Sociedad de la Información y Firma Electrónica

Bloque I. Tema 1

Gestión de Sistemas e Informática

Curso 2017 - 18

Juan José Aguado Gil

05 Febrero 2018

1. Ley 59/2003 de Firma Electrónica

La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.

Los sujetos que hacen posible el empleo de la firma electrónica son los denominados **prestadores de servicios de certificación**. Para ello expiden **certificados electrónicos**, que son documentos electrónicos que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito telemático como firmante.

La ley obliga a los prestadores de servicios de certificación a efectuar una tutela y gestión permanente de los certificados electrónicos que expiden. Los detalles de esta gestión deben recogerse en la llamada **declaración de prácticas de certificación**, donde se especifican las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos. Además, estos prestadores están obligados a mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados en el que debe indicarse de manera actualizada si éstos están vigentes o si su vigencia ha sido suspendida o extinguida.

Asimismo, debe destacarse que la ley define una clase particular de certificados electrónicos denominados **certificados reconocidos**, que son los certificados electrónicos que se han expe-

dido cumpliendo requisitos cualificados en lo que se refiere a su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica.

Los certificados reconocidos constituyen una pieza fundamental de la llamada **firma electrónica reconocida**, que se define siguiendo las pautas impuestas en la Directiva 1999/93/CE como la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. A la firma electrónica reconocida le otorga la ley la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica.

Por otra parte, la ley contiene las garantías que deben ser cumplidas por los **dispositivos de creación de firma** para que puedan ser considerados como dispositivos seguros y conformar así una firma electrónica reconocida.

Artículos importantes:

- Artículo 3: concepto de firma electrónica avanzada y reconocida.
- Artículo 6: concepto de certificado electrónico.
- Artículo 11: concepto de certificado reconocido.

1.1. Artículo 1. Objeto

1. Esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.
2. Ver ley ...

1.2. Artículo 3. Firma Electrónica y Documentos Firmados Electrónicamente

1. La **firma electrónica** es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
2. La **firma electrónica avanzada** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
3. Se considera **firma electrónica reconocida** la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

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

1.2.1. Comentarios Firma Avanzada vs Reconocida [?]

¿Cómo conseguimos, en la práctica, que una firma electrónica sea reconocida y por tanto, equivalente a la firma manuscrita?. Una firma electrónica reconocida debe cumplir las siguientes propiedades o requisitos:

- Identificar al firmante.
- Verificar la integridad del documento firmado.
- Garantizar el no repudio en el origen.
- Contar con la participación de un tercero de confianza.
- Estar basada en un certificado electrónico reconocido.
- Debe de ser generada con un dispositivo seguro de creación de firma.

Los 4 primeros puntos son posibles gracias al uso de las **claves criptográficas** contenidas en el certificado y a la existencia de una estructura de Autoridades de Certificación que ofrecen confianza en la entrega de los certificados. Pero según la Ley 59/2003, esos 4 puntos sólo nos ofrecen una firma avanzada. Para que la firma electrónica sea **equivalente a la manuscrita**, es decir, que una firma electrónica sea reconocida, debe además:

- **Estar basada en un certificado reconocido**: el certificado debe haber sido reconocido por el Ministerio de Industria y Comercio como habilitado para crear firmas reconocidas y debe estar listado en su página web como tal. Se pueden ver todos los certificados reconocidos por el MITyC en la dirección https://sedeaplicaciones2.minetur.gob.es/prestadores/ Son certificados reconocidos porque tanto el prestador que los emite como el contenido mismo del certificado, cumplen con los requisitos declarados en el Capítulo II de la Ley 59/2003 de firma electrónica sobre Certificados reconocidos (artículos del 11 al 16).
- **Ser generada con un dispositivo seguro de creación de firma**: Las características de un dispositivo seguro de creación de firma están recogidas en el artículo 24 de la Ley 59/2003 de Firma Electrónica. Principalmente, el dispositivo seguro debe garantizar que las claves sean únicas y secretas, que la clave privada no se puede deducir de la pública y viceversa, que el firmante pueda proteger de forma fiable las claves, que no se altere el contenido del documento original y que el firmante pueda ver qué es lo que va a firmar. Desde un punto de vista técnico, según el artículo 27 de la Ley 59/2003, un dispositivo seguro de firma **debe ser certificado** como que cumple las características anteriores según las normas técnicas publicadas en la Decisión 2003/511/CE, de 14 de julio de 2003 de la Comisión Europea.

- El DNI Electrónico es considerado un dispositivo seguro de creación de firma y por tanto, las firmas generadas con él, son reconocidas y tienen la misma validez que la firma manuscrita. ¿Son reconocidas las firmas generadas en el ordenador con un certificado software instalado en el navegador?
- Puesto que el ordenador no es un dispositivo seguro de creación de firma, las firmas generadas son sólo firmas avanzadas según la definición de la ley.

1.3. Artículo 5. Régimen de Prestación de los Servicios de Certificación

1. La prestación de los servicios de certificación **no está sujeta a autorización previa** y se realizará en **régimen de libre competencia**. No podrán establecerse restricciones para los servicios de certificación que procedan de otro Estado miembro del Espacio Económico Europeo.

2. Los órganos de defensa de la competencia velarán por el mantenimiento de condiciones de competencia efectiva en la prestación de servicios de certificación al público mediante el ejercicio de las funciones que tengan legalmente atribuidas.

3. La prestación al público de servicios de certificación por la Administraciones públicas, sus organismos públicos o las entidades dependientes o vinculadas a las mismas se realizará con arreglo a los principios de objetividad, transparencia y no discriminación.

1.4. Artículo 6. Concepto de Certificado Electrónico y de Firmante

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

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

1.5. Artículo 7. Certificados Electrónicos de Personas Jurídicas

1. Podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos. Los certificados electrónicos de personas jurídicas no podrán afectar al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica.

2. La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico.

3. Los datos de creación de firma sólo podrán ser utilizados cuando 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 o concernientes a su giro o tráfico ordinario. Asimismo, la persona jurídica podrá imponer límites adicionales, por razón de la cuantía de la materia, para el uso de dichos datos que, en todo caso, deberán figurar en el certificado electrónico.

4. Se entenderán hechos por la persona jurídica los actos o contratos en los que su firma se hubiera empleado dentro de los límites previstos en el apartado anterior.
   Si la firma se utiliza transgrediendo los límites mencionados, la persona jurídica quedará vinculada frente a terceros sólo si los asume como propios o se hubiesen celebrado en su interés. En caso contrario, los efectos de dichos actos recaerán sobre la persona física responsable de la custodia de los datos de creación de firma, quien podrá repetir, en su caso, contra quien los hubiera utilizado.

1.6. Artículo 8. Extinción de la Vigencia de los Certificados Electrónicos

Son causas de extinción de la vigencia de un certificado electrónico:

1. Expiración del período de validez que figura en el certificado.

2. Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

3. Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.

4. Resolución judicial o administrativa que lo ordene.

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

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

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

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

1.7. Artículo 11. Concepto y Contenido de los Certificados Reconocidos

- Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.
- Los certificados reconocidos incluirán, al menos, los siguientes datos:
  - La indicación de que se expiden como tales.
  - El código identificativo único del certificado.
  - La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
  - La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
  - La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.
  - Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
  - El comienzo y el fin del período de validez del certificado.
  - Los límites de uso del certificado, si se establecen.
  - Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

1.8. Artículo 12. Obligaciones Previas a la Expedición de los Certificados Reconocidos

Antes de la expedición de un certificado reconocido, los prestadores de servicios de certificación deberán cumplir las siguientes obligaciones:

- Comprobar la identidad y circunstancias personales de los solicitantes de certificados con arreglo a lo dispuesto en el artículo siguiente.
- Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.
- Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.
- Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.

