Diputación de Cádiz

AMJ/MARP
SECRE-00085-2023

Almudena Martínez del Junco, Presidenta de la Diputación Provincial de Cádiz, en uso de las atribuciones que me están conferidas, he resuelto dictar con esta fecha el siguiente

DECRETO

Vistos los siguientes **Antecedentes de hecho:**

La Diputación Provincial de Cádiz aprueba su Política de Firma Electrónica por decreto de la Presidencia de 8 de mayo de 2017 (*Boletín Oficial de la Provincia de Cádiz* de 24 de mayo de 2017), cuyo objeto es informar de las condiciones generales aplicables a la firma electrónica en la Diputación de Cádiz, que pretende cumplir las especificaciones que dicta la política de firma de la Administración General del Estado para los casos concretos de formato de la firma, proceso, certificados y validación de la firma que Diputación de Cádiz utiliza (apdo. 1.1).

El tiempo transcurrido desde la aprobación de la vigente Política de Firma Electrónica (2017), con los avances tecnológicos, normativos y organizativos producidos desde entonces, pone de manifiesto la necesidad de actualizar tal Política, adecuándola a los sistemas de identificación y firma utilizados por la Corporación.

A tal fin se tramita un contrato menor de servicios cuyo objeto es la contratación del servicio de asesoramiento específico para la definición y desarrollo de una política de identificación y firma electrónica, la cual resulta imprescindible para el despliegue efectivo de la administración electrónica de conformidad con las obligaciones impuestas por las Leyes 39 y 40/2015. Dicho contrato se adjudica a la empresa Agtic Consulting S. L. por decreto de la Presidencia de 24 de enero de 2023.

Tras diversas reuniones mantenidas entre Agtic y el grupo de trabajo formado por representantes de Presidencia, Secretaría General y EPICSA, la empresa entrega el documento el 30 de marzo de 2023, si bien este ha sido objeto de algunas modificaciones posteriores, como la inclusión de un anexo.

Una vez que se dispone del documento íntegro, y dada la relevancia del mismo para una implantación efectiva de la administración electrónica, en tanto que aportará una mayor seguridad jurídica y técnica en un asunto fundamental como es el de la identificación y firma electrónicas, que incide en la relación de nuestra organización con la ciudadanía, vemos conveniente que la Diputación Provincial de Cádiz afronte la aprobación de la nueva Política de Firma Electrónica.

Conforme a los siguientes **Fundamentos de Derecho:**

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica dicta, en su art. 18.1, que la Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para el reconocimiento de las firmas electrónicas basadas en certificados de documentos administrativos en las Administraciones Públicas. Las restantes Administraciones Públicas, según el art. 18.2, podrán acogerse a la mencionada política de firma electrónica y de certificados.

Asimismo determina, en su art. 18.3, que las Administraciones Públicas podrán aprobar otras políticas de firma electrónica dentro de sus respectivos ámbitos competenciales.

De acuerdo con el citado art. 18, la Diputación Provincial de Cádiz aprueba su Política de Firma Electrónica por decreto de la Presidencia de 8 de mayo de 2017 (*Boletín Oficial de la Provincia de*

Cádiz de 24 de mayo de 2017),a la que ya nos hemos referido en los antecedentes de hecho.

El Reglamento Regulador de la Administración Electrónica en la Diputación Provincial de Cádiz, aprobado por el Pleno en sesión celebrada el 24 de abril de 2019 y publicado su texto íntegro en el *Boletín Oficial de la Provincia de Cádiz* de 24 de junio de 2019, regula, en su Título IV, la identificación y firma electrónica en la Diputación Provincial de Cádiz, tratando, entre otras cuestiones, los sistemas de identificación y firma electrónica de las personas físicas, de las personas jurídicas o del personal al servicio de la Diputación.

