturación electrónica y se impulsa el Servicio Central de Gestión de la Facturación Electrónica en el ámbito de la Administración General del Estado.

- Real Decreto 3/2011 (BOE, 16-11-2011) de texto refundido de la Ley 30/2007 de Contratos del Sector Público.

**Normativa comunitaria**

- Directiva 1997/6/CE del Consejo, de 17 de mayo de 1977, en materia de armonización de las legislaciones de los Estados miembros relativas a los impuestos sobre el volumen de negocios. Sistema común del IVA: Base imponible uniforme. (Vigente a 15-05-2004).

- Directiva 1999/93/CE del Consejo, de 13 de diciembre de 1999, cuya finalidad es facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico, creando un marco jurídico, tanto para la firma electrónica como para determinados servicios de certificación electrónica para dar seguridad jurídica a la comunicación y al comercio electrónico.

- Directiva 2001/115/CE del Consejo, de 20 de diciembre del 2001, por la que se modifica la Directiva 77/388/CEE a fin de simplificar, modernizar y armonizar las condiciones impuestas a la facturación en relación con el impuesto sobre el valor añadido.

- Directiva 2006/112/CE del Consejo, de 28 de noviembre del 2006, relativa al sistema común del impuesto sobre el valor añadido.

- Directiva 2010/45/UE del Consejo, de 13 de julio del 2010, por la que se modifica la Directiva 2006/112/CE, respecto a las normas de facturación.

Existen algunas normativas internacionales aplicables de manera general a la factura electrónica, aunque Naciones Unidas, por medio de la UN/CEFACT, ha publicado recomendaciones, como por ejemplo UNeDocs, que definen plantillas para las facturas impresas y formatos EDI y XML para las modalidades electrónicas. En Europa, la facturación electrónica se regula en la Directiva 2001/115, que debía ser adoptada en cada país antes del 31 de diciembre del 2003, tal como sucedió en España.

En la actualidad la organización GS1 (antes EAN/UCC) ha organizado comités internacionales de usuarios de 108 países miembros para conformar las guías de facturación electrónica estándar a escala mundial.

# 2. Factura electrónica: firma y certificados reconocidos

En este apartado daremos unas nociones sobre la firma electrónica para su utilización en la factura electrónica, así como en las infraestructuras que están implicadas en ella.

## 2.1. Infraestructuras de clave pública: PKI

En el ámbito de la facturación electrónica es imprescindible garantizar la identidad de los usuarios, además de los servicios de seguridad: confidencialidad, integridad, autenticación y no rechazo.

Para que estas operaciones se puedan realizar de manera fiable se deben cumplir dos condiciones:

- Que la clave privada se custodie de manera segura y no se revele a nadie. Para conseguirlo, la clave privada se almacena en un soporte físico imposible de duplicar, como una tarjeta inteligente. Además, para acceder al contenido de la tarjeta se necesita un número personal que solo conoce su poseedor legítimo.

- Que se pueda determinar a qué persona pertenece una clave pública. De esta manera se puede saber, por ejemplo, quién ha llevado a cabo la firma electrónica de un documento.

Para dar cumplimiento a esta última condición, se utiliza el certificado electrónico, cuyo soporte tecnológico es la criptografía de clave pública. Así, se puede ver un certificado electrónico como un documento electrónico que asocia una clave pública a su propietario.

El certificado electrónico contendrá la clave pública junto a datos de carácter personal del poseedor de la clave (nombre, DNI, etc.). Normalmente contiene más información (datos de validez y otros), así como también se refiere al ámbito de utilización del certificado, lo que se conoce como política de certificación. Por ejemplo, si es un certificado de uso personal nos acredita para actuar en nombre de una empresa.

Al realizar una firma electrónica se suele adjuntar el certificado electrónico del firmante, de manera que se puede extraer su clave pública para verificar la firma y al mismo tiempo comprobar la identidad del firmante.

Una infraestructura de clave pública (*public key infrastructure, PKI*) es una estructura de sistemas informáticos, procedimientos de operación, protocolos, políticas de certificación, repositorios de información, estándares, declaraciones de prácticas y recursos humanos cuya finalidad es ofrecer a los usuarios una plataforma para la gestión de la identidad digital.

Una PKI dispone de los elementos y de la arquitectura necesarios para integrar todos los procedimientos de solicitud de certificados, verificación de identidades, generación de claves, almacenaje y publicación de certificados electrónicos, renovación, revocación, etc.

Las infraestructuras de clave pública se fundamentan en la interacción de diferentes subsistemas, de los que destacan los siguientes:

- **Autoridad de certificación, CA**: una autoridad de certificación (*certificate authority*) es una entidad de confianza cuya finalidad es emitir, renovar y revocar certificados electrónicos. Las autoridades de certificación constituyen el núcleo de las infraestructuras de clave pública, que permite utilizar los **certificados electrónicos** con total seguridad.

**Ejemplos de CA: Verisign, FNMT, CATCert, etc.**

En la actualidad, un usuario puede elegir entre múltiples CA para conseguir un certificado electrónico, pero las más utilizadas son a escala internacional Verisign (www.verisign.com), a escala estatal FNMT (www.fnmt.es) y en el ámbito catalán CATCert (www.catcert.cat).

- **Autoridad de registro, RA**: una autoridad de registro (*registration authority*) es una entidad encargada de llevar a cabo los procesos de verificación de identidad, solicitud y distribución de certificados electrónicos. Normalmente, en una PKI los usuarios finales no interactúan directamente sobre la CA, sino que canalizan sus operaciones por medio de una o varias RA. No obstante, estos subsistemas no pueden expedir certificados electrónicos por sí mismos.

- **Certificados electrónicos**: un certificado electrónico es un archivo o documento electrónico expedido y firmado por una CA en el que se vincula una identidad a una clave pública, vinculada, a su vez, a la correspondiente clave privada. Para obtener un certificado electrónico, el usuario se dirige a una RA (autoridad de registro), que verifica la identidad del usuario y solicita a la CA que expida el certificado.

**La recomendación X.509 de la ITU-T**

Esta recomendación forma parte de la serie de recomendaciones X.500 del sector de estandarización de telecomunicaciones de la ITU (International Telecommunications Union), cuya finalidad es definir un servicio de directorio. Por directorio se entiende un servidor o conjunto distribuido de servidores que gestionan una base de datos de información sobre usuarios. En la actualidad, hablar de X.509 y certificados electrónicos es hablar del mismo concepto.

- **Sistemas gestores de certificados electrónicos: la recomendación X.509**: el auge de la certificación electrónica nace de la consolidación internacional del protocolo estándar X.509 de la ITU-T. Los sistemas gestores de certificados electrónicos son el conjunto de aplicaciones que aprovechan los servicios de la identidad digital junto a los paquetes de software que implementan las funciones básicas de una PKI. Su implementación responde a tres categorías: las integradas en el sistema operativo, las libres (de código abierto) y las comerciales.

- **Directorio LDAP (***lightweight directory access protocol***)**: su finalidad es mantener un registro de usuarios y actuar como almacén para los certificados

electrónicos y la lista de certificados revocados (CRL). El protocolo LDAP es una versión simplificada del protocolo X.500, que especifica tanto el modelo de información como los mecanismos de acceso a esta.

- **Listas de certificados revocados (CRL) y el protocolo OCSP**: una lista de certificados revocados (*certificate revocation list*) es un documento electrónico expedido y firmado por una CA en el que se incluyen los números de serie de todos aquellos certificados que, sin haber expirado, han sido revocados por algún motivo. La recomendación X.509 define un formato estándar para las listas CRL.

  Al recibir un certificado electrónico, el usuario debe consultar la CRL de la CA que firma el certificado para verificar su validez. El protocolo OCSP (*online certificate status protocol*) permite realizar consultas en tiempo real sobre la base de datos de certificados revocados de una CA. Algunos navegadores web ya incluyen soporte para OCSP.

**Validación de certificados**

La validación de certificados en tiempo real es imprescindible para el desarrollo de la factura electrónica.

- **Prestador de servicios de certificación, PSC**: el prestador de servicios de certificación es una entidad, reconocida por los participantes, que hace la gestión de los subsistemas de la PKI para evitar la interceptación de los mensajes por parte de un interlocutor ilegítimo que se introduce en el circuito de intercambio de claves. Evidentemente, el PSC debe ser una entidad de confianza (o también denominada *trusted third party, TTP*), que en su política de certificación debe incluir cláusulas aceptables para los diferentes interlocutores, que permita, entre otras cosas, la verificación de identidad, que dé información sobre uso y validez de los certificados y que realice la gestión de certificados revocados y ofrezca la lista de certificados expedidos.

  El PSC recibe la petición de un participante para que emita un certificado que garantice que su clave pública es, precisamente, suya. Cuando el PSC tiene certeza de esta identidad, emite un certificado en el que se recogen los datos de identificación e, inseparablemente, la clave pública del peticionario. En el certificado, todos estos datos están encriptados con la clave privada del PSC. Teniendo en cuenta que su clave pública es conocida por todos los interlocutores, cualquiera es capaz de extraer los datos del certificado. No obstante, nadie es capaz de suplantar al PSC emitiendo certificados falsos, ya que para eso debería disponer de su clave privada.

  Los parámetros que definen a un PSC son su dirección de red (nombre distinguido) y su clave pública. Además, es necesario especificar en su identificación la entidad emisora del certificado, el departamento u organización responsable de la custodia de la clave privada y la ubicación (ciudad, país, etc.). También son importantes aspectos como el identificativo fiscal o referencia registral.

## 2.2. Los certificados electrónicos

En cuanto a los certificados, para cualquier tipo de empresa, podemos distinguir los cuatro tipos siguientes:

- **Certificados de pertenencia de persona física**. Este certificado permite que el titular se identifique como trabajador de una empresa, al mismo tiempo que garantiza la identidad de la empresa de la persona física titular del certificado y su vinculación, en virtud del cargo que ocupa en ella. El uso de este certificado se restringe únicamente al titular y la cesión del certificado es exclusivamente responsabilidad suya.

- **Certificados de persona jurídica**. Este certificado identifica una empresa con personalidad jurídica y se puede utilizar siempre que se admita en las relaciones que mantenga la persona jurídica con las administraciones públicas o en la contratación de bienes o servicios que sean propios de su actividad ordinaria. Su custodia es responsabilidad de la persona física que lo solicita; todo ello, sin perjuicio de que lo puedan utilizar otras personas físicas vinculadas a la empresa.

- **Certificados de persona física de representante**. Este certificado se emite a favor de una persona física representante de una empresa que le permite actuar en nombre de la empresa a la que pertenece. El titular se identifica como persona física perteneciente a una empresa, al mismo tiempo que añade la cualificación de representante legal de la misma. El uso de este certificado se restringe solo al titular y la cesión del certificado es exclusivamente responsabilidad suya.