1.9. Artículo 14. Equivalencia Internacional de Certificados Reconocidos

Los certificados electrónicos que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro del Espacio Económico Europeo expidan al público como certificados reconocidos de acuerdo con la legislación aplicable en dicho Estado se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumpla alguna de las siguientes condiciones:

1. Que el prestador de servicios de certificación reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos y haya sido certificado conforme a un sistema voluntario de certificación establecido en un Estado miembro del Espacio Económico Europeo.

2. Que el certificado esté garantizado por un prestador de servicios de certificación establecido en el Espacio Económico Europeo que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos.

3. Que el certificado o el prestador de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

1.10. Artículo 16. Requisitos y Características del Documento Nacional de Identidad Electrónico

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

2. La Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados.

1.11. Artículo 18. Obligaciones de los Prestadores de Servicios de Certificación que Expidan Certificados Electrónicos

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

2. Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:

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

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

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

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

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

f) Las demás informaciones contenidas en la declaración de prácticas de certificación.

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

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

1.12. Artículo 20. Obligaciones de los Prestadores de Servicios de Certificación que Expidan Certificados Reconocidos

1. Los prestadores de servicios de certificación que expidan certificados reconocidos deberán cumplir las siguientes obligaciones:

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

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

c) Emplear personal con la cualificación, conocimientos y experiencia en la materia.

d) Utilizar sistemas y productos fiables que garanticen la seguridad técnica.

e) Tomar medidas contra la falsificación de certificados.

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

g) Utilizar sistemas fiables para almacenar certificados reconocidos.

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

1.13. Artículo 21. Cese de la Actividad de un Prestadores de Servicios

El prestador de servicios de certificación que vaya a cesar en su actividad deberá comunicarlo a los firmantes. La citada comunicación se llevará a cabo con una **antelación mínima de dos meses** al cese efectivo de la actividad e informará en su caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados.

1.14. Artículo 24. Dispositivos de Creación de Firma Electrónica

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

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

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

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

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

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

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

1.15. Artículo 27. Certificación de Dispositivos Seguros de Creación de Firma Electrónica

1. La certificación de dispositivos seguros de creación de firma electrónica es el procedimiento por el que se comprueba que un dispositivo cumple los requisitos establecidos en esta ley para su consideración como dispositivo seguro de creación de firma.

2. La certificación podrá ser solicitada por los fabricantes o importadores de dispositivos de creación de firma y se llevará a cabo por las entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo.

1.16. Artículo 31. Infracciones

Las infracciones de los preceptos de esta ley se clasifican en muy graves, graves y leves.

Son infracciones muy graves:

- El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, siempre que se hayan causados daños graves a los usuarios o la seguridad de los servicios de certificación se hayan visto gravemente afectados. Lo dispuesto en este apartado no será de aplicación respecto al incumplimiento de la obligación de constitución de la garantía económica prevista en el apartado 2 del artículo 20.
- Ver ley ...

Son infracciones graves:

- La falta de constitución por los prestadores que expidan certificados reconocidos de la garantía económica contemplada en el apartado 2 del artículo 20.
- La resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley y la falta o deficiente presentación de la información solicitada por parte del Ministerio de Ciencia y Tecnología en su función de inspección y control.
- El incumplimiento de las resoluciones dictadas por el Ministerio de Ciencia y Tecnología para asegurar que el prestador de servicios de certificación se ajuste a esta ley.
- Ver ley ...

Son infracciones leves:

- Ver ley ...

1.17. Artículo 32. Sanciones

Por la comisión de infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

	Sanciones
Muy Graves	de 150.001 a 600.000 euros
Graves	de 30.001 a 150.000 euros
Leves	hasta 30.000 euros

Tabla 1: Sanciones a las infracciones de la Ley 59/2003.

2. Aplicaciones de Firma

Existen algunos programas de uso cotidiano, por ejemplo, Adobe Acrobat o Microsoft Word, que permiten firmar el mismo documento que se genera. Sin embargo, este tipo de firma tiene dos inconvenientes:

- No todos los programas que generan documentos son capaces también de firmarlos.
- En general, el destinatario del documento firmado deberá tener la misma aplicación para ser capaz de verificar la firma.

Las aplicaciones de Firma son los programas que permiten firmar un documento electrónico. Las herramientas o aplicaciones específicas de firma electrónica son capaces de firmar cualquier tipo de documento electrónico y ayudan a superar los inconvenientes anteriores. Además se pueden descargar gratuitamente. A continuación describimos tres aplicaciones de firma ofrecidas por la Administración Pública que ayudan a firmar documentos: **AutoFirma**, **@Firma** y **eCoFirma**.

2.1. AutoFirma

Autofirma es una aplicación de firma realizada por el Ministerio de Hacienda y Administraciones Públicas. Su principal objetivo es ofrecer al usuario un sistema de firma en el que éste pueda firmar cualquier tipo de documento de manera sencilla. El usuario indica qué fichero quiere firmar y la aplicación escoge automáticamente el formato de firma qué debe aplicar, liberando así, al usuario de cualquier duda técnica.

2.2. @Firma

La aplicación @Firma, realizada por el Ministerio de Hacienda y Administraciones Públicas, es una aplicación java instalable en cualquier sistema operativo. El Cliente @Firma es una aplicación avanzada de firma que soporta la firma en múltiples formatos y permite la firma múltiple mediante la **co-firma** y la **contra-firma**. Para mayor flexibilidad, @Firma permite al usuario elegir el formato en el que desea firmar.

2.3. eCoFirma

eCoFirma, realizada por el Ministerio de Industria, es una aplicación de firma que permite generar y validar firmas electrónicas en formato XML **XAdES**.

2.4. Portal VALIDe

VALIDe es un servicio on-line ofrecido por el Ministerio de Hacienda y Administraciones Públicas para la validación de Firmas y Certificados electrónicos. Es una solución de referencia para cumplir con las medidas de Identificación y autentificación descritas en el Capítulo II de la Ley 11/2007 de Acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP).

El objetivo de este servicio es permitir a un usuario comprobar que el certificado utilizado es un certificado válido y que no ha sido revocado. También permite comprobar la validez de una firma electrónica realizada mediante certificado digital emitido por un prestador de servicios de certificación reconocido, y realizar firmas mediante certificado digital del que se disponga de la clave privada correspondiente.

La aplicación está disponible en **https://valide.redsara.es** y ofrece las siguientes secciones:

- **Validar Certificado**. Permite validar el estado de un certificado digital emitido por cualquier entidad de servicio de certificación reconocida.
- **Validar Certificado de Sede Electrónica**. Permite validar el estado de un certificado digital de sede electrónica.
- **Validar Firma**. Permite consultar la validez de un documento firmado electrónicamente con múltiples formatos y tipos de certificados, como facturas electrónicas, contratos, etc.
- **Realizar Firma**. Permite firmar electrónicamente un documento con cualquier certificado reconocido con las máximas garantías de integridad y autenticidad.
- **Visualizar firma**. Permite descargar un justificante pdf de la firma en el que aparece el documento original junto con el nombre y DNI/NIF de los firmantes impresos en el lateral.