En varias ocasiones se cita la Política de Firma Electrónica (art. 28.6, art. 29.1, art. 32.2, etc.), siendo de especial relevancia la exigencia de conformidad con ella de los certificados cualificados de sello y de firma electrónica de que se dote la Diputación Provincial de Cádiz (art. 33.1).

En una línea similar al aludido Reglamento, la Política de Gestión de Documentos Electrónicos de la Diputación Provincial de Cádiz, aprobada por decreto de 5 de marzo de 2021, establece, en su párrafo 30, que los documentos electrónicos deberán ser autenticados conforme a la Política de Firma Electrónica.

La aprobación de la Política de Firma Electrónica, a tenor del art. 56 del mencionado Reglamento Regulador de la Administración Electrónica en la Diputación Provincial de Cádiz, le corresponde a la Presidencia, mediante decreto.

Por lo anteriormente expuesto, visto el informe del archivero de Secretaría General y a propuesta de este Servicio, **vengo en resolver:**

PRIMERO.- Aprobar la Política de Identidad y Firma Electrónicas de la Diputación Provincial de Cádiz (PIFE-DPCA). Dicha Política se anexa al presente decreto.

SEGUNDO.- Dar traslado de la aprobación de la Política de Identidad y Firma Electrónicas de la Diputación Provincial de Cádiz (PIFE-DPCA) a la Empresa Provincial de Información de Cádiz S. A. (EPICSA) y a la Unidad Administrativa de Trabajo en Materia de Administración Electrónica (UTAE), a fin de que procedan a realizar todas las actuaciones que resulten convenientes para la consecución de cuanto antecede.

TERCERO.- Publicar este acuerdo en la página web de la Diputación Provincial de Cádiz y en la Sede Electrónica de la misma, así como trasladarlo a todas las áreas de la Corporación para su conocimiento y constancia.

ANEXO DEL DECRETO

POLÍTICA DE IDENTIDAD Y FIRMA ELECTRÓNICAS DE LA DIPUTACIÓN PROVINCIAL DE CÁDIZ (PIFE-DPCA)

1. Introducción y objeto

Mediante la presente Política de Identidad y Firma Electrónicas la Diputación de Cádiz, en adelante la Diputación, se evidencia el compromiso de la institución en el establecimiento del uso de la identidad y la firma electrónicas para el establecimiento de relaciones telemáticas y la producción de documentos electrónicos con plena validez jurídica como uno de los elementos vertebradores, junto con la Política de gestión del documento electrónico, de la estrategia de implantación de la administración electrónica.

Esta Política regula, en el ámbito competencial de la Diputación, los siguientes aspectos de acuerdo con lo previsto en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica y la Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración:

- El alcance y ámbito de aplicación subjetivo de la presente Política.
- Los datos de identificación de la presente Política.
- La atribución de roles y responsabilidades a los diferentes actores que deben regir la gestión y desarrollo de la presente Política.
- Las directrices generales relativas a la identidad electrónica en la Diputación.
- La identificación de certificados digitales y otros mecanismos de identificación usados y admitidos por la Diputación, así como la descripción de los procedimientos para su obtención y gestión por parte de la Diputación.
- Los sistemas y formatos de identificación y firma electrónicas admitidos.
- Las recomendaciones comunes sobre el formato de las firmas electrónicas basadas en certificados digitales.
- Los casos de uso de la firma electrónica, que permitirán tener un modelo de referencia de los sistemas de firma que se podrán utilizar y admitir en cada caso.
- Las comprobaciones, automáticas y manuales, que realizará la Diputación cuando reciba una firma electrónica por parte de terceros.
- La estrategia de preservación de documentos y firmas electrónicas.
- Directrices al respecto del mantenimiento y desarrollo de la presente Política.

En la elaboración de esta Política se ha tenido en cuenta la normativa aplicable en la materia, tanto a nivel supranacional, estatal, autonómico y aquella propia de la Diputación, como estándares internacionales y otras convenciones detalladas en el Anexo III. Cabe destacar especialmente las siguientes normativas:

- Reglamento Europeo (UE) 910/2014 del Parlamento Europeo y Consejo, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior –en adelante, Reglamento eIDAS.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad –en adelante, ENS.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

- Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica –en adelante, ENI.