- **Certificado de factura electrónica**. Este es exclusivo para la actividad de facturación. No permite realizar ningún otro trámite, en nombre de la empresa, que no sea la facturación electrónica, ni con la Administración ni entre empresas. Este certificado ofrece una seguridad extra en la firma de facturas, especialmente para las grandes empresas, que confían en el certificado a la hora de emitir facturas electrónicas. La Agencia Estatal de Administración Tributaria los certifica como válidos al efecto de la facturación electrónica y, según lo que dispone la directiva de la UE, están vinculados a una persona y son válidos para emitir facturas en el extranjero.

Respecto a los certificados reconocidos, el artículo 11.1 establece que son los certificados electrónicos emitidos por un proveedor de servicios de certificación que cumpla los requisitos que establece esta ley 59/2003, en cuanto a la comprobación de la identidad y el resto de las circunstancias de los solicitantes y en cuanto a la fiabilidad y las garantías de los servicios de certificación que presta.

## 2.3. La firma electrónica

Desde el punto de vista técnico, en el marco del European Telecommunications Standards Institute (ETSI) destacan los tipos de firma electrónica de relevancia legal siguientes:

- **Simple.** Constituida por datos que puedan ser usados para identificar y autenticar al firmante.
- **Avanzada.** Cuando, además de identificar al firmante, permite garantizar la integridad del documento.
- **Reconocida.** Cuando es una firma avanzada, amparada por un certificado reconocido y realizada con un dispositivo seguro de creación de firma. Esta firma también se denomina **cualificada**.

**Lectura recomendada**

Consideraremos que se conocen los algoritmos de firma electrónica, como RSA, DSA, etc. Pero para profundizar en ellos se puede consultar el libro: **L. Huguet, J. Rifa, J. Tena**. *Criptografia Avanzada*.

Material docente de la UOC, PID_00185087.

En el proceso de firma se emplea un certificado de usuario que garantiza la autenticidad del emisor y una marca, o huella digital (normalmente una función *hash*), que garantiza la integridad. Es decir, en caso de modificación de la factura durante el proceso telemático, la firma es invalidada por el software del receptor.

***hash* o MAC**

El *hash* o MAC (*message authentication code*) es una función resumen que calcula un valor, siempre del mismo tamaño en número de bits, dependiendo del documento sobre el que se calcula, y que es diferente para diferentes documentos, aunque su diferencia sea pequeña. Esta es una función unidireccional, en el sentido de que conocer el resumen no nos aporta información del documento, aunque identifica de manera unívoca el documento sobre el que se ha aplicado.

La firma avanzada puede incluir más o menos información, relativa al momento de creación o a la validez de los certificados. La más sencilla recoge los elementos esenciales de la firma electrónica: el resumen del documento firmado (*hash*), el certificado del firmante asociado a la clave pública del firmante y el resultado de aplicar la clave privada del firmante al resumen, que es la firma electrónica propiamente dicha.

Por otro lado, hablaremos de **firma fechada** si se añade a la firma básica información temporal sobre el momento de la firma o de su verificación (sellado de tiempo o *time stamping*), y de **firma validada** si se añade a la firma fechada información sobre la vigencia del certificado utilizado en el momento de la firma o de su verificación. La firma validada se denomina también **firma completa** porque incluye todos los elementos que permiten comprobar que el certificado utilizado por el firmante estaba vigente en el momento de la firma, y permite así su almacenamiento a largo plazo.

**Sellado de tiempo**

El sello temporal o *time stamping* garantiza el momento exacto de tiempo en el que se ha producido la firma de un documento. El servicio de sellado temporal, que normalmente realiza una Autoridad de Certificación, permite al usuario acreditar el día y la hora en las que ha recibido o enviado un archivo informático, y esto resulta fundamental en el caso de la factura electrónica o en el caso de almacenamiento temporal de documentos digitales.

A pesar de que los datos relativos, tanto en el sellado de tiempo como en la revocación del certificado, son de gran utilidad y aportan un gran valor añadido al procedimiento de firma, no son de obligado cumplimiento para la validez de una factura electrónica.

El artículo 3.2 de la Ley 59/2003 indica que la firma electrónica avanzada es la que permite identificar al firmante y detectar cualquier cambio posterior de los datos firmados. Está vinculada al firmante y a los datos a los que hace referencia, de manera única y ha sido creada por medios que el firmante puede mantener exclusivamente bajo su control.

Y en el artículo 3.3 define la firma electrónica reconocida como la firma electrónica avanzada basada en un certificado reconocido (que cumple los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y otras circunstancias de los solicitantes) y generada mediante un dispositivo seguro de creación de firma.

**Validez de la firma electrónica**

La firma electrónica, para ser usada en facturación electrónica, debe ser reconocida con el fin de conseguir el mayor grado de seguridad de acuerdo con la Ley 59/2003. Solo la firma reconocida tiene validez legal igual a la manuscrita.
El plazo de resolución es de seis meses, contando desde la fecha de presentación de la solicitud en el registro.
Si la verificación no hubiese finalizado en este plazo, o no se hubiese dictado resolución expresa, la solicitud se podrá entender desestimada por silencio administrativo.

La ley define estos dispositivos como los que ofrecen, al menos, las garantías siguientes:

- Que los datos utilizados para la generación de la firma se pueden producir solo una vez y asegurar 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. Además, 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 manera fiable por el firmante contra su utilización por terceros.
- Que el dispositivo utilizado no altera los datos o el documento que se deba firmar ni impide que este se muestre al firmante antes del proceso de firma.
- Que el consentimiento de ambas partes (del emisor y del receptor) se necesita para que la facturación electrónica tenga la misma validez legal que la factura en papel.

En los países en los que la legislación lo admite, la validez de una factura electrónica es exactamente la misma que la de la factura en papel y gracias a la firma electrónica que incluye se garantiza su integridad y un alto nivel de trazabilidad, por lo que judicialmente es un documento considerado vinculante y que no necesita mayor prueba o consignación que su propia existencia.

## 2.4. Esquema de la firma electrónica

Veamos un esquema del procedimiento de firma electrónica y de su verificación, suponiendo que emisor y receptor disponen de un sistema criptográfico asimétrico (por ejemplo, el criptosistema RSA) y que el receptor dispondrá del certificado de la clave pública del firmante.

**Criptosistema RSA**

El criptosistema RSA consiste en encriptar valores numéricos asociados a bloques, de una determinada longitud, de caracteres en los que están escritos los mensajes originales (por ejemplo, encriptar los valores numéricos de bloques de caracteres ASCII). Supongamos $m \in [2,n-1]$ correspondiente a un cierto bloque que encriptar.

El **algoritmo de encriptación** se reduce al cálculo de una exponencial donde la clave pública es el par de números $(e,n)$:

$$c = E_{(e,n)}(m) = m^e \bmod n$$

El **algoritmo de desencriptación**, para poder obtener $m$ a partir de $c$, consiste también en una exponenciación, donde la clave privada es ahora otro par de números $(d,n)$:

$$m = D_{(d,n)}(c) = c^d \bmod n$$

Los parámetros $n$, $e$ y $d$ se obtienen de la manera siguiente:

**1)** Encontrar el valor $n = p \cdot q$, donde $p$ y $q$ son dos números primos grandes (al inicio ya se sugerían un centenar de dígitos cada uno).
**2)** Conociendo $p$ y $q$, calcular: $\phi(n) = (p-1) \cdot (q-1)$.
**3)** Tomar $e$ relativamente primo con $\phi(n)$.
**4)** Calcular $d = e^{-1} \bmod \phi(n)$.

**Firma electrónica, basada en el criptosistema RSA**

Los algoritmos de encriptación y desencriptación del algoritmo RSA son conmutativos; es decir: $D_k(E_k(m) = E_k(D_k(m))$, por tanto, el esquema RSA puede ser utilizado para ambos objetivos de privacidad y autenticidad.

En función de esta conmutatividad se puede utilizar el criptosistema RSA para construir firmas electrónicas. En este caso, si suponemos que un usuario $A$ quiere enviar un mensaje $m$ a otro usuario $B$ y la clave pública de $A$ es $(e_A,n_A)$ y la clave privada $(d_A,n_A)$, podremos arbitrar un sistema de firma electrónica para que $B$ pueda autenticar a $A$, de la manera siguiente:

Por parte del usuario $A$: Firma $m$ con su clave privada: $s = D_{(d_A,n_A)}(m) = m^{d_A} \bmod n_A$ y entonces enviará al usuario $B$: $(m,s)$

Por parte de $B$, una vez recibido el criptograma $(m,s)$, hará:

**1)** Encriptar $s$ con la clave pública de $A$: $E_{(d_A,n_A)}(s) = s^{e_A} \bmod n_A$
**2)** Verificar si el valor encontrado anteriormente es igual a $m$.
En este caso se da la firma por válida. En caso contrario, significa que ha habido algún problema en la transmisión de $m$, o en la propia firma.

**Fortaleza de la función unidireccional logaritmo discreto**

En un cuerpo finito $\mathbb{Z}_p$ es fácilmente calculable $y = \alpha^x \bmod p$; pero para valores grandes de $p$, dado $y$ es computacionalmente ineficiente calcular el logaritmo discreto $x = log_\alpha y \bmod p$.
En la dificultad de este cálculo se basa la fortaleza del criptosistema ElGamal y, por tanto, también del algoritmo DSA.

Como alternativa a la firma electrónica RSA, en 1991 el National Institute of Standards and Technology (NITS) realizó la propuesta del algoritmo DSA (*digital signature algorithm*) como un estándar de firma electrónica, basado en el sistema criptográfico asimétrico de ElGamal, que se basa en la función unidireccional exponencial discreta en un cuerpo finito $\mathbb{Z}_p$ respecto de un elemento primitivo $\alpha$.

Este algoritmo DSA fue desarrollado por la National Security Agency (NSA) con el propósito de reducir la longitud del mensaje *m* a encriptar. Por esta razón, en el proceso de firma se utiliza una función *hash*, por ejemplo SHA.

Los parámetros de esta firma DSA son:

- $p$, un número primo cuyo valor está comprendido entre 512 y 1024 bits.
  $q$, un factor primo de $p-1$ de unos 160 bits. Sea $n = (p-1)/q$
  $\alpha$, de modo que $\alpha = g^n \bmod p$, donde $g$ es un número menor que $p-1$ y de manera que $\alpha \bmod p > 1$.
- $x$, un número cualquiera menor que $q$. Entonces se calcula $y$, de modo que $y = \alpha^x \bmod p$.

Los números $p$, $q$ y $\alpha$ son públicos para todos los usuarios de la red, así como será público el *hash*, $H()$, que se usará (por ejemplo, el *hash* SHA-1, que, sea cual sea la extensión del mensaje que se haya de firmar, dará un resumen de 160 bits).
Por otro lado, $x$ es la clave privada de un usuario, y $y$ es la correspondiente clave pública.
Sea $m$ el mensaje que $A$ quiere transmitir a $B$, que quiere firmar para que $B$ pueda realizar la autenticación. El usuario A, del que se suponen conocidos los parámetros anteriores, excepto $x$, deberá realizar las operaciones siguientes:

**1)** Elegir un número aleatorio $k$, menor que $q$.

**2)** Generar dos valores $r$ y $s$, de manera que:
$r = (\alpha^k \bmod p) \bmod q$, y
$s = ((H(m) + x \cdot r) \cdot k^{-1}) \bmod q$.