3. Formatos de Firma

El formato de firma es la forma como se genera el documento de firma y como se guarda o estructura la información de firma en el documento generado. La existencia de múltiples formatos de firma se debe a razones históricas, a cómo se ha introducido la firma en formatos de documentos ya existentes y a cómo se han ido añadiendo funcionalidades a lo largo del tiempo. Un fichero de firma tiene un formato que viene determinado por los siguientes aspectos:

- Estructura de la Firma: formatos CAdES, XAdES, PAdES, OOXML, ODF.
- Firmas con múltiples usuarios.
- Longevidad de la firma y sello de tiempo.

3.1. Estructura de la Firma

Una firma electrónica es un fichero que contiene información sobre el documento original, el firmante, la fecha de la firma, algoritmos utilizados y posible caducidad de la firma. Cómo se estructura esta información (el orden de esa información dentro del fichero, las etiquetas que indican cuando empieza y termina cada campo, etc.) viene determinado por distintos formatos:

- **CAdES**: CMS Avanzado. Es apropiado para firmar ficheros grandes, especialmente si la firma contiene el documento original porque optimiza el espacio de la información. La información se guarda en forma binaria.
- **XAdES**: XML Avanzado. El resultado es un fichero de texto XML.
- **PAdES**: PDF Avanzado. Es el formato adecuado cuando el documento original es un pdf. El destinatario de la firma puede comprobar fácilmente la firma y el documento firmado. Con los formatos anteriores esto no es posible si no se utilizan herramientas externas.
- **OOXML y ODF**. Son los formatos que utilizan Microsoft Office y Open Office, respectivamente.

3.2. ¿Dónde se guarda el documento original?

Según cómo se referencie o dónde se guarde el documento original en el fichero de firma, podemos tener dos casos:

- El documento original se incluye en el fichero de firma. En el caso de CAdES estas firmas se llaman **firmas implícitas**. En el caso de firmas XAdES XML, lo habitual es que el documento esté incluido en el fichero de firma.
- El documento no se incluye en la firma. En el caso de CAdES estas firmas se llaman **firmas explícitas**.

3.3. Firmas con Múltiples Usuarios

Atendiendo al criterio del número de firmantes podemos tener:

- **Firmas simples**. Son las firmas básicas que contiene la firma de un solo firmante.
- **Co-firma**: (firma en línea). Es la firma múltiple en la que todos los firmantes están al mismo nivel y en la que no importa el orden en el que se firma. Se utiliza en documentos que son resultados de reuniones, conferencias o comités.

- **Contra-firma**: (firma en cascada). Es la firma múltiple en la que el orden en el que se firma es importante, ya que cada firma debe refrendar o certificar la firma del firmante anterior. Se utiliza especialmente en aplicaciones como los *Porta Firmas*, en los que un documento debe seguir una línea específica a través de varios firmantes hasta que todo el proceso es aprobado.

Las aplicaciones de firma *@Firma* y *eCoFirma* permiten ambas los tres tipos de firma, a elección del usuario.

3.4. Firmas Longevas y Sello de Tiempo

Para verificar una firma es necesario:

- Comprobar la integridad de los datos firmados asegurando que éstos no hayan sido modificados.
- Comprobar que el estado del certificado con el que se firmó era el correcto, es decir vigente en el momento de la operación.

Preguntas que surgen:

- ¿Cómo saber que el certificado estaba vigente en la fecha en que se firmó el documento?.
- ¿Qué debe hacerse para validar una firma en el futuro y que la validación sea posible aunque el certificado caduque?.

Los formatos AdES (forma genérica de llamar a los formatos CAdES, XAdES y PAdES) contemplan la posibilidad de incorporar a la firma electrónica información adicional que garantice la validez de un firma a largo plazo, una vez vencido el periodo de validez del certificado. Concretamente existen distintos formatos de firma (**AdES T**, **AdES C**, **AdES X**, **AdES XL** y **AdES A**) que van incrementando la calidad de la firma hasta conseguir que una firma pueda ser verificada a largo plazo (de forma indefinida) con plenas garantías jurídicas.

- **Firma Básica (AdES - BES)**. Es el formato básico para satisfacer los requisitos de de firma electrónica avanzada.
- **AdES T**. Añade un sellado de tiempo (T de TimeStamp) con el fin de situar el instante de tiempo en que se firma un documento.
- **AdES C**. Añade un conjunto de referencias a los certificados de la cadena de certificación y su estado (C de Cadena), como base para una verificación longeva.
- **AdES X**. Añade sellos de tiempo a las referencias AdES C (X de eXtendida).
- **AdES XL**. Añade los certificados y la información de revocación de los mismos para su validación a largo plazo (XL de eXtendido Largo plazo).
- **AdES A**. Permite la adición de sellos de tiempo periódicos para garantizar la integridad de la firma archivada para futuras verificaciones (A de Archivo).

4. Plataformas de Firma

4.1. @Firma

Las Administraciones Públicas ofrecen servicios públicos electrónicos en los que se necesita firma electrónica y métodos avanzados de identificación o autenticación basados en certificados digitales. Debido a los múltiples certificados que pueden utilizarse y la multitud de estándares, implantar sistemas que soporten todas las funcionalidades puede resultar complejo y costoso.

Por ello, el Ministerio de Hacienda y Administraciones Públicas ofrece la **plataforma de servicios de validación y firma electrónica** multi-PKI @firma, como un servicio de validación de certificados y firmas electrónicas, desacoplado de las aplicaciones. Es una solución de referencia para cumplir con las medidas de Identificación y autentificación descritas en el Capítulo II de la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP).

El objetivo es comprobar que el certificado utilizado por el ciudadano es un certificado válido y que no ha sido revocado y que por tanto sigue teniendo plena validez para identificar a su propietario. Los servicios de la plataforma son aplicables a todos los certificados electrónicos cualificados publicados por cualquier proveedor de servicio de certificación supervisado por el Ministerio de Industria Turismo y Comercio en España, incluidos los certificados del DNIe.

La plataforma de validación del Ministerio de Hacienda y Administraciones Públicas funciona como un servicio no intrusivo, que puede ser utilizado por todos los servicios telemáticos ofrecidos por las distintas **Administraciones Públicas, tanto estatal, como autonómica o local**. Para facilitar la integración con el servicio se proporcionan unas librerías de integración Integr@, que también permiten firma en servidor.

Además de ofrecerse como servicio, está disponible como software para instalar por las administraciones públicas (modelo federado), con múltiples utilidades de valor añadido, entre las que se encuentran la generación y validación de firmas electrónicas en múltiples formatos.

Relacionados con la plataforma de validación @firma, existen otros servicios de la **Suite @firma**, como una plataforma de sellado de tiempo, un cliente de firma en entornos de usuario, un visualizador de documentos electrónicos firmados, etc, que pueden consultarse en la iniciativa correspondiente.

5. Entidades Públicas de Certificación

5.1. CERES

CERES (CERtificación ESpañola) es una iniciativa puesta en marcha por la Administración, liderada por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-

RCM), que consiste en establecer una Entidad Pública de Certificación que permita autentificar y garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y administraciones públicas a través de las redes abiertas de comunicación.

Entre los servicios de certificación prestados por CERES están:

- Emisión, renovación y revocación de certificados de usuario, de representación para administradores únicos y solidarios, de persona jurídica y de entidad sin personalidad jurídica de la FNMT-RCM. Certificados de empleado público.
- Revocación on-line y a través de call center.
- Verificación del estado del certificado propio en el web.
- Servicio de verificación de la validez de los certificados electrónicos (OCSP, URL/HTTP y Servicio de directorio LDAP).
- Servicio de sellado de tiempo.
- Certificados de servidor SSL (estándar, wildcard y multidominio), firma de código, sello de entidad, sede electrónica, sello electrónico.

6. Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE)

Se acoge, en la Ley, un concepto amplio de *Servicios de la Sociedad de la Información*, que engloba, además de la contratación de bienes y servicios por vía electrónica, el suministro de información por dicho medio (como el que efectúan los periódicos o revistas que pueden encontrarse en la red), las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), **siempre que represente una actividad económica para el prestador**. Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico.

Ha sido modificada por la Ley 56/2007 de Medidas de Impulso de la Sociedad de la Información.

6.1. Artículo 6. No Sujeción a Autorización Previa

La prestación de servicios de la sociedad de la información **no estará sujeta a autorización previa**.

6.2. Artículo 9. Constancia Registral del Nombre de Dominio

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

6.3. Artículo 10. Información General

Sin perjuicio de los requisitos que en materia de información se establezcan en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

- Su nombre o denominación social; su residencia o domicilio, o en su defecto, la dirección de unos de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.
- Los datos de su inscripción en el Registro a que se refiere el artículo 9.
- Si ejerce una profesión regulada deberá indicar los datos del Colegio profesional al que, en su caso pertenezca y número de colegiado.
- El número de identificación fiscal que le corresponda.
- Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.
- Ver ley ...

6.4. Artículo 11. Deber de Colaboración de los Prestadores de Servicios

Cuando un órgano competente por razón de la materia hubiera ordenado, en ejercicio de las funciones que legalmente tenga atribuidas, que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España y para ello fuera necesario la colaboración de los prestadores de servicio de intermediación, podrá ordenar a dichos prestadores, directamente o mediante solicitud motivada al Ministerio de Ciencia y Tecnología, que suspendan la tramitación, el

alojamiento de datos, el acceso a las redes de telecomunicaciones o la prestación de cualquier otro servicio equivalente de intermediación que realizaran.

6.5. Artículo 22. Derechos de los Destinatarios de Comunicaciones Comerciales

1. Si el destinatario de servicios debiera facilitar su dirección de correo electrónico durante el proceso de contratación o de suscripción de algún servicio y el prestador pretendiera utilizarla posteriormente para el envío de comunicaciones comerciales, deberá poner en conocimiento de su cliente esa intención y solicitar su consentimiento para la recepción de dichas comunicaciones, antes de finalizar el procedimiento de contratación.

2. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente. A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado. Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

6.6. Artículo 23. Validez y Eficacia de los Contratos Celebrados por vía Electrónica.

- Para que sea válida la celebración de contratos por vía electrónica no será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos.

- Siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico.

6.7. Artículo 28. Información Posterior a la Celebración del Contrato

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

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

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

6.8. Artículo 29. Lugar de Celebración del Contrato

Los contratos celebrados por vía electrónica en los que intervenga como parte un consumidor se presumirán celebrados en el lugar en que éste tenga su residencia habitual.

Los contratos electrónicos entre empresarios o profesionales, en defecto de pacto entre las partes, se presumirán celebrados en el lugar en que esté establecido el prestador de servicios.

6.9. Artículo 37. Responsables

Los prestadores de servicios de la sociedad de la información están sujetos al régimen sancionador establecido en este título (Título VII) cuando la presente Ley les sea de aplicación.

6.10. Artículo 38. Infracciones

Son infracciones **muy graves**:

- El incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, cuando un órgano administrativo competente lo ordene, en virtud de lo dispuesto en el artículo 11.
- Ver ley ...

Son infracciones **graves**:

- El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor.
- La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley.
- Ver ley ...

Son infracciones **leves**:

- El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a los destinatarios que no hayan solicitado o autorizado expresamente su remisión, cuando no constituya infracción grave.
- Ver ley ...

6.11. Artículo 41. Infracciones y Sanciones. Medidas de Carácter Provisional

En los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar medidas de carácter provisional. En particular:

- Suspensión temporal de la actividad del prestador de servicios y, en su caso, cierre provisional de sus establecimientos.
- Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.
- Advertir al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas.

6.12. Artículo 45. Prescripción de Infracciones y Sanciones

	Infracciones	**Sanciones**
Muy Graves	3 años	3 años
Graves	2 años	2 años
Leves	6 meses	1 año

Tabla 2: Prescripción de Infracciones y Sanciones.

6.13. ANEXO

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

1. La contratación de bienes o servicios por vía electrónica.
2. La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
3. La gestión de compras en la red por grupos de personas.
4. El envío de comunicaciones comerciales.
5. El suministro de información por vía telemática.
6. El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción.

No tendrán consideración de servicios de la sociedad de la información los que NO reúnan las características señaladas y, en particular, los siguientes:

1. Los servicios prestados por medio de telefonía vocal, fax o télex.
2. El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.
3. Los servicios de radiodifusión televisiva contemplados en el artículo 3.a) de la Ley 25/1994.
4. Los servicios de radiodifusión sonora.
5. El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

7. Ley 56/2007 de Medidas de Impulso de la Sociedad de la Información (LMISI)

7.1. Artículo 1. Medidas de Impulso de la Factura Electrónica

- La facturación electrónica en el marco de la contratación con el sector público estatal será **obligatoria** en los términos que se establezcan en la Ley reguladora de la contratación en el sector público y en su normativa de desarrollo.

  A estos efectos, se entenderá que la factura electrónica es un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la **autenticidad de su origen** y la **integridad de su contenido**, lo que impide el repudio de la factura por su emisor.

- El Gobierno determinará el órgano competente de la Administración General del Estado que impulsará el empleo de la factura electrónica entre empresarios, profesionales y demás agentes del mercado, en particular, entre las pequeñas y medianas empresas y en las denominadas microempresas, con el fin de fomentar el desarrollo del comercio electrónico.

- Los Ministerios de Industria, Turismo y Comercio y de Economía y Hacienda, teniendo en cuenta las competencias reconocidas a las Comunidades Autónomas, aprobarán, en un plazo máximo de 6 meses desde la entrada en vigor de esta Ley, las normas sobre formatos estructurados estándar de facturas electrónicas que sean necesarias para facilitar la interoperabilidad del sector público con el sector privado y favorecer y potenciar el tratamiento automatizado de las mismas.

7.2. Artículo 2. Obligación de Disponer de un Medio de Interlocución Telemática para la Prestación de Servicios al Público de Especial Trascendencia Económica

Sin perjuicio de la utilización de otros medios de comunicación a distancia con los clientes, las empresas que presten servicios al público en general de especial trascendencia económica

deberán facilitar a sus usuarios un medio de interlocución telemática que, mediante el uso de certificados reconocidos de firma electrónica, les permita la realización de, al menos, los siguientes trámites:

- Contratación electrónica de servicios, suministros y bienes, la modificación y finalización o rescisión de los correspondientes contratos, así como cualquier acto o negocio jurídico entre las partes, sin perjuicio de lo establecido en la normativa sectorial.
- Consulta de sus datos de cliente, que incluirán información sobre su historial de facturación de, al menos, los últimos tres años y el contrato suscrito, incluidas las condiciones generales si las hubiere.
- Presentación de quejas, incidencias, sugerencias y, en su caso, reclamaciones, garantizando la constancia de su presentación para el consumidor y asegurando una atención personal directa.
- Ejercicio de sus derechos de acceso, rectificación, cancelación y oposición en los términos previstos en la normativa reguladora de protección de datos de carácter personal.

8. Reglamento UE 919/2014 eIDAS (Identificación Electrónica y Servicios de Confianza)

El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (eIDAS) establece las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro, así como las normas para los servicios de confianza y un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.