2. Ámbito de aplicación subjetivo

Este documento se aplica a todas aquellas personas o entidades que establezcan relaciones con la Diputación que requieran la producción o intercambio de documentos electrónicos auténticos, tal y como se expone a continuación.

Esta Política se aplica a todos los miembros de la Diputación, con independencia de la modalidad contractual que determine su relación con la institución, la posición jerárquica que ocupen dentro de la organización y sea cual fuere su centro de trabajo donde presten servicios.

Esta Política también es de aplicación a las siguientes entidades:

a) Los órganos administrativos integrantes de la Diputación.

b) Los organismos públicos y entidades de derecho público vinculados o dependientes de esta.

c) Las sociedades mercantiles y otras entidades de derecho privado vinculadas o dependientes de aquella, cuando ejerzan potestades administrativas y en aquellos contenidos de esta Política que específicamente se refieran a las mismas.

Asimismo, se aplicará a los adjudicatarios de contratos de concesión de servicios y contratos de concesión de obras de la Diputación, cuando así lo dispongan los pliegos de licitación u otros documentos contractuales, en sus relaciones con la Diputación y con los usuarios y la ciudadanía, en el marco de la prestación de servicios públicos correspondientes.

Esta Política será igualmente aplicable a la ciudadanía, entendiendo por tal a quienes tengan capacidad de obrar ante las administraciones públicas, cuando utilicen medios electrónicos en sus relaciones con la Diputación y con el resto de las entidades referidas en este mismo apartado.

El sector institucional y las fundaciones relacionados con la Diputación podrán optar por aplicar como propia esta Política mediante la simple decisión de su adhesión a la misma.

La presente Política se referirá a la Diputación haciendo referencia al ámbito de aplicación subjetivo que se expone en este apartado.

3. Datos de la Política de Identidad y Firma Electrónicas

Los datos identificativos de la Política de Identidad y Firma Electrónicas son los que se incluyen a continuación:

Nombre del documento	Política de Identidad y Firma Electrónicas de la Diputación Provincial de Cádiz (PIFE-DPCA)
Versión	2.0

URI de referencia	Política_Identificacion_Firma_Electronicas_ LA0009013_v2.0
URL de referencia	https://sede.dipucadiz.es/normativa
Fecha de expedición	Fecha de aprobación mediante decreto de la Presidencia
Ámbito de aplicación	Documentos y expedientes electrónicos producidos, recibidos y/o custodiados por la Diputación Provincial de Cádiz y otras entidades, según lo establecido en el apartado 2 de la presente política sobre el ámbito de aplicación subjetivo.
Nombre del gestor	Secretaría General. Unidad Administrativa de Trabajo en Materia de Administración Electrónica (UTAE)
Identificador del gestor	LA0009013
Datos de contacto del gestor	utae@dipucadiz.es 956240333 Plaza de España, s/n, 11071 Cádiz

4. Roles y responsabilidades

A continuación, se establece la atribución de roles y responsabilidades de las áreas de la Diputación implicadas por la presente Política:

4.1. Presidencia

Le corresponden al Área de Presidencia las siguientes responsabilidades:

- Desplegar, aprobar, publicar y mantener la presente Política.
- Aprobar, mediante resolución, cualquier cambio en la Política o sus Anexos.
- Actualizar la lista de prestadores y tecnologías admitidas en la entidad para las certificaciones digitales.
- Gestionar la formación al personal de la entidad sobre el uso de la Política.
- Proponer la ejecución de auditorías internas o externas para verificar el cumplimiento de la Política. Coordinar el inventario de certificados digitales de sello electrónico.