**3)** Enviar el mensaje $m$ y su firma electrónica $(r,s)$.

El usuario $B$, al recibir el mensaje $m$, y su firma electrónica correspondiente $(r,s)$, podrá seguir el siguiente proceso de autenticación:

**1)** Seleccionar del directorio público los parámetros de $A$: $p,q,\alpha$ y $H(.)$.

**2)** Calcular: $w = s^{-1} \bmod q$,
$u_1 = (H(m) \cdot w) \bmod q$ y
$u_2 = (r \cdot w) \bmod q$.

**3)** Calcular: $v = ((\alpha^{u_1} \cdot y^{u_2}) \bmod p) \bmod q$.

**4)** Autenticar:
Si $v = r$ entonces la firma electrónica de $A$, $(r,s)$, es aceptada por $B$.
En caso contrario, el mensaje $m$ o la firma $(r,s)$ han sufrido algún cambio durante la transmisión.

**Procedimiento de la firma electrónica**

De manera general, el procedimiento de la firma electrónica sigue lo que hemos indicado para el caso de la firma RSA y DSA. Olvidándonos de fórmulas, partimos de un documento original (en este caso, la factura electrónica), que es sometido por el emisor a los pasos siguientes:

**1)** El emisor aplica al documento original (e-factura) la función unidireccional *hash*, con lo que obtiene el correspondiente resumen.

**2)** El emisor encripta, con su clave privada, el resumen resultante de la aplicación anterior. El resultado será su firma electrónica.

**3)** El emisor envía al destinatario el conjunto formado por el documento original (la e-factura), su firma electrónica y el certificado de su clave pública.

**Comprobación/verificación de la firma electrónica**

El receptor recibe el conjunto formado por el documento original (la e-factura), la firma electrónica y el certificado de la clave pública del emisor. A partir del certificado, el receptor podrá extraer la clave pública del emisor y seguir los pasos siguientes:

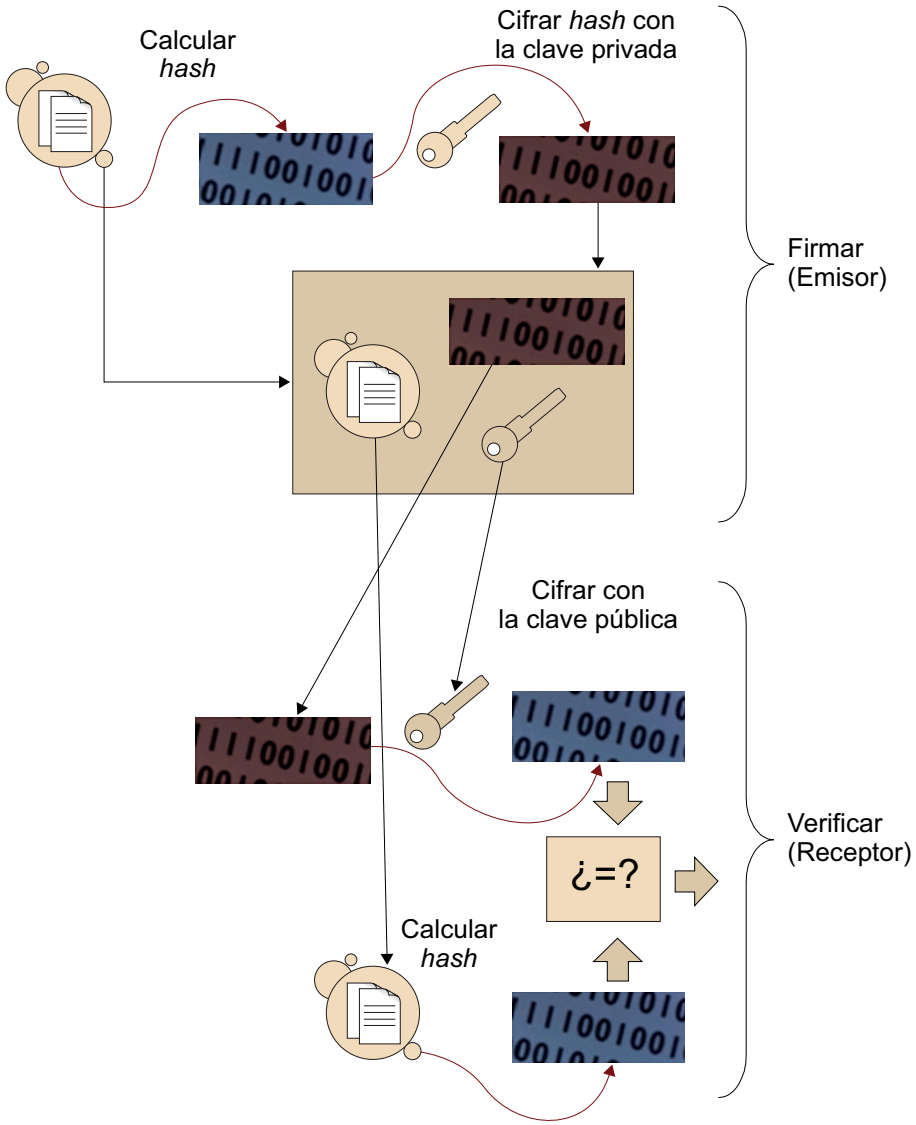
**1)** Dado que el receptor dispone del documento original, puede calcular el *hash*, con lo que obtiene el mismo resumen que había obtenido el emisor.

**2)** El receptor, con la clave pública del emisor, podrá encriptar la firma electrónica y, por tanto, obtener el *hash* que se calculó en origen.

Al comparar el *hash* obtenido en el paso 1 con el *hash* obtenido en el paso 2, deben coincidir.

En caso de que no coincidan, o bien el documento o bien el *hash* firmado ha tenido alguna incidencia en la transmisión y, por tanto, la firma no es válida.

En la figura siguiente se puede ver el diagrama de funcionamiento:




Procedimiento de firma electrónica y su verificación

## 2.5. Formato XML de firma en facturación electrónica

No hay requisitos formales respecto a la forma en la que se debe proceder en la codificación de la factura, pero para cada formato existe una manera peculiar de codificar la firma electrónica. Las modalidades más habituales son las siguientes:

**1)** PDF. Cuando al destinatario solo le interesa guardar electrónicamente la factura, pero no evitará volver a teclear los datos, ya que con este formato no se facilita el ingreso de los datos de la factura en el ordenador del receptor.

El formato de firma queda incluido dentro del formato PDF y permite asociar una imagen, por lo que es uno de los más adecuados para su visualización. Se utiliza AcrobatReader v7 o Foxit PDF Reader. La apariencia de la firma es muy visual, ya que es posible asociarle un gráfico como firma electrónica o un sello de empresa.

**2)** EDIFACT. Cuando el envío se realiza de ordenador a ordenador, lo que significa que el destinatario es una empresa que tiene capacidad tecnológica para tratar de manera automatizada la información recibida, y así los datos se ingresan en el ordenador de destino automáticamente. Este estándar es desarrollado por la organización Global System 1 (GS1; desde el 2005, unión de las antiguas European Article Number [EAN] y Uniform Code Council [UCC]), que es la organización más reconocida mundialmente en la elaboración de normas relativas a la distribución y suministro.

En España, es la Asociación de Fabricantes y Distribuidores de España (AECOC), como representante de GS1, la encargada de desarrollar y velar por el cumplimiento de los estándares EDI.

Aunque hay un mensaje EDI específico para la firma, esta se lleva a cabo mediante un mensaje CMS (*cryptographic message syntax*), derivado del estándar PKCS 7, usado para encriptar y firmar mensajes en una PKI. Pero, si la factura es EDIFACT, la RD 1496/2003 y la Directiva europea 2001/115 posibilitan la exoneración de la firma.

**3)** XML. Esta es otra sintaxis cuando el envío es de ordenador a ordenador. XML es un lenguaje extendido principalmente en América del Norte que poco a poco va ganando terreno en Europa. Existen diferentes variantes, las más importantes de las cuales son: UBL, protegido por OASIS, y el lenguaje GS1, protegido por la organización del mismo nombre. En España, la variante de factura CCI-AEAT, denominada *Facturae*, protegida por el Centro de Cooperación Interbancaria y la Agencia Tributaria es la más difundida, y dispone de sistemas de traducción en y desde UBL.

El formato de firma electrónica en XML se denomina XAdES. De las diferentes modalidades de firma XAdES, la más recomendable es XAdES–X-L, que incluye información sobre el tiempo en el que se llevó a cabo la firma electrónica e información sobre la validez del certificado electrónico cualificado que la acompaña.

Aquí nos centraremos en el formato XML, que se recoge en la norma europea TS 101 903.

El lenguaje XML (*extensible markup language*) es un lenguaje desarrollado por el World Wide Web Consortium (W3C), a partir del estándar XMLDSig, que permite definir la gramática de lenguajes específicos para estructurar grandes documentos, especialmente útil a la hora de comunicar entre sí varias aplicaciones. Cuando se usa el formato XML se emplea el lenguaje UBL universal (*universal business language*), que simplifica el intercambio de información financiera de manera automática, posibilitando la interoperabilidad de las facturas emitidas por cualquier Estado miembro de la Unión Europea.

Actualmente el formato XML se ha convertido, de hecho, en un estándar para el intercambio de información estructurada entre diferentes plataformas,

ya que permite, de manera fácil, la compatibilidad entre sistemas para compartir la información de una manera segura y fiable (como en el caso de la facturación electrónica) entre particulares.

De esta manera, cuando las facturas electrónicas se codifiquen en XML utilizaremos las firmas XML, aunque se pueden aplicar a cualquier tipo de documento, con independencia de su formato, destacando el formato XML *advanced electronic signature*, conocido como **firma XAdES**.

En toda firma XML, según el estándar XMLDSig, existen tres modalidades:

- *Enveloped*, en el que la firma se añade al final del documento XML como un elemento más. Este es el formato usado por *facturae*.
- *Enveloping*, en el que el documento se incluye dentro de la firma, en la que se referencia el firmante como objeto introducido en la firma.
- *Detached*, en el que la firma y el documento se separan en dos archivos (la URL (*uniform resource locator*) donde está el documento puede aparecer en la propia firma).

**Facturae**

Cuando el cliente es la Administración pública (Gobierno central, gobiernos autonómicos, ayuntamientos y diputaciones), a partir del 30/10/2010 las empresas están obligadas a remitir todas las facturas en formato electrónico utilizando la plataforma **www.facturae.es**.

La norma europea TS 101 903 establece también dos modalidades de firma electrónica que incluyen el sellado de tiempo. La variante T añade el sellado a una firma básica (BES) y la variante C, que además del sellado de tiempo añade información sobre la ruta de verificación de la validez del certificado obtenido de una consulta OCSP o de CRL. Por otro lado, esta misma norma prevé la modalidad X-L, que incluye información sobre el estado de revocación del certificado, con lo que obtiene de esta manera una firma que libera al receptor del problema de validación del certificado frente al proveedor de servicios.