8.1. Tipos de Certificados según eIDAS

A raíz de la entrada en vigor del Reglamento UE 919/2014 (eIDAS), desaparecen algunos de los tipos de certificados existentes, que estaban basados en las posibilidades abiertas por la Ley 59/2003 (persona física, persona jurídica, entidad sin personalidad jurídica,...) y por la Ley 11/2007 (empleado público, sello electrónico y certificado web de sede electrónica), sustituyéndose por las nuevas posibilidades contempladas en el eIDAS (firma de persona, sello de entidad, autenticación web). Los nuevos tipos según el Reglamento eIDAS son:

- **Certificado de firma**: orientado a la identificación y firma de personas físicas (firmantes). La firma implica la garantía de origen e integridad de los datos firmados, así como

la conformidad con dichos datos (prestación del consentimiento) y vinculación con el contenido. Es equivalente al certificado de firma de persona física de la ley 59/2003.

- **Certificado de sello**: orientado al sello de personas jurídicas (creadoras de sello). Tiene cierta similaridad con el certificado de persona jurídica de la Ley 59/2003, con las siguientes diferencias:
  - No requiere indicar una persona como custodio o responsable del certificado.
  - Se orienta al sello (garantía de origen e integridad de los datos).
  - Además de autenticar el documento expedido por la persona jurídica, los sellos electrónicos se pueden utilizar para autenticar cualquier activo digital de la persona jurídica, por ejemplo, programas informáticos o servidores (considerando 65 del eIDAS).
  - Cuando una transacción exija un sello electrónico cualificado de una persona jurídica, debe ser igualmente aceptable una firma electrónica cualificada del representante autorizado de la persona jurídica (considerando 58 del eIDAS). Esta equivalencia no se aplica a la inversa.
- **Certificado de autenticación web**: orientado a vincular el sitio web (dominio de Internet) con la persona física o jurídica titular del certificado.
- **Certificado no cualificado**: cualquiera no expresamente previsto en el eIDAS. Puede estar orientado tanto a personas físicas, como jurídicas, componentes, SSL.

Un aspecto muy importante es que los nuevos certificados pueden incluir en el Serial Number números de identificación de la persona física o jurídica diferentes según el esquema de identificación utilizado. En España es frecuente utilizar el DNI, pero puede utilizarse el pasaporte, el número de afiliado a la seguridad social u otro dato que se gestione con un registro fuerte. Y en empresas, el CIF/NIF, o el número DUNS (no mencionado oficialmente)

9. Preguntas de Exámenes

1. (PI.2016.04). **Según la Ley 59/2003, de firma electrónica, indique cuál es el tipo de firma electrónica que: "tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel":**

   a) Firma electrónica avanzada.

   b) Firma electrónica intermedia.

   c) Firma electrónica reconocida.

   d) Firma electrónica final.

2. (PI.2016.06). **La aplicación eCoFirma, realizada por el Ministerio de Energía, Industria y Agenda Digital, permite generar y validar firmas electrónicas en formato:**

   a) PAdES.

   b) CAdES.

   c) XAdES.

   d) XDES.

3. (PI.2015.01). **Señale la respuesta correcta respecto a lo indicado en la Ley 34/2002, respecto a la prescripción de infracciones y de sanciones:**

   a) Las infracciones muy graves prescribirán a los 3 años, las graves a los 2 años y las leves al año.

   b) Las infracciones muy graves prescribirán a los 2 años, las graves al año y las leves a los seis meses.

   c) Las sanciones impuestas por faltas muy graves prescribirán a los 3 años, las impuestas por faltas graves a los 2 años y las impuestas por faltas leves al año.

   d) Las sanciones impuestas por faltas muy graves prescribirán a los 2 años, las impuestas por faltas graves al año y las impuestas por faltas leves los seis meses.

4. (PI.2015.08). **El perfil XAdES-X:**

   a) añade la posibilidad de timestamping periódico de documentos activados para prevenir que puedan ser comprometidos debido a la debilidad de la firma durante un periodo largo de almacenamiento.

   b) añade sellos de tiempo a las referencias introducidas por XAdES-C para evitar que pueda verse comprometida en el futuro una cadena de certificados.

   c) es una forma básica a la que se la ha añadido información sobre la política de firma solamente.

d) añade sellos de tiempo a las referencias introducidas por XAdES-A para evitar que pueda verse comprometida en el futuro una cadena de certificados.

5. (PI.2014.02). **Indique la afirmación correcta respecto a XAdES-T :**

   a) Contiene la forma básica de firma que cumple los requisitos legales de la Directiva para firma electrónica avanzada, información sobre la política de firma (opcional) y añade un campo de sellado de tiempo para proteger contra el repudio.

   b) Es la forma básica de firma a la que se la ha añadido información sobre la política de firma.

   c) Añade a la forma básica de firma la posibilidad de timestamping periódico de documentos archivados para prevenir que puedan ser comprometidos debido a la debilidad de la firma durante un periodo largo de almacenamiento.

   d) Añade sellos de tiempo a las referencias introducidas por XAdES-C para evitar que pueda verse comprometida en el futuro una cadena de certificados.

6. (PI.2014.03, PI.2013.01). **La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, en el artículo 45 detalla la prescipción para las sanciones e infracciones. Señale la respuesta correcta:**

   a) Las infracciones muy graves prescribirán a los 3 años, las graves al año y las leves a los 6 meses.

   b) Las sanciones impuestas por faltas muy graves prescribirán a los 3 años, las impuestas por faltas graves a los 2 años y las impuestas por faltas leves a los seis meses.

   c) Las infracciones muy graves prescribirán a los 5 años, las graves a los 3 años y las leves al año.

   d) Las sanciones impuestas por faltas muy graves prescribirán a los 3 años, las impuestas por faltas graves a los 2 años y las impuestas por faltas leves al año.

7. (PI.2014.04). **La Ley 34/2002, LSSICE, en al artículo 41 se establecen las medidas de caracter provivional que se pueden adoptar con el fin de asegurar la eficacia de la resolución que se dicte en relación con los procedimientos sancionadores iniciados por infracciones graves o muy graves. Señale cuál de las siguientes medidas NO se contempla:**

   a) Suspensión temporal de la actividad del prestador de servicios y, en su caso, cierre provisional de sus establecimientos.

   b) Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.

   c) Intervención provisional de los activos y bienes del prestador de servicios bajo resolución judicial.

d) Advertir al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas.

8. (PI.2013.02, LI.2013.12). **Según la Ley 59/2003 de Firma electrónica, los prestadores de servicios de certificación que expidan certificados reconocidos deberán conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido al menos durante:**

   a) 5 años.

   b) 10 años.

   c) Permanentemente.

   d) 15 años.

9. (PI.2013.03, LI.2013.11). **En la Ley 59/2003, de firma electrónica, se indica que la prestación de servicios de certificación:**

   a) Está sujeta a autorización previa por parte del Ministro de Hacienda.

   b) Está sujeta a autorización previa por parte del Consejo de Ministros.

   c) No está sujeta a autorización previa.

   d) Es una competencia autonómica.

10. (PI.2013.05). **Conforme a la Ley 59/2003, de Firma electrónica, el prestador de servicios de certificación que vaya a cesar en su actividad deberá comunicarlo a los firmantes que utilicen los certificados electrónicos que haya expedido así como a los solicitantes de certificados expedidos a favor de personas jurídicas, con una antelación al cese efectivo de la actividad, como mínimo de:**

    a) Al menos seis meses.

    b) Un año natural.

    c) Al menos dos meses.

    d) Al menos dos semanas.