4.2. Secretaría General

Le corresponden al Área de Secretaría General las siguientes responsabilidades:

- Garantizar la publicación en Sede Electrónica de las versiones actualizadas de la presente Política.
- Encargarse de la superior dirección de Registro General, de conformidad con lo previsto en el artículo 3.2 del Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional.
- Proponer a Presidencia la actualización de las tecnologías admitidas en la entidad para la identificación y firma electrónicas, previa autorización del Ministerio que en cada momento tenga la competencia de su aprobación.

4.3. Unidad Administrativa de Trabajo en Materia de Administración Electrónica (UTAE)

Le corresponden a la UTAE, unidad dependiente de Secretaría según artículo 3.2 del Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional, las siguientes responsabilidades:

- Encargarse de la coordinación y el seguimiento de la implantación de la Política, incluidas las auditorías que se realicen a petición de la Presidencia de la Diputación.
- Encargarse del mantenimiento y la actualización de la Política y elevar las propuestas a Presidencia.
- Coordinar el uso de los certificados digitales de sello electrónico.
- Proponer e impartir la formación al personal de la entidad sobre el uso de la Política.

4.4. Empresa Provincial de Información de Cádiz S.A. (EPICSA)

Le corresponden a EPICSA las siguientes responsabilidades:

- Implantar y mantener las plataformas y soluciones tecnológicas apropiadas para dar cumplimiento a esta Política.
- Encargarse de la solicitud y obtención de los certificados digitales de sello electrónico de la entidad.
- Encargarse del mantenimiento del inventario de certificados digitales de sello electrónico de la entidad.
- Proponer e impartir la formación al personal de la entidad sobre el uso de la Política.

4.5. Registro General

Le corresponden al Área de Registro General las siguientes responsabilidades:

- Gestionar las solicitudes y renovaciones de los certificados digitales, bajo la superior dirección de Secretaría General.
- Encargarse del mantenimiento del inventario de certificados digitales de la entidad, bajo la superior dirección de Secretaría General.

4.6. Todas las áreas y unidades

Les corresponden a todas las áreas y unidades de la Diputación las siguientes responsabilidades:

- Conocer la Política de Identidad y Firma Electrónicas de la Diputación Provincial de Cádiz.
- Cumplir con su contenido.

5. Identidad electrónica admitida por la Diputación Provincial de Cádiz

El uso de las relaciones telemáticas implica la necesidad de identificar a todas las partes participantes de forma segura garantizando el no repudio de estas relaciones. En este apartado se recopilan los distintos sistemas para la identificación electrónica de las personas que se relacionan con la Diputación, de acuerdo con el marco jurídico vigente.

5.1. Certificados digitales admitidos

El mecanismo de firma o de sello electrónico con certificado digital se sustenta en la existencia de autoridades de certificación que emiten certificados digitales y permiten comprobar que un

certificado concreto ha sido correctamente emitido y que sigue siendo válido en el momento de su uso, es decir, cuando se emite una firma o un sello electrónicos.

La relación entre la Autoridad de Certificación y la entidad que valida el certificado es una relación que se fundamenta en la confianza: los certificados se aceptan únicamente en la medida en que la entidad que debe validarla confíe en la honestidad de la Autoridad de Certificación.

El Reglamento eIDAS establece la obligación de los Estados miembros de la Unión Europea de admitir los sistemas de identificación electrónica notificados a la Comisión Europea por parte del resto de Estados miembros, así como los sistemas de firma y sello electrónicos basados en certificados digitales cualificados emitidos por prestadores de servicios que figuren en las listas de confianza otros Estados miembros de la Unión Europea.

Asimismo, la Diputación debe admitir, según lo establecido por la Ley 39/2015, todos los certificados digitales emitidos por prestadores de servicios de certificación incluidos en la Trusted Services List (TSL). Esta Lista ha sido elaborada de acuerdo con lo previsto en el artículo 22, apartado 1, del Reglamento eIDAS, y se puede consultar en el siguiente enlace: https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx (o el que le sustituya a futuro).

En consecuencia, la Diputación admite todos los certificados digitales emitidos por