**Las firmas electrónicas y** *facturae*

Las firmas electrónicas utilizadas en el caso de *facturae* se dan en las modalidades XAdES-BES y XAdES-X-L.

**XAdES** (*XML advanced electronic signatures*) es un conjunto de extensiones en las recomendaciones XML-DSig para adecuarlas a la firma electrónica avanzada.

Mientras XML-DSig es un marco general para la firma electrónica de documentos XML, XAdES especifica perfiles precisos de XML-DSig para ser utilizados con firma electrónica reconocida tal como se define en la Directiva 1999/93/CE.

Un beneficio importante de la XAdES es que los documentos firmados electrónicamente pueden continuar siendo válidos durante largos periodos de tiempo, incluso si los algoritmos criptográficos subyacentes se han roto.

La figura siguiente muestra la cadena de formatos XAdES de firmas electrónicas, según el nivel de protección que ofrece:

| Cadena de formatos XAdES | |
|---|---|
| **Formato** | **Descripción** |
| **XAdES-BES** | Forma básica, para firma electrónica avanzada |
| **XAdES-EPES** | Forma básica más información sobre la política de firma. |
| **XAdES-T** (*timestamp*) | Añade sellado de tiempo para proteger contra el repudio. |
| **XAdES-C** (*complete*) | Añade referencias a datos de verificación (certificados y listas de revocación) para permitir la verificación y la validación fuera de línea. |
| **XAdES-X** (*extended*) | Añade sellado de tiempo en XAdES-C para evitar que la cadena de certificados se pueda ver comprometida en un futuro. |
| **XAdES-X-L** (*extended long-term*) | Añade los certificados y las listas de revocación en los documentos firmados para permitir la verificación en el futuro, incluso si los originales ya no están disponibles. |
| **XAdES-A** (*archival*) | Añade la posibilidad de sellado de tiempo periódico de documentos archivados para prevenir que puedan ser comprometidos a causa del debilitamiento de la firma si permanecen archivados durante un largo periodo de tiempo. |

En cuanto a la perdurabilidad de las firmas a lo largo del tiempo, se debe tener en cuenta el tema de la validación de las firmas a largo plazo. Actualmente, por lo que respecta a la mayoría de las firmas, solo se realiza una comprobación de la CRL/OCSP (lista de certificados rechazados, con el protocolo de certificación en línea del certificado) en el momento de realizar la firma, pero no se conserva ninguna evidencia de esta. Así, cuando en el futuro se quiera comprobar la validez de la firma y el certificado ya haya caducado o se haya rechazado, no se podrá determinar si en el momento de firmar el certificado la firma era válida.

Para evitar este efecto, se recomienda usar procedimientos de firma que permitan crear una firma completa y autoverificable y que incorporen a la firma electrónica los elementos temporales (sello temporal de la autoridad de certificación) y de validación, que permiten verificar la firma sin ayuda externa. De esta manera, se podrán hacer las validaciones sin necesidad de conectarse en línea con ningún servicio de la autoridad de certificación.

Con el sellado de tiempo, el usuario, sin conexión a Internet, podrá tener una factura electrónica con toda la información necesaria para que sea válida independientemente del tiempo transcurrido.

**CAdES** (*CMS advanced electronic signatures*) es un conjunto de extensiones de sintaxis de mensajes criptográficos (*cryptographic message syntax, CMS*) de datos firmados mediante firma electrónica avanzada. Mientras que CMS es un marco general para la firma electrónica de documentos, como el correo electrónico (por medio de S/MIME ) o PDF, CAdES especifica perfiles precisos de CMS para ser usados con firma electrónica avanzada, tal como se define en la Directiva

1999/93/CE. Un beneficio importante de la CAdES es que los documentos firmados electrónicamente pueden continuar siendo válidos durante largos periodos de tiempo, incluso si los algoritmos criptográficos subyacentes han sido rotos.

La figura siguiente muestra la cadena de formatos CAdES de firmas electrónicas, según el nivel de protección que ofrece:

| Cadena de formatos CAdES | |
|---|---|
| **Formato** | **Descripción** |
| **CAdES** | Forma básica, para firma electrónica avanzada. |
| **CAdES-T** (*timestamp*), | Añade sellado de tiempo para proteger contra el repudio. |
| **CAdES-C** (*complete*) | Añade referencias a datos de verificación (certificados y listas de revocación) para permitir la verificación y la validación fuera de línea. |
| **CAdES-X** (*extended*) | Añade sellado de tiempo en CAdES-C para evitar que la cadena de certificados se pueda ver comprometida en un futuro. |
| **CAdES-X-L** (*extended long-term*) | Añade los certificados y las listas de revocación en los documentos firmados para permitir la verificación en el futuro, incluso si los originales ya no están disponibles. |
| **CAdES-A** (*archival*) | Añade la posibilidad de sellado de tiempo periódico de documentos archivados para prevenir que puedan ser comprometidos a causa del debilitamiento de la firma si permanecen archivados durante un largo periodo de tiempo. |

# 3. Los sistemas de facturación electrónica

Tal como hemos dicho, la factura electrónica es un tipo de factura que se diferencia de la factura en papel por la forma de gestión informática y el envío mediante un sistema de comunicaciones que, conjuntamente, permite garantizar la autenticidad y la integridad del documento electrónico.

**Integración de la e-factura**

La factura electrónica gana potencia cuando se integra en los procesos de gestión de la empresa, tanto respecto a su emisión como en cuanto a su recepción. Así se multiplican los beneficios al tratar los documentos de manera eletrónica dentro de la empresa.

Una factura electrónica se construye en dos fases: en la primera se crea la factura tal como se ha hecho siempre y se almacena en un fichero de datos y, en la segunda, se procede a su firma con un certificado electrónico, propiedad del emisor, que cifra el contenido de factura y, de manera opcional, se añade el sello digital (*time stamping*). Esta firma electrónica, generada por el emisor, permitirá al receptor verificar la integridad de la firma y la autenticación del firmante. Los algoritmos criptográficos utilizados tanto por el *hash* del documento como por la firma deben estar plenamente aceptados por la comunidad internacional: por ejemplo, RSA y DSA, para la firma, y SHA como función *hash*.

El sellado de tiempo en los documentos electrónicos contiene el resumen (el *hash* del documento), la fecha y la hora en la que fue generado, obtenido de una fuente fiable, y la firma electrónica. Estos sellos permiten garantizar que la información contenida en el documento no se ha modificado desde el momento en el que se generó el sello y se puede adjuntar a la información para garantizar su no rechazo (pensad en la importancia del sellado de tiempo en los contratos con las compañías de seguros).

El emisor envía la factura al receptor por medios electrónicos, como CD, memorias USB e, incluso, Internet. Si bien se dedican muchos esfuerzos para unificar los formatos de factura electrónica, actualmente está sometida a distintas normativas y tiene diferentes requisitos legales exigidos por las autoridades tributarias de cada país, de manera que no siempre es posible el uso de la factura electrónica, especialmente en las relaciones con empresas extranjeras, que tienen normativas diferentes a la del propio país.

Los requisitos legales respecto al contenido mercantil de las facturas electrónicas son exactamente los mismos que regulan las facturas en papel. Los requisitos legales en relación con la forma imponen un determinado tratamiento para garantizar la integridad y la autenticación y ciertos formatos que faciliten la interoperabilidad.

La factura electrónica permite que instituciones, empresas y profesionales dejen atrás las facturas en papel y las reemplacen por la versión electrónica del

documento tributario. Tiene exactamente la misma validez y funcionalidad tributaria que la factura tradicional en papel. Todo el ciclo de la facturación puede ser administrado en formato electrónico.

### 3.1. Requisitos de todas las facturas

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 son:

- Número de factura, y si es necesario, serie.
- Fecha de expedición.
- Nombre y apellidos, o razón social, del emisor y del receptor.
- NIF del emisor y del receptor.
- Domicilio fiscal de los dos tributadores: del emisor y del receptor.
- Descripción de las operaciones (base imponible).
- Fecha de la entrega del bien o de la prestación del servicio (si es distinta a la de expedición).
- Referencia, de manera inequívoca, al albarán, si lo hay.
- Tipo impositivo aplicable a la operación.
- Cuota tributaria o repercutida.

Para cumplir 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 firmada mediante una firma electrónica avanzada, basada en certificado reconocido, y ser transmitida de un ordenador a otro, recogiendo el consentimiento de ambas partes.

**Renuncia a la facturación electrónica**

En cualquier momento, tanto el emisor como el receptor de facturación electrónica puede renunciar a continuar con el procedimiento.

Puede haber otros requisitos, marcados por parte del emisor o del receptor, dirigidos a facilitar la conciliación automática de las facturas en los sistemas de información propios.

### 3.2. Obligaciones legales para el emisor

**1) Consentimiento del receptor**. Este consentimiento se podrá formular de manera expresa por cualquier medio, verbal o escrito (según el artículo 2 de la Orden 962/2007). También se deberá acordar con el receptor el formato de la factura electrónica y cuál debe ser el medio telemático de envío.

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

**3) Firma electrónica reconocida**. Para garantizar la autenticidad del origen y la integridad de las facturas.

**4) Remisión telemática**. El fichero de la factura electrónica, en el formato acordado, se transmite por cualquier medio de comunicación electrónico y/o digital, desde el ordenador del emisor al ordenador del receptor para su proceso administrativo, incluidos el de contabilización y anotación en los registros del IVA, según directrices de la autoridad tributaria.

**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. Si se conserva la matriz de la factura, ya no es necesario conservar las copias de las facturas electrónicas firmadas, ya que a partir de la matriz se pueden volver a generar.

**Matriz de la factura**

Se entiende por matriz de una factura electrónica el conjunto de datos, tablas, bases de datos y/o ficheros que contienen todas los datos reflejados en la factura, junto a los programas que permitieron generarla.

**6) Conservación durante el periodo de prescripción**. La ley exige conservar las facturas de los últimos cinco años. Para conservar las facturas electrónicas correctamente, hay que tener en cuenta la Orden EHA 962/2007, en la que se recoge la validez de la digitalización de las facturas y la homologación del software necesario, así como admite la impresión de las facturas electrónicas por medio del código PDF-417.

En el supuesto del artículo 6 de la Orden EHA-962/2007, un documento impreso en papel con este código es válido siempre que se mantenga el mencionado repositorio en el que está el documento y su firma electrónica, cuando existe un mecanismo de verificación de la firma y se puede acceder de manera completa al documento mediante este código electrónico de autenticación. Esta es la solución más sencilla: indicar en la factura impresa la URL o el localizador del documento electrónico de donde procede la factura en papel. De esta manera se dispone de la misma validez que puede aportar la impresión con PDF-417. Además, la conversión a documento electrónico es inmediata, simplemente accediendo a la fuente, de manera que cualquiera puede comparar el contenido del papel con el documento electrónico.