11. (PI.2011.03). **De acuerdo con lo establecido en la Ley 56/2007, de Medidas de Impulso de la Sociedad de la Información, la factura electrónica en el marco de la contratación con el sector público estatal:**

    a) Será obligatoria en los términos que se establezcan en la Ley reguladora de la contratación en el sector público y en su normativa de desarrollo.

    b) Será obligatoria en los términos que se establezcan en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

c) No se prevé que resulte obligatoria, puesto que se trata de un documento sin validez jurídica, sólo emitido a título informativo.

d) Seá obligatoria en los términos que se establezcan en la Ley 11/2007.

12. (PI.2011.19). **Según la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico se considera infracción muy grave:**

a) El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor.

b) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley.

c) El incumplimiento de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios cuando no constituya infracción grave.

d) El incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, cuando un órgano administrativo competente lo ordene, en virtud de lo dispuesto en el artículo 11.

13. (PI.2011.20, LI.2011.13). **Una empresa tiene una página web con información sobre su actividad, productos y servicios que vende, pero éstos no pueden comprarse a través de la página web. ¿Le afectan a la empresa las obligaciones establecidas en la Ley de Servicios de la Sociedad de la Información para los prestadores de servicios?:**

a) Sí, ya que se trata de una actividad con trascendencia económica que se realiza por medios electrónicos.

b) No, al no haber venta directa de productos por medios electrónicos.

c) Sí, cualquier servicio que se preste a través de internet incurre en estas obligaciones.

d) No, la Ley no establece obligaciones para los prestadores de servicios.

14. (PI.2011.21). **Sin perjuicio de los requisitos que en materia de información se establezcan en la materia vigente, el prestador de servicios de la sociedad de la información ofrecerá de forma permanente, fácil, directa y gratuita, una serie de información ¿Cuál NO está incluido en esta obligación, según la Ley 34/2002, de 11 de julio?:**

a) Nombre o denominación social.

b) Si la profesión está regulada, los datos del Colegio Profesional al que pertenece.

c) Los códigos de conducta a los que, en su caso, está adherido.

d) Un número de teléfono donde poder establecer una comunicación directa con el prestador.

15. (PI.2010.14). **El impulso de la factura electrónica, como obligatoria en el marco de la contratación en el sector público estatal se establece en la ley:**

    a) 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

    b) 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

    c) 59/2003, de 19 de diciembre, de Firma Electrónica.

    d) 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

16. (PI.2008.17). **A efectos de la Ley 34/2002, de 11 de julio, de seervicios de la sociedad de la información y de comercio electrónico, señale cuál NO es un servicio de la soiedad de la información:**

    a) La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.

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

    c) El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción.

    d) El suministro de información por vía telemática.

17. (PI.2008.24, LI.2008.17). **Respecto al ámbito de actuación en la Plataforma de validación y firma electrónica, @firma, del Ministerio de Administraciones Públicas, señale la opción correcta:**

    a) Administración General del Estado y sus Organismos Públicos.

    b) Todas las Administraciones Públicas y Organismos asociados.

    c) Se exceptúan las Entidades Locales, Diputaciones provinciales y Cabildos, que acceden a los servicios proporcionados por las Comunidades Autónomas de su ámbito territorial.

    d) Se ofrecen los servicios de validación y firma a cualquier organización de carácter público y privado.

18. (LI.2016.11). **Señale la respuesta correcta que identifica los nuevos tipos de certificados según el Reglamento (UE) 910/2014 (eIDAS):**

    a) Certificados cualificados de firma electrónica, certificados cualificados de sello, certificados cualificados de autenticación web.

b) Certificados cualificados de firma electrónica, certificados cualificados de sesión, certificados cualificados de cifrado, certificados cualificados de persona jurídica, y de persona física.

c) Certificados cualificados de firma electrónica, certificados cualificados de Órgano, certificados cualificados de autenticación web y componentes.

d) Certificados cualificados de autenticación, certificados cualificados de cifrado, certificados cualificados de firma y certificados cualificados de sello.

19. (LI.2015.11). **Según la Ley 59/2003, de Firma Electrónica, la cuantía de las multas para los distintos tipos de infracciones serán:**

a) Para las muy graves de 300.001 a 600.000 euros; graves de 30.001 a 300.000 euros; leves hasta 60.000 euros.

b) Para las muy graves de 150.001 a 600.000 euros; graves de 60.001 a 150.000 euros; leves hasta 60.000 euros.

c) Para las muy graves de 150.001 a 300.000 euros; graves de 60.001 a 150.000 euros; leves hasta 30.000 euros.

d) Para las muy graves de 150.001 a 600.000 euros; graves de 30.001 a 150.000 euros; leves hasta 30.000 euros.

20. (LI.2015.12). **Según se indica en la Ley 59/2003, de firma electrónica, en cuanto al régimen de prestación de servicios de certificación:**

a) Está sujeta a autorización precia.

b) Los órganos de defensa de la competencia velarán por el mantenimiento de condiciones de competencia efectiva en la prestación de servicios de certificación al público mediante el ejercicio de las funciones que tengan legalmente atribuidas.

c) No podrán ser proporcionados por la Administraciones públicas, sus organismos públicos o las entidades dependientes o vinculadas a las mismas por motivo de los principios de objetividad, transparencia y no discriminación.

d) No se realizará en régimen de libre competencia.

21. (LI.2015.13). **A tenor de lo que expresa la Ley 59/2003 en su artículo 31 relativo a infracciones, señale cuál de las siguientes sería considerada muy grave:**

a) La falta de constitución por los prestadores que expidan certificados reconocidos de la garantía económica para afrontar el riesgo de la responsabilidad por los daños y perjuicios que puedan ocasionar el uso de de los certificados que expidan.

b) Almacenar o copiar los datos de creación de firma de la persona a la que el prestador de servicios de certificación haya expedido un certificado reconocido, y que éste hecho haya causado graves al usuario.

c) El incumplimiento de las resoluciones dictadas por el Ministerio de Ciencia y Tecnología para asegurar que el prestador de servicios de certificación se ajuste a esta Ley.

d) La resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados en esta Ley.

22. (LI.2015.18). **Señale qué servicio NO es ofrecido por el portal VALIDe:**

a) Validación de sede electrónica.

b) Realización de firma electrónica.

c) Visualización de firma electrónica.

d) Renovación de certificado electrónico.

23. (LI.2014.09). **Señale la respuesta correcta. Según se establece en la Ley de Firma Electrónica 59/2003 en su artículo 32, las multas establecidas al infractor serán de:**

a) Por la comisión de infracciones muy graves, multa de 150.001 a 600.000 euros, por la comisión de infracciones graves, se impondrá al infractor multa de 30.001 a 150.000 euros y por la comisión de infracciones leves, se impondrá al infractor una multa de hasta 30.000 euros.

b) Por la comisión de infracciones muy graves, multa de 60.001 a 600.000 euros, por la comisión de infracciones graves, se impondrá al infractor multa de 6.001 a 60.000 euros y por la comisión de infracciones leves, se impondrá al infractor una multa de hasta 6.000 euros.

c) Por la comisión de infracciones muy graves, multa de 120.001 a 600.000 euros, por la comisión de infracciones graves, se impondrá al infractor multa de 12.001 a 120.000 euros y por la comisión de infracciones leves, se impondrá al infractor una multa de hasta 12.000 euros.

d) Por la comisión de infracciones muy graves, multa de 150.001 a 600.000 euros, por la comisión de infracciones graves, se impondrá al infractor multa de 15.001 a 150.000 euros y por la comisión de infracciones leves, se impondrá al infractor una multa de hasta 15.000 euros.