**El artículo 6 de la Orden EHA-962/2007 prevé una solución alternativa**

Cuando el emisor y/o receptor de facturas y documentos sustitutivos electrónicos sea un tercero que actúa en nombre y por cuenta de los obligados tributarios deberá cumplir los requisitos expresados anteriormente. No obstante, una vez cumplidos, podrán poner a disposición de sus clientes aplicaciones informáticas que gestionen un repositorio de facturas y documentos sustitutivos emitidos o recibidos, según corresponda, junto con la firma electrónica generada o verificada en los términos de esta orden, proporcionando un código de autenticación de mensajes asociado a cada documento. Este código permitirá el acceso al documento asociado existente en el repositorio y garantizará, a quien acceda a él, que cumple los requisitos previstos en esta orden.

**7) Garantía de accesibilidad completa**. Se deben gestionar las facturas de manera que permitan: la visualización, la búsqueda selectiva, la copia o la descarga en línea y la impresión. Esta es una obligación inherente a la conservación de las facturas por medios electrónicos que trata de facilitar la auditoría e inspección de las facturas electrónicas.

**8) Subcontratación a un tercero**. Todas las fases anteriores pueden ser subcontratadas a un tercero, sin que el emisor pierda su responsabilidad respecto a las obligaciones tributarias.

### 3.3. Obligaciones legales para el receptor

**1) Recepción de la factura por medio electrónico**. El receptor se debe asegurar de la legibilidad en el formato original en el que se haya recibido, así como, si es necesario, de las fechas asociadas y los mecanismos de verificación de firma. Para ello, el receptor debe conservar los originales firmados, lo que permitirá la verificación de los contenidos mínimos exigibles de la factura y la verificación segura de la firma electrónica.

**Regulación según la Orden EHA 962/2007**

Esta orden regula la obligación que tiene el receptor de verificar la firma y comprobar la validez de los certificados de las facturas trasmitidas por medios electrónicos. Es decir, el receptor deberá disponer del software necesario que le permita saber si la firma de la factura es válida o no.

**2) Herramientas de verificación de firmas y vigencia de certificados**. Deberá disponer de herramientas que permitan la verificación de la firma y de la identidad del emisor, al mismo tiempo que deberá poder verificar la vigencia del certificado del emisor; es decir, que el certificado utilizado para la generación de la firma electrónica no ha perdido su eficacia por revocación, caducidad o cualquier causa establecida en el ordenamiento jurídico.

**3) Contabilización y anotación en registros de IVA**. Siguiendo las directrices de la autoridad tributaria.

**4) Conservación durante el periodo de prescripción**. Eventualmente, podrá conservar la factura impresa con marcas gráficas (nubes de puntos) en formato PDF-417. O, alternativamente, tal como se ha mencionado en el caso de la emisión, haciendo uso de lo que dispone el artículo 6 de la Orden EHA-962/2007.

**5) Garantía de accesibilidad completa**. Se deben gestionar las facturas de manera que permitan la visualización, la búsqueda selectiva, la copia o la descarga en línea y la impresión.

**Obligaciones de los terceros**

En la facturación, electrónica o no, siempre hay dos obligados tributarios: el que tiene la obligación de remitir la factura, y guardar al menos la matriz, y el cliente, que tiene la obligación de recibirlas y conservar las facturas tal cual.
Estas obligaciones se pueden ceder a terceros para que actúen en nombre del obligado tributario.
En cualquier caso, los responsables últimos ante las autoridades tributarias son los obligados tributarios, es decir, el profesional que debe expedirla y su cliente destinatario.

**6) Subcontratación a un tercero**. Todas las fases anteriores pueden ser subcontratadas a un tercero, sin que el receptor pierda la responsabilidad.

### 3.4. Conservación electrónica de las facturas

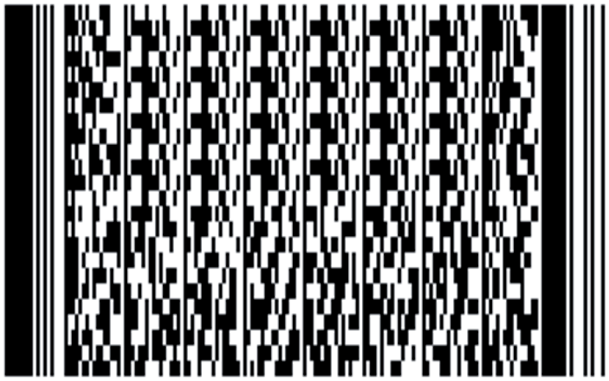
La ley exige conservar las facturas de los últimos cinco años, lo que implica archivar, gestionar y conservar los documentos correspondientes.

La factura electrónica es un fichero informático y, como tal, se puede guardar en diferentes soportes: disquete, CD-ROM, memoria USB, disco duro o papel.

Respecto a las facturas electrónicas, se establece que el receptor puede conservar las facturas en el mismo formato y soporte original en el que fueron emitidas, salvo que se opte por alguna de las formas de conversión autorizadas en la Orden EHA/962/2007. Según esta orden, podemos considerar dos procedimientos para la conservación de las facturas: el de conservar electróni-

camente una factura en papel, mediante una digitalización certificada, y el de conservar en papel una factura electrónica, mediante el formato PDF-417.

La figura siguiente muestra la nube de puntos del código PDF-417:



En el primer caso, si así se quiere, la digitalización certificada consiste en el proceso por el que se transforman las facturas recibidas en papel en una imagen digitalizada (escáner) que después se firmará electrónicamente. Una vez realizada la digitalización certificada de una factura, se puede destruir el documento en papel, ya que el documento transformado tiene el carácter de original.

Para realizar la digitalización certificada basta con utilizar software homologado por la Agencia Tributaria.

En el segundo caso, el de querer conservar en papel una factura electrónica, se utiliza el formato PDF-417, aunque actualmente ya ha caído en desuso porque no es un requisito de la facturación electrónica y, además, es necesario un software especial para poder imprimir las facturas en formato electrónico. No obstante, cuando se emitan facturas en papel, se deberá adjuntar un conjunto de códigos PDF-417 que recojan en un fichero UBL todos los datos de la factura con el fin de facilitar su digitalización.

**e-factura en papel**

Siempre es más sencillo enviar la factura electrónica en cualquier formato, firmada electrónicamente, de manera que el receptor, si quiere, la pueda abrir e imprimir.
La e-factura firmada electrónicamente es lo único que se debe conservar para la inspección tributaria.

La Orden ministerial EHA/962/2007 define los elementos necesarios para convertir las facturas recibidas en papel en su equivalente electrónico, siempre que en la operativa de digitalización se utilice un proceso que garantice que el resultado de la digitalización es imagen fiel del documento original en papel y que el dispositivo de digitalización (escáner) produce la imagen acompañada de una firma electrónica cualificada, tal como se define en la Directiva comunitaria 1999/93. El proceso se denomina digitalización certificada.

Para poder realizar este tipo de impresión, la factura electrónica que se ha recibido deberá haber sido emitida con un software específico que genere e incluya en la factura electrónica esta nube de puntos del código PDF-417. Además, en esta normativa se indica que las facturas electrónicas se pueden transcribir en papel incluyendo marcas gráficas de autenticación, producidas según la especificación PDF 417, tal como se dispone en la Resolución de la AEAT 2/2003.

La impresión de una factura electrónica en formato PDF-417 tiene validez legal, ya que este formato incluye en el documento impreso un código, en nube de puntos, para su identificación y validación. Esta nube de puntos es una marca gráfica que incluye el contenido íntegro de los datos de la factura y la firma electrónica del fichero.

## 3.5. Procedimientos de emisión y recepción de facturas electrónicas

Se ha dicho que la obligación básica del emisor es firmar la factura electrónicamente y la del receptor, verificar la factura y conservarla en el formato original.

Suponiendo que disponemos de una plataforma de facturación electrónica y del correspondiente certificado electrónico reconocido por una autoridad de certificación, vamos a describir los procedimientos de emisión y recepción de facturas electrónicas.

Respecto a la **emisión de facturas electrónicas**, se siguen los pasos siguientes:

**1)** Con la plataforma de facturación electrónica se genera la factura o la recuperamos de una base de datos del propio sistema de información de la empresa, donde están almacenados los ficheros o matrices de las facturas.

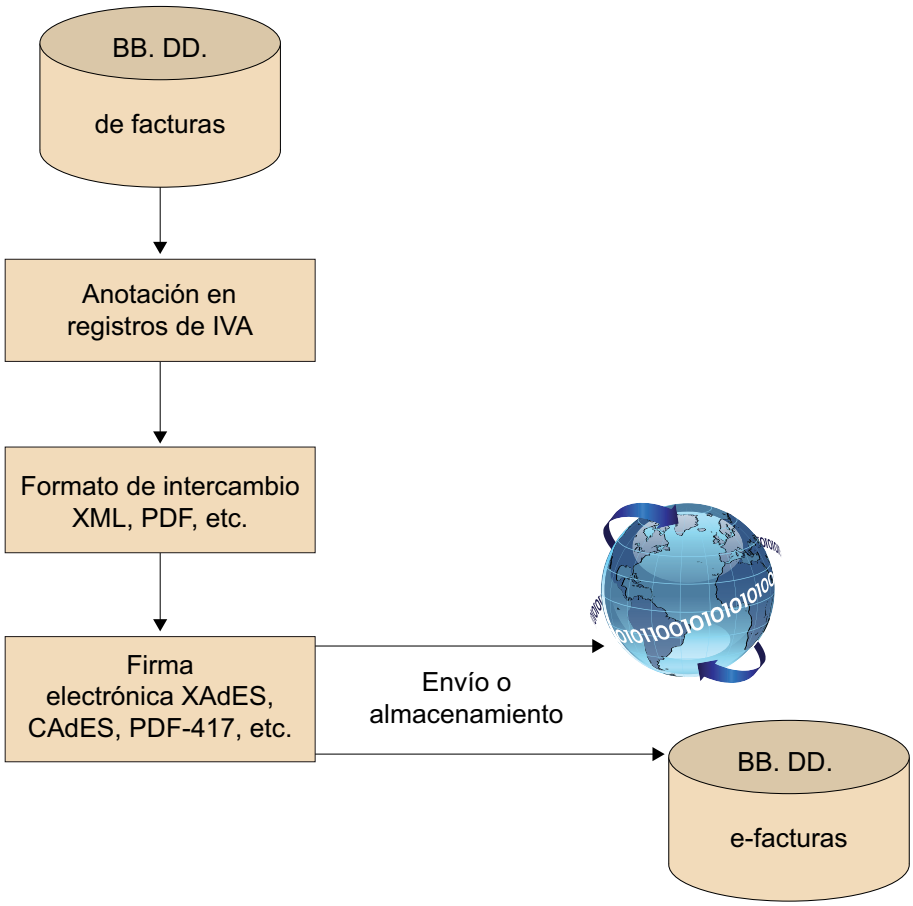
**2)** Una vez recuperada la factura, se hace la correspondiente anotación en los registros de IVA de la empresa, si no lo ha hecho automáticamente la plataforma de facturación.

**3)** La factura se codifica en el formato de intercambio elegido, según el medio de transmisión posterior.

**4)** La factura es firmada electrónicamente, según el formato elegido, con la clave privada del emisor. Es interesante que la aplicación elegida pueda verificar la firma, es decir, determinar si es válida o no, si está caducada o si se ha revocado. De esta manera se asegura que se ha enviado al receptor una factura electrónica con una firma correcta.

**5)** La factura firmada es enviada o almacenada en una base de datos a la que podrá acceder el receptor. La podemos enviar por correo electrónico, a través de una plataforma web (*Web service*), o en papel, por correo ordinario, para lo que se deberá imprimir el código PDF-417 o alternativamente el código de autenticación. En cuanto al almacenamiento, se supone que la plataforma de facturación electrónica las depositará en lugares seguros y de una manera estructurada, para facilitar su recuperación por fecha, nombre, CIF, etc.

La figura siguiente muestra el diagrama del flujo de emisión de facturas electrónicas:




Respecto a la **recepción de facturas electrónicas**, en primer lugar se debe saber cómo se recibirá la factura y por qué medio telemático se recibirán: si por correo electrónico, si debemos descargarla de una página web (en este caso deberá introducirse un nombre de usuario y clave de paso), si en papel, recibida mediante correo ordinario, donde se ha incluido el código PDF-417 o el código de autenticación, etc.

Una vez recibida o recuperada la factura electrónica, se siguen los pasos siguientes para su gestión:

**1)** Se debe verificar la validez de la firma electrónica, comprobando primero si el certificado electrónico con el que se ha firmado es válido o no lo es. A través de las listas CRL de las autoridades de certificación: si el certificado no es válido, entonces tampoco lo será la factura que lo contiene.

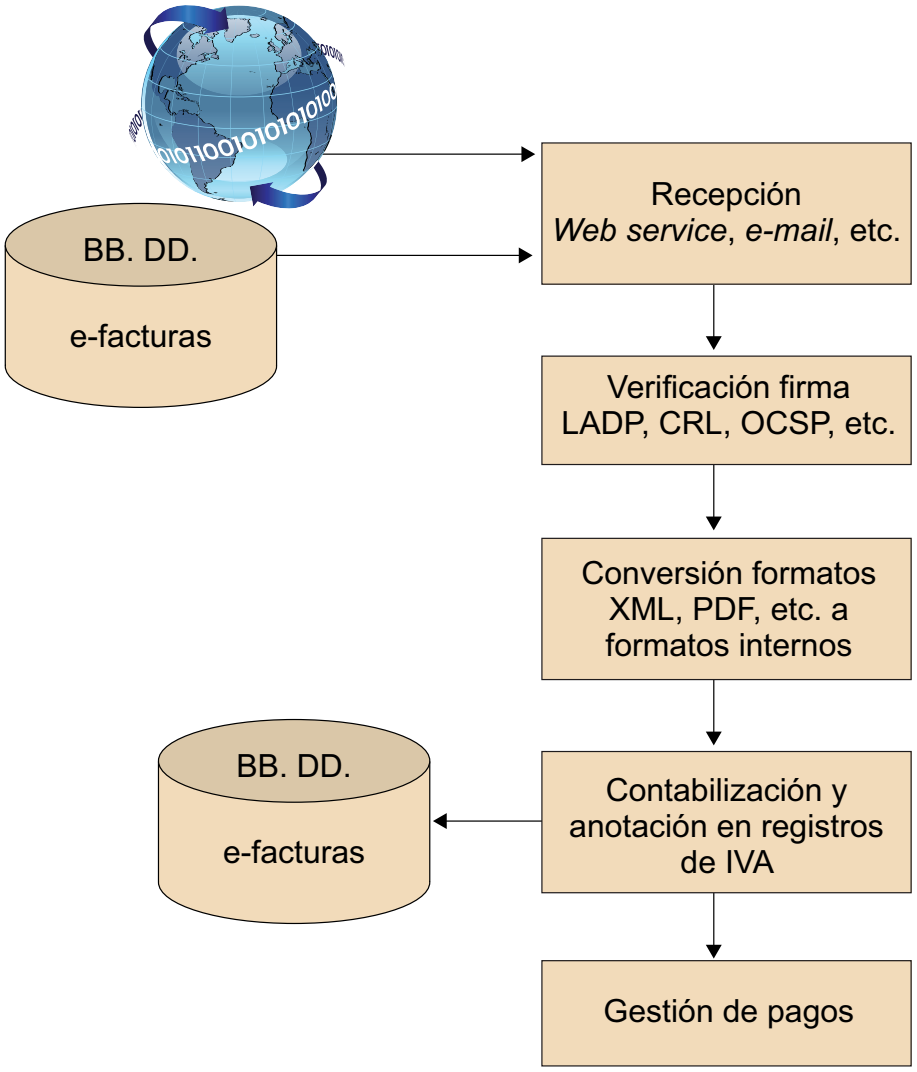
**2)** Convertir el formato de la firma recibida en el formato interno para su gestión, especialmente para poderlas integrar en los ERP de la empresa.

**3)** Contabilizar la factura en la contabilidad de la empresa y hacer las anotaciones pertinentes en los registros de IVA.

**Verificación en CRL**

En Internet hay visores gratuitos que permiten ver el estado de la firma y aplicaciones estándar que, si encuentran un fichero PDF firma, automáticamente verifican la validez de la misma.
Con un visor de firmas podremos ver las propiedades del certificado: saber quién lo ha emitido, si el documento se ha modificado después de haberlo firmado y, si procede, consultar el sello temporal.

La figura siguiente muestra el diagrama del flujo de recepción de facturas electrónicas:




Asimismo, existen otros modelos de facturación electrónica, como las plataformas de terceros y la autofacturación.

**Plataformas de terceros y autofacturación**

Recordemos que en la facturación, aplicando la legislación a la modalidad electrónica, hay dos obligados tributarios:

- Un profesional o empresario, que tiene la obligación de enviar telemáticamente las facturas en formato electrónico, si así lo ha solicitado expresamente el cliente, firmadas electrónicamente y conservar al menos su matriz.

- Un cliente, que tiene la obligación de recibirlas y conservar las facturas en el mismo formato que las ha recibido.

Se puede optar por dar cumplimiento a estas obligaciones mediante sistemas informáticos propios con los que ejecutar todos los servicios de la facturación electrónica de emisión, de firma, de envío y de conservación.

Pero también se puede optar por ceder y delegar estas obligaciones. Existen dos modelos de delegación: acudir a plataformas de terceros o a la autofacturación.

**Plataformas de terceros**: En este caso, el emisor puede ceder la expedición, la firma y el envío de las facturas a un tercero, así como la conservación de las facturas o sus matrices. Por otro lado, el receptor puede ceder la recepción y conservación de las facturas.

Esta opción es la más práctica para las pequeñas y medianas empresas, ya que se simplifican las tareas y el esfuerzo, y normalmente el coste es proporcional al número de facturas electrónicas emitidas y/o recibidas.

**Autofacturación**: En este caso es el receptor de la factura quien emite la factura electrónica, de tal manera que es el propio cliente quien controla el formato y garantiza la conciliación contable.

**Observación**

Es muy importante tener en cuenta que siempre, independientemente del modelo elegido, los responsables últimos ante las autoridades tributarias son los obligados tributarios; es decir, el profesional o el empresario (emisor) que debe expedir la factura y el cliente destinatario (receptor).

## 4. Descripción de un caso real

**Coautores**

En la redacción de esta sección hemos contado con la inestimable colaboración de los consultores de facturación electrónica **Margarita Martínez Aguiló** y **Joan Miquel Ramon Tur**, que han aportado su experiencia en la implantación de soluciones de factura electrónica, tanto en el ámbito de grandes empresas como en el diseño e implementación de plataformas de facturación electrónica.

Para abordar la implantación de la factura electrónica en una empresa, los requisitos dependerán en gran medida del alcance del proyecto, dependiendo esencialmente del volumen de facturas que la empresa maneja, tanto recibidas como emitidas.

En este sentido, se puede comenzar solo emitiendo facturas electrónicas, o solo recibiéndolas, y hacerlo en cualquier momento. Además, no es necesario facturar electrónicamente a todos los clientes de la empresa, ni tampoco que todas las facturas emitidas en un mismo ejercicio para el mismo cliente sean electrónicas.

Existen muchas maneras de implantar la factura electrónica en una empresa, desde el envío por correo electrónico de facturas en formato PDF firmadas, hasta la implantación de soluciones avanzadas integradas en los sistemas propios de la empresa, pasando por soluciones intermedias, como las plataformas de facturación independientes del resto de los sistemas de la empresa.

Antes de poner en marcha un proyecto de facturación electrónica, se deben considerar una serie de parámetros para elegir la plataforma (aplicación informática y certificado electrónico) que se adapte mejor a las necesidades de la empresa y al presupuesto disponible.

Respecto al coste de la implantación de la facturación electrónica, este dependerá, básicamente, de varios factores:

**1) Situación inicial**: el coste variará dependiendo de si la empresa dispone o no del software o hardware que se requiere para emitir y/o recibir facturas electrónicas.

**2) Necesidades**: no es lo mismo tener que emitir facturas electrónicas a todos los clientes de la empresa que solo a una parte de esta.

**3) Modalidad**: el coste de facturar electrónicamente con plataformas de terceros es diferente del coste que hay que invertir cuando la facturación electrónica se realiza totalmente con sistemas propios.

La inversión será proporcional al ahorro de costes, de tiempo y al aumento de la eficiencia que se quiera obtener. Se pueden poner en marcha proyectos

de facturación electrónica con un presupuesto bajo, pero si se quiere la integración en los sistemas de gestión de la empresa, aumenta el precio de la implantación, al mismo tiempo que los ahorros globales del procedimiento de facturación son también más elevados.

### 4.1. Refexiones sobre la implantación de una solución de facturación electrónica

Antes de abordar la implantación de una solución real de facturación electrónica, haremos unas reflexiones, desde la experiencia, que pueden ser de utilidad.

El argumentario más común para la implementación de la factura electrónica en una empresa se basa en estas consideraciones:

- **Disminución de costes**:

  **1)** **Variables**. Dependiendo de la cantidad de facturas emitidas. Papel, tóner, franqueo, personal, etc.

  **2)** **Fijas**. Recursos e infraestructuras para emitir las facturas. Por ejemplo, impresoras, plegadoras, personal, archivo, etc.

- **Simplificación de los procesos administrativos**: la manipulación física pasa a ser informática/telemática. Esto incluye archivo y comunicación de rechazo del cliente.

- **Mejora del circulante** por optimización de la gestión de cobro:

  **1)** La factura entra antes en el circuito de pago del cliente.

  **2)** Disminuyen las facturas en vía muerta.

- **Mejora en las relaciones comerciales**:

  **1)** Evitando discrepancias por asuntos administrativos.

  **2)** Creando un ambiente ágil de intercambio de información.

Pero la realidad es que existe una implantación progresiva y emisión muy lenta de facturas hasta que se consigue la sustitución total de las facturas en papel, con lo que no se consiguen la mayoría de las mejoras mencionadas anteriormente, ni la disminución de costes, ni la simplificación de procesos (durante un cierto tiempo se duplican). Por tanto, para alcanzar el objetivo de la implementación de la facturación electrónica, se debe tener en cuenta que:

- Es necesario realizar esfuerzos e invertir recursos para que los clientes acepten la factura electrónica.