24. (LI.2010.10). **Un prestador de servicios de certificación, ¿durante qué periodo de tiempo tiene que conservar la información relativa a los certificados reconocidos expedidos, de manera que puedan verificarse las firmas efectuadas con los mismos, de acuerdo a lo dispuesto en la Ley 59/2003, de 19 de diciembre, de Firma electrónica?:**

a) Al menos durante 15 años contados desde la fecha de fin de validez del certificado.

b) Al menos durante 15 años contados desde el momento de su expedición.

c) Un máximo de 15 años contados desde la fecha de fin de validez del certificado.

d) Un máximo de 15 años contados desde el momento de su expedición.

25. (LI.2010.20). **Señale cuál de los siguientes servicios NO se ofrece en la platforma de validación y firma electrónica @Firma:**

a) Sellado de tiempo (TSA) según la RFC 3161.

b) Validación, conforme a la RFC 3280, de certificados X.509 de todas las Autoridades de Certificación reconocidas en el pais por el Ministerio de Industria, Turismo y Comercio.

c) Expedición de certificados de firma electrónica del personal al servicio de las Administraciones Públicas para el cumplimiento de sus funciones.

d) Validación de firma vía servicios web (WS) de un elemento firmado.

26. (LI.2008.08). **En la Ley 59/2003, de 19 de diciembre, sobre firma electrónica, se establecen las siguientes definiciones, indicar la definición incorrecta:**

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

b) Firma electrónica: es el conjunto de datos, en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

c) Firma electrónica reconocida: es el documento electrónico generado mediante un dispositivo seguro de creación de firma.

d) Documento electrónico: el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente.

27. (SSTI.PI.2007.19). **Según la Ley 59/2003, de 19 de diciembre, de firma electrónica, un dispositivo seguro de creación de firma es un dispositivo que debe ofrecer al menos ciertas garantías. ¿Cuál de las siguientes NO es una de ellas?:**

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

b) Que los datos utilizados para la generación de firma puedan ser derivados de los de verificación de firma o de la propia firma.

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

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

28. (SSTI.PI.2007.24). **Según la ley 59/2003, de 19 de diciembre, de firma electrónica, ¿cuál de las siguientes NO es causa de extinción de la vigencia de un certificado?:**

    a) Expiración del periodo de validez que figura en el certificado.

    b) Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

    c) Resolución judicial o administrativa que lo ordene.

    d) Transferencia de la gestión de los certificados electrónicos expedidos por el prestador a otro prestador de servicios de certificación, cuando el firmante haya dado su consentimiento expreso.

29. (SSTI.LI.2011.66). **En el contexto de la firma electrónica y su regulación en España señale la afirmación FALSA:**

    a) Los funcionarios al servicio de las administraciones públicas españolas pueden firmar en el ejercicio de su cargo utilizando su DNI electrónico.

    b) Los códigos de verificación segura (CSV) junto con los sellos de órgano sirven para dotar de firma electrónica reconocida a la actuación administrativa automatizada.

    c) Un dispositivo seguro de creación de firma debe garantizar que los datos usados para generar la firma pueden producirse sólo una vez.

    d) Un certificado electrónico reconocido ha de incluir la firma electrónica avanzada del prestador de servicios de certificación que lo expide.

30. (SSTI.LI.2014.67). **Respecto a los ficheros de firma electrónica y los documentos firmados electrónicamente, señale la respuesta correcta:**

    a) El documento firmado siempre va incluido en el fichero de firma, tanto en XAdES como en CAdES.

    b) En CAdES, el documento puede no incluirse en el fichero de firma. Estas firmas se llaman explícitas.

    c) El documento firmado se incluye en el fichero de firma en XAdES, y no se puede incluir en CAdES.

    d) En XAdES, sólo se puede firmar de forma implícita, en la que el documento no se incluye en el resultado de firma y solamente se incluye una referencia al lugar en el que se encuentra.

31. (SSTI.LI.2016.43). **Señale la respuesta CORRECTA en relación a la firma digital:**

    a) Es un certificado electrónico que asocia una clave pública con la identidad de su propietario.

b) Se sirve de la criptografía asimétrica para garantizar la confidencialidad y la integridad del mensaje enviado.

c) Permite al receptor de un mensaje verificar la autenticidad del origen del mensaje y su integridad.

d) Es el criptograma resultante de aplicar una función hash al mensaje y cifrarlo con la clave pública del firmante.

32. (TAI.LI.2008.09, TAI.LI.2015.14). **Según la Ley 59/2003, de firma electrónica,los certificados electrónicos de personas jurídicas:**

a) Pueden afectar al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica.

b) Siempre deben incluir una identificación de persona física.

c) No pueden incluir límites de uso por cuantía.

d) No pueden incluir límites de uso por materia.

33. (TAI.LI.2008.10). **¿Qué objetivo tiene el proyecto CERES, que lidera la Fábrica Nacional de Moneda y Timbre?:**

a) Crear una red para la comunicación interministerial a través de Internet.

b) Crear una red para la comunicación interministerial a través de una intranet propia de la Administración.

c) Establecer una Entidad Pública de Certificación.

d) Dotar a los ciudadanos de una tarjeta inteligente dotada de microchip que sirva como tarjeta sanitaria.

34. (TAI.LI.2008.12). **¿Qué requisitos de seguridad debe satisfacer una factura electrónica, de acuerdo con la ley 56/2007, de Medidas de Impulso de la Sociedad de la Información?:**

a) Autenticidad de su origen y confidencialidad.

b) Integridad de su contenido y confidencialidad.

c) Autenticidad de su origen e integridad de su contenido.

d) Autenticidad de su origen, integridad de su contenido y confidencialidad.

35. (TAI.LI.2008.13). **¿Qué normativa regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación?:**

a) Real Decreto Ley 14/1999, de 17 de septiembre.

b) Ley 4/1996, de 10 de enero.

c) Real Decreto-Ley 12/2001, de 29 de junio.

d) Ley 59/2003, de 19 de Diciembre.

36. (TAI.PI.2008.03). **Señale cuál es la Ley de Firma Electrónica vigente en la actualidad:**

    a) Ley 15/1999.

    b) Ley 59/2003.

    c) Ley 30/2007.

    d) Ley 11/2007.

37. (TAI.PI.2010.02). **La ley 59/2003 de firma electrónica, en su artículo 18, establece una información mínima que el prestador de servicios de certificación debe proporcionar al solicitante del certificado antes de su expedición. Señale qué información NO proporciona el prestador de los servicios de información:**

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

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

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

    d) Los dispositivos seguros de creación de firma, con los que comprobar la integridad de los medios usados.

38. (TAI.PI.2010.03). **En el artículo 12 de la ley 59/2003 de firma electrónica, antes de la expedición de un certificado reconocido, los prestadores de servicios de certificación deberán cumplir las siguientes obligaciones. Señale la respuesta INCORRECTA:**

    a) Verificar que la información contenida en el documento es exacta y que incluye toda la información prescrita para un certificado reconocido.

    b) Comprobar que el firmante utiliza un dispositivo seguro de creación de firma para la generación de la misma.

    c) Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

    d) Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.

39. (TAI.PI.2014.01). **La ley 34/2002, de servicios de la sociedad de la información y comercio electrónico, en su artículo 45 trata la prescripción. Señale la respuesta correcta respecto a las infracciones:**

a) Las muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

b) Las muy graves prescribirán a los cinco años, las graves a los dos años y las leves a los seis meses.

c) Las muy graves prescribirán a los tres años, las graves a los dos años y las leves a los seis meses.

d) Las muy graves prescribirán a los cinco años, las graves a los tres años y las leves al año.

40. (TAI.LI.2015.11). **Según la ley 59/2003, de firma electrónica, el certificado electrónico es un documento:**

a) generado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

b) firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

c) generado electrónicamente por un prestador de servicios de certificación que no vincula los datos de verificación de firma a un firmante y confirma su identidad.

d) firmado electrónicamente por un prestador de servicios de certificación que no vincula los datos e verificación de firma a un firmante y no necesita confirmar su identidad.

41. (TAI.LI.2015.12). **Según el artículo 10 de la Ley 34/2002 de servicios de la Sociedad de la Información y de comercio electrónico, expone qué información está obligado el prestador de servicios de la sociedad de la información a poner a disposición por medios electrónicos, señale la FALSA entre las siguientes:**

a) Los prestadores de servicios de intermediación que presten colaboración con la entidad.

b) Los datos de su inscripción en el Registro Mercantil o el registro público en el que hay adquirido personalidad jurídica.

c) El número de identificación fiscal que le corresponda.

d) Su dirección de correo electrónico.

42. (TAI.PI.2015.02). **Un dispositivo seguro de creación de firma ofrece al menos las siguientes garantías. Señale la respuesta INCORRECTA según la ley 59/2003:**

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

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

c) El dispositivo utilizado no altera los datos o el documento que debe firmarse, impidiendo que éste se muestre al firmante antes del proceso de firma.

d) Los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

43. (TAI.LI.2016.14, TAI.PI.2016.03.Reserva). **La Ley 59/2003, de firma electrónica, establece en el artículo 32, la cuantía para las sanciones a aplicar por la comisión de infracciones, siendo las cuantías a aplicar:**

a) Infracciones leves: hasta 3000 euros, graves: de 3001 a 150000 euros, muy graves: de 150001 a 600000 euros.

b) Infracciones leves: hasta 30000 euros, graves: de 30001 a 150000 euros, muy graves: de 150001 a 600000 euros.

c) Infracciones leves: hasta 30000 euros, graves: de 30001 a 300000 euros, muy graves: de 300001 a 600000 euros.

d) Infracciones leves: hasta 60000 euros, graves: de 60001 a 300000 euros, muy graves: de 300001 a 600000 euros.

44. (TAI.LI.2016.16). **Según la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, señale la respuesta correcta:**

a) En la celebración de un contrato por medios electrónicos, el oferente está obligado a confirmar la recepción de la aceptación del contrato por cualquier medio electrónico en un plazo máximo de 72 horas.

b) Para que sea válida la celebración de contratos por vía electrónica es necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos.

c) Siempre que Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico. No obstante lo anterior, será necesario almacenar una copia en papel de la que se pueda verificar su veracidad en formato impreso.

d) Los contratos celebrados por vía electrónica en los que intervenga como parte un consumidor se presumirán celebrados en el lugar en que éste tenga su residencia habitual.

45. (BAQUEDANO.376). **La Ley 56/2007 de medidas de Impulso de la Sociedad de la Información, en su Artículo 1:**

a) introduce un temario básico de formación en Nuevas Tecnologías a nivel de Educación Secundaria Obligatoria.

b) fomenta el impulso del empleo de la factura electrónica.

c) subvenciona las empresas que opten por automatizar su cadena de producción.

d) limita el uso de los ficheros de datos que contienen información personal.

46. (BAQUEDANO.377). **Según el Artículo 2 de la Ley 56/2007 de Impulso de la Sociedad de la Información, las empresas que presten servicios al público en general, de especial trascendencia económica, deberán facilitar el siguiente trámite telemático:**

    a) Contratación electrónica de personal a su servicio.

    b) Consulta de sus datos de proveedores.

    c) Presentación de presupuestos y ofertas.

    d) Ejercicio de sus derechos de acceso, rectificación, cancelación y oposición según la normativa reguladora de protección de datos de carácter personal.

47. (BAQUEDANO.378). **Los Ministerios de Industria, Turismo y Comercio y de Economía y Hacienda aprobarán las normas sobre formatos estructurados estándar de facturas electrónicas para facilitar la interoperabilidad del sector público con el sector privado:**

    a) en el plazo de un año improrrogable desde la entrada en vigor de la Ley de Datos.

    b) en un plazo máximo de 6 meses desde la entrada en vigor de la Ley 56/2007.

    c) en el plazo de 2 semanas desde la entrada de vigor de la Ley de Administraciones Públicas.

    d) sin plazo alguno, cuando la Administración desarrolle dichas normas.

48. (BAQUEDANO.380). **La Ley de Firma electrónica 59/2003 de 19 de diciembre otorga a los prestadores de servicios de certificación la función de:**

    a) expedir los certificados electrónicos.

    b) efectuar una tutela y gestión permanente de los certificados electrónicos que expiden.

    c) mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados.

    d) todas las respuestas son correctas.

49. (BAQUEDANO.381). **La llamada "firma electrónica reconocida" se equipara funcionalmente a la firma manuscrita sólo si:**

    a) la firma electrónica está basada en un certificado encriptado.

    b) la firma electrónica está basada en un certificado reconocido y ha sido creada por un dispositivo seguro de creación.

    c) el certificado ha sido expedido en el año en curso.

    d) el certificado que avala la firma electrónica ha sido supervisado por la autoridad competente.

50. (BAQUEDANO.382). **Si una firma electrónica se utilizasen actos transgrediendo los límites legales:**

    a) la persona jurídica titular quedaría vinculada frente a terceros sólo si los asume como propios.

    b) la persona jurídica titular no queda en ningún caso vinculada frente a terceros.

    c) los efectos de dichos actos recaerían directamente sobre la persona física que los utilizó.

    d) los efectos de dichos actos recaerían directamente sobre la autoridad certificadora.

51. (BAQUEDANO.383). **Los certificados electrónicos que expidan los prestadores de servicios de certificación establecidos en un Estado no miembro del Espacio Económico Europeo, se considerarán equivalentes a los expedidos por los establecidos en España siempre que:**

    a) el prestador de servicios de certificación reúna los requisitos establecidos en la normativa comunitaria.

    b) el certificado esté garantizado por un prestador de servicios de certificación reconocido y establecido en el Espacio Económico.

    c) el certificado o el prestador de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral.

    d) todas las respuestas son correctas.

10. Soluciones

1. C
2. C
3. C
4. B
5. A
6. D
7. C
8. D
9. C
10. C
11. A
12. D
13. A
14. D
15. B
16. B
17. B
18. A
19. D
20. B
21. B
22. D
23. A
24. B
25. C
26. Anulada
27. B
28. D
29. B
30. B
31. C
32. B
33. C
34. C
35. D
36. B
37. D
38. B
39. C
40. B
41. A
42. C
43. B
44. D
45. B
46. D
47. B
48. D
49. B
50. A
51. D

Referencias

[1] **Ley 59/2003 de Firma Electrónica (LFE)**.
http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf

[2] **Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE)**.
http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf

[3] **Ley 56/2007 de Medidas de Impulso de la Sociedad de la Información (LMISI)**.
http://www.boe.es/boe/dias/2007/12/29/pdfs/A53701-53719.pdf

[4] https://administracionelectronica.gob.es/

[5] http://firmaelectronica.gob.es/

[6] http://firmaelectronica.gob.es/Home/Ciudadanos/Base-Legal.html

[7] https://valide.redsara.es/valide/