- Es un objetivo difícil de alcanzar a corto plazo.

  Por esta razón, durante un periodo más o menos largo, se produce una convivencia de emisión de facturas electrónicas y facturas en papel. Esta situación se da en una gran mayoría de empresas y es el caso más común y la principal barrera de entrada que interesa analizar con profundidad.

Otras barreras de entrada, que provocan que las empresas no quieran abordar la facturación electrónica, radican en el hecho de que existen muchas plataformas de facturación electrónica de terceros al mismo tiempo que provocan un aislamiento de estas diferentes plataformas. La competencia entre ellas hace que sea muy difícil la interoperación; además, ofrecen valores añadidos diferentes según criterios de su negocio: las asociadas a bancos, ofreciendo *factoring* o *confirming*; las asociadas a centrales de compras, ofreciendo pedido/albarán; las que proceden del mundo de la gestión documental, ofreciendo otros servicios, entre otros. En general, la casuística de la gestión de las facturas es muy amplia, pero podemos destacar que:

- Existen muchas empresas que quieren emitir o recibir la factura en papel. En particular, aquellas que entregan las facturas junto a la mercancía y la entregan al cliente en mano (por ejemplo, clientes directos en los hoteles) y las que requieren adjuntar a la factura otros documentos (trazabilidad, bonos, albaranes, etc.).

- Cuando hay un volumen de facturas muy elevado, no se justifica el hecho de pagar una variable por factura en la plataforma de un tercero; a la empresa le interesa más un desarrollo propio.

- Cuando la empresa tiene una venta directa mediante su portal web, hay receptores muy deslocalizados, diferentes países y distintas legislaciones.

- Los emisores con un número muy bajo de facturas aceptan hacer uso de una plataforma pero les parece caro, aún más si no pueden establecer relaciones con todos sus receptores, o si se las envían a ellos por otro canal.

El planteamiento para abordar los requisitos de la implantación de la factura electrónica en una empresa dependerá, en gran medida, del alcance del proyecto, pero en nuestro caso nos fijaremos en el cumplimiento de cinco objetivos que creemos que son claves para la correcta adopción, por parte de la empresa, de la factura electrónica.

**1)** Involucrar a los terceros (clientes y proveedores) en el uso de la factura electrónica, facilitando la gestión del consentimiento y del establecimiento de la relación.

**2)** La integración de los datos estructurados de la factura electrónica entre el sistema de gestión y los terceros (sistemas de los receptores/emisores).

**3)** Garantizar la autenticidad de la factura electrónica y el cumplimiento legal.

**4)** Permitir gestionar los distintos eventos relacionados con la factura electrónica (pagada, rechazada, incidencias).

**5)** Custodiar la factura electrónica legalmente, facilitando la conciliación y dando soporte para el cobro.

La necesidad de plantearlo como un proyecto se justifica porque con el fomento del uso de la factura electrónica se ha hecho necesario gestionar legalmente situaciones no previstas antes:

- Gestionar los distintos medios, canales y formatos para enviar o recibir facturas electrónicas (en lugar de un único canal, el papel).
- Concentrar en un repositorio los diferentes almacenes de facturas electrónicas (por ejemplo, las recibidas de la operadora de teléfonos y la de la luz de cada una de sus webs).
- La necesidad de gestionar el consentimiento y la información de cómo se reciben o se envían las facturas electrónicas (por ejemplo, qué formato PDF/XML, si es necesario un aviso por correo electrónico, etc.).
- La necesidad de generar firmas electrónicas y disponer de mecanismos de validación de las facturas electrónicas recibidas.

## 4.2. Implantación de una solución de facturación electrónica: caso real

### La empresa

Nos centraremos en el caso de que la empresa interesada en implantar la solución de facturación electrónica es una cadena hotelera que dispone de varios centenares de hoteles dispersos en diferentes países y continentes. Algunos de los hoteles son propios y otros solo los gestiona cobrando por este servicio de gestión.

La organización se basa en una sola central administrativa desde donde se intenta supervisar y realizar la mayoría de los cobros y pagos. Idealmente, en la central administrativa se deberían recibir y emitir todas las facturas. Actualmente esto no es posible por dos factores:

- Muchos proveedores locales de productos perecederos (pan, verduras y otros alimentos) remiten las facturas a los hoteles directamente.

- Los hoteles tienen la necesidad de emitir las facturas y cobrar a los denominados clientes directos, que son los que llegan al hotel sin un bono emitido por la agencia de viajes u otro intermediario.

La central administrativa tiene, actualmente, otro problema más importante para realizar su labor y deriva del hecho de que depende completamente de los datos que recibe de cada uno de los hoteles, sean propios o gestionados. No todos los hoteles utilizan los mismos aplicativos de gestión, lo que tiene como consecuencia que los datos que se reciben no son homogéneos en el formato ni en la información que se puede extraer de ellos.

**Las expectativas**

La empresa apuesta firmemente por la facturación electrónica y se inicia el proyecto con los objetivos siguientes:

- Disminuir los costes y ser más eficientes.

- Contribuir a la política medioambiental estimando que con el proyecto podría llegar a ahorrar el consumo de cerca de seis toneladas de papel al año.

- Mejorar sustancialmente su servicio y las relaciones con sus clientes y proveedores para evitar errores, pérdidas de documentación y gestionar más rápidamente las incidencias que se producen.

- Disminuir el tiempo transcurrido entre la emisión y el cobro de las facturas.

- Obtener un beneficio (o descuento en su emisión) para cada proveedor que ellos aporten a la plataforma de facturación electrónica.

**Solución de facturación electrónica adoptada y acuerdo comercial**

Después de considerar que internamente no se tienen suficientes conocimientos, ni técnicos ni legales, sobre facturación electrónica, se opta por una solución de factura electrónica completamente externa a la organización. Se estudian las alternativas que cumplen los requisitos legales y técnicos. Finalmente

se firma un acuerdo comercial con una plataforma de facturación, que ofrece la factura electrónica como un servicio.

La plataforma de facturación seleccionada garantiza, a emisores y a receptores, el estricto cumplimiento de la legislación vigente en materia de firma y facturación electrónica, con servicios de delegación de firma y custodia legal (actuando como tercera parte de confianza), preparada para aceptar a los prestadores de servicios de certificación reconocidos por la AEAT. Además, ofrece comprobación de la validez de los certificados electrónicos que acompañan a la factura.

Desde el punto de vista técnico, también proporciona seguridad a las transacciones electrónicas, soporta múltiples formatos de entrada y salida, una administración simple y flexible. También servicios web necesarios para poder integrarse con los sistemas de información de la empresa, lo que es muy necesario para la automatización de los flujos de trabajo y de datos de la empresa.

**Fases del proyecto**

Analizando con un poco más de detalle el proyecto, se observa que los sistemas y procedimientos afectados por la emisión de facturas son muy distintos a los afectados por la recepción de facturas. Con estas premisas, el proyecto se divide en dos fases: recepción de factura electrónica y emisión de factura electrónica.

Se decide que la primera fase sea la que más ahorros de costes proporcione, por lo que se valoran como más significativos:

| Emisión | Recepción |
|---|---|
| Impresión: consumibles y papel | Manipulación, clasificación |
| Envío: ensobrado y correo | Extracción y contabilización de la información |

El coste más elevado corresponde, en ambos casos, a los recursos humanos dedicados a la tarea, y sin duda las mayores dedicaciones son las de traspasar los datos del papel a los sistemas de información de la empresa, así como los de contabilizar las facturas recibidas.

De esta manera, la **primera fase** es la que hace referencia a la recepción de facturas electrónicas. Esta fase se aborda en tres subfases:

**1)** Prueba piloto con dos proveedores de confianza: se realizan pruebas de envíos, hasta que se dan por válidos y se pone el sistema en producción. Durante esta prueba piloto no se aborda la integración en los sistemas contables de la

cadena, por lo que se continúa contabilizando manualmente. Esto implica que en esta fase no se obtienen los ahorros esperados.

**2)** Extensión a treinta proveedores más. Se seleccionan aquellos de los que se recibe mayor volumen de facturas.

**3)** Resto de proveedores: mismos pasos que en la subfase anterior.

La **segunda fase** es la que hace referencia a la emisión de facturas electrónicas. También se planea en tres subfases:

**1)** Hacer un piloto con una agencia de viajes (minorista) y con un operador turístico (mayorista).

**2)** Extensión a cinco operadores turísticos y cinco agencias de viajes.

**3)** Incorporación gradual del resto de los clientes, teniendo en cuenta la casuística del cliente directo, que se quiere llevar la factura en mano.

En ambas fases del proyecto se han tenido que abordar aspectos y tareas técnicas y funcionales y otras de tipo más logístico y comercial.

Las primeras obviamente se han asumido por parte de la dirección de los sistemas de información de la cadena hotelera y las segundas por parte de los recursos comerciales, tanto de la propia cadena hotelera como de la empresa que gestiona la plataforma de facturación.

Respecto a la parte **técnica y funcional** del proyecto de implantación, se puede destacar fundamentalmente la necesidad de conectar los sistemas de información de todos los agentes involucrados con la cadena hotelera, es decir, la propia cadena, sus clientes y sus proveedores (la integración debe contemplar recibir facturas de la plataforma, así como también enviarlas) y de integrar la información en los sistemas de información de cada uno de los intervinientes en la relación comercial con la cadena.

Una vez que todos los agentes involucrados se comunican utilizando la plataforma, surgen problemas que resolver y que no tienen nada que ver con la factura electrónica y su presentación o formato. Están más bien relacionados con la información contenida y la semántica exacta de cada dato. Esto exige una solución mediante consultoría, que se debe hacer con mucho cuidado, y en la que es necesario que un consultor especializado en la plataforma haga de intermediario entre la cadena de clientes y proveedores para conseguir el acuerdo entre las partes.

Respecto a la parte logística y comercial del proyecto de implantación y para que el proyecto tenga éxito, se detecta como un elemento crítico el hecho

de que se sumen al proyecto cuantos más proveedores y clientes se pueda. Para alcanzar tanta involucración como sea posible se elabora una campaña promocionando la solución de factura electrónica entre los clientes y proveedores. La campaña incluye diferentes tipos de acciones y un seguimiento del cumplimiento de los objetivos marcados.

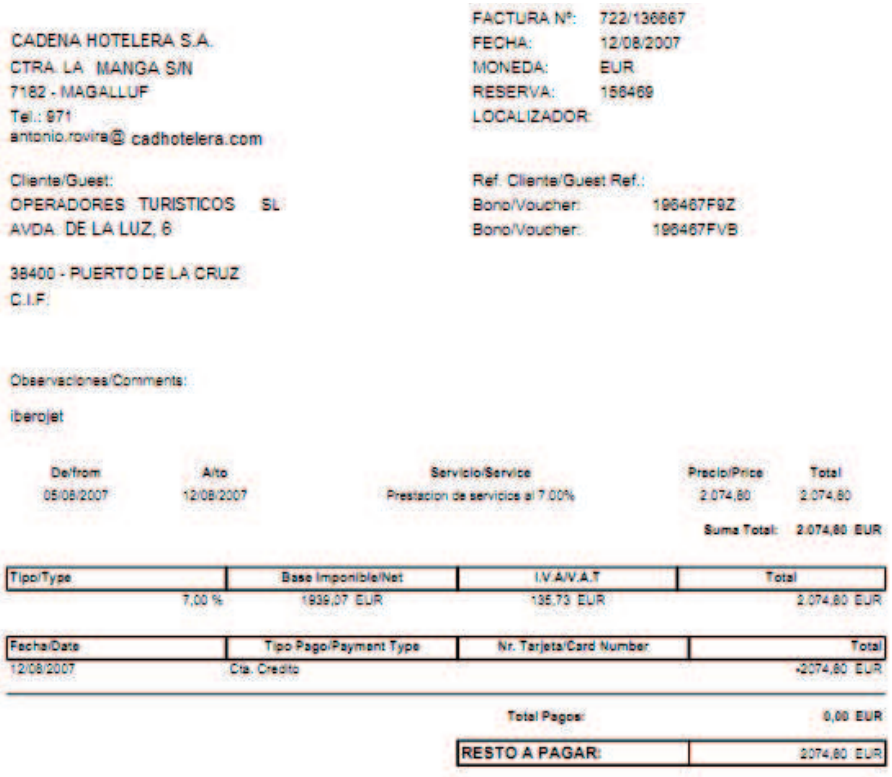
### Conclusiones

Aunque el proyecto ha ido cumpliendo sus fases, su éxito no ha sido completo al no cubrirse todas las expectativas planteadas inicialmente por ciertas razones fundamentales:

- La masa de clientes y proveedores se suman muy lentamente al proyecto. Esto provoca que la sustitución total de las facturas en papel por las electrónicas plantee cada vez un horizonte más lejano.

- El coste de adhesión de clientes y proveedores es más alto de lo considerado, por las diferentes casuísticas e incidencias que hay que resolver.

- Para conseguir enviar y recibir la mayor cantidad de facturas de manera electrónica, no queda más remedio que plantearse adherirse a otras plataformas de factura electrónica:



CADENA HOTELERA S.A.
CTRA. LA MANGA S/N
7182 - MAGALLUF
Tel.: 971
antonio.rovira@ cadhotelera.com

FACTURA Nº: 722/136667
FECHA: 12/08/2007
MONEDA: EUR
RESERVA: 156469
LOCALIZADOR:

Cliente/Guest:
OPERADORES TURISTICOS SL
AVDA. DE LA LUZ, 6

38400 - PUERTO DE LA CRUZ
C.I.F.:

Ref. Cliente/Guest Ref.:
Bono/Voucher: 196467F9Z
Bono/Voucher: 196467FVB

Observaciones/Comments:
iberojet

| De/from | A/to | Servicio/Service | Precio/Price | Total |
|---|---|---|---|---|
| 05/08/2007 | 12/08/2007 | Prestacion de servicios al 7.00% | 2.074,80 | 2.074,80 |

Suma Total: 2.074,80 EUR

| Tipo/Type | Base Imponible/Net | I.V.A/V.A.T | Total |
|---|---|---|---|
| 7,00 % | 1939,07 EUR | 135,73 EUR | 2.074,80 EUR |

| Fecha/Date | Tipo Pago/Payment Type | Nr. Tarjeta/Card Number | Total |
|---|---|---|---|
| 12/08/2007 | Cta. Credito | | -2074,80 EUR |

Total Pagos: 0,00 EUR

RESTO A PAGAR: 2074,80 EUR

```
<?xml version="1.0"?>
<inv:Invoice xmlns:inv="http://www.docontime.es/Biztayer/UBL/Invoice-1.0" xmlns:mul="http://www.docontime.es/Biztayer/UBL/MultipleInvoice-1.0"
xmlns:cac="urn:oasis:names:specification:ubl:schema:xsd:CommonAggregateComponents-1.0"
xmlns:cbc="urn:oasis:names:specification:ubl:schema:xsd:CommonBasicComponents-1.0"
xmlns:cur="urn:oasis:names:specification:ubl:schema:xsd:CurrencyCode-1.0" xmlns="urn:oasis:names:specification:ubl:schema:xsd:Invoice-1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <ID>722/136667</ID>
  <cbc:IssueDate>2007-08-12</cbc:IssueDate>
  <cbc:Note/>
  <TaxPointDate>2007-08-12</TaxPointDate>
  <InvoiceCurrencyCode>EUR</InvoiceCurrencyCode>
  <AdditionalDocumentReference>
    <cac:ID>196467F9Z</cac:ID>
  </AdditionalDocumentReference>
  <AdditionalDocumentReference>
    <cac:ID>196467FVB</cac:ID>
  </AdditionalDocumentReference>
  <cac:BuyerParty>
    <cac:SellerAssignedAccountID>65746</cac:SellerAssignedAccountID>
    <cac:Party>
      <cac:PartyIdentification>
        <cac:ID>B38044921</cac:ID>
      </cac:PartyIdentification>
      <cac:PartyName>
        <cbc:Name>OPERADORES TURISTICOS S.L.</cbc:Name>
      </cac:PartyName>
      <cac:Address>
        <cbc:StreetName>AVDA.DE LA LUZ, 6 ED</cbc:StreetName>
        <cbc:CityName>PUERTO DE LA CRUZ</cbc:CityName>
        <cbc:PostalZone>38400</cbc:PostalZone>
        <cbc:Region>TENERIFE</cbc:Region>
        <cac:Country>
          <cac:IdentificationCode>ES</cac:IdentificationCode>
        </cac:Country>
      </cac:Address>
    </cac:Party>
  </cac:BuyerParty>
  <cac:SellerParty>
    <cac:Party>
      <cac:PartyIdentification>
        <cac:ID>A75504976</cac:ID>
      </cac:PartyIdentification>
      <cac:PartyName>
        <cbc:Name>CADENA HOTELERA, S.A.</cbc:Name>
      </cac:PartyName>
      <cac:Address>
        <cbc:StreetName>Gremio PAR, Polígono 2</cbc:StreetName>
        <cbc:CityName>Palma de Mallorca</cbc:CityName>
        <cbc:PostalZone>07004</cbc:PostalZone>
        <cac:Country>
          <cac:IdentificationCode>ES</cac:IdentificationCode>
        </cac:Country>
      </cac:Address>
    </cac:Party>
  </cac:SellerParty>
  <cac:PaymentMeans>
    <cac:PaymentMeansCode>ZZZ</cac:PaymentMeansCode>
    <cbc:DuePaymentDate>2007-08-12</cbc:DuePaymentDate>
    <cac:Payment>
      <cac:ID>Cta. Credito</cac:ID>
      <cbc:PaidAmount amountCurrencyID="EUR">2074.80</cbc:PaidAmount>
      <cbc:ReceivedDate>2007-08-12</cbc:ReceivedDate>
    </cac:Payment>
  </cac:PaymentMeans>
  <cac:TaxTotal>
    <cbc:TotalTaxAmount amountCurrencyID="EUR">135.73</cbc:TotalTaxAmount>
    <cac:TaxSubTotal>
      <cbc:TaxableAmount amountCurrencyID="EUR">1939.07</cbc:TaxableAmount>
      <cbc:TaxAmount amountCurrencyID="EUR">135.73</cbc:TaxAmount>
      <cac:TaxCategory>
        <cac:ID>VAT</cac:ID>
        <cbc:Percent>7.00</cbc:Percent>
        <cac:TaxScheme>
          <cac:TaxTypeCode>VAT</cac:TaxTypeCode>
        </cac:TaxScheme>
      </cac:TaxCategory>
    </cac:TaxSubTotal>
  </cac:TaxTotal>
  <cac:LegalTotal>
    <cbc:LineExtensionTotalAmount amountCurrencyID="EUR">2074.80</cbc:LineExtensionTotalAmount>
    <cbc:TaxExclusiveTotalAmount amountCurrencyID="EUR">1939.07</cbc:TaxExclusiveTotalAmount>
    <cbc:TaxInclusiveTotalAmount amountCurrencyID="EUR">2074.80</cbc:TaxInclusiveTotalAmount>
  </cac:LegalTotal>
  <cac:InvoiceLine>
    <cac:ID>1</cac:ID>
    <cbc:InvoicedQuantity quantityUnitCode="PCE">1.00</cbc:InvoicedQuantity>
    <cbc:LineExtensionAmount amountCurrencyID="EUR">2074.80</cbc:LineExtensionAmount>
    <cac:Delivery>
      <cac:ID>156469</cac:ID>
      <cbc:RequestedDeliveryDateTime>2007-08-05T00:00:00</cbc:RequestedDeliveryDateTime>
      <cbc:PromisedDateTime>2007-08-12T00:00:00</cbc:PromisedDateTime>
    </cac:Delivery>
    <cac:Item>
      <cbc:Description>Prestacion de servicios al 7.00%</cbc:Description>
      <cac:TaxCategory>
        <cac:ID>VAT</cac:ID>
        <cbc:Percent>7.00</cbc:Percent>
        <cac:TaxScheme>
          <cac:TaxTypeCode>VAT</cac:TaxTypeCode>
        </cac:TaxScheme>
      </cac:TaxCategory>
    </cac:Item>
    <cac:BasePrice>
      <cbc:PriceAmount amountCurrencyID="EUR">2074.80</cbc:PriceAmount>
    </cac:BasePrice>
  </cac:InvoiceLine>
  <inv:SellerDepartment>
    <cac:PartyIdentification>
      <cac:ID>722</cac:ID>
    </cac:PartyIdentification>
    <cac:PartyName>
      <cbc:Name>CADENA HOTELERA S.A.</cbc:Name>
    </cac:PartyName>
    <cac:Address>
      <cbc:StreetName>CTRA. LA MANGA, S/N</cbc:StreetName>
      <cbc:CityName>MAGALLUF</cbc:CityName>
      <cbc:PostalZone>7182</cbc:PostalZone>
        </cac:Country>
      </cac:Address>
      <cac:Contact>
        <cbc:Telephone>971131958</cbc:Telephone>
        <cbc:Telefax>antonio.rovira@cadhotelera.com</cbc:Telefax>
      </cac:Contact>
    </inv:SellerDepartment>
</inv:Invoice>
```

## Ejercicios de autoevaluación

**1.** ¿Qué es un certificado electrónico y en qué consiste la CRL y la OSCP de una PKI?

**2.** ¿En qué normativa europea se reconocen las modalidades de la firma XML? ¿Cuáles son según el estándar XMLDesig?

**3.** ¿Cuáles son las principales diferencias de las modalidades de firma electrónica XAdES y CAdES?

# Bibliografía

**J. Rifa, L. Huguet** (1991). *Comunicación digital: Teoría matemática de la información. Codificación algebraica. Criptología*. Ed. Masson.

www.facturae.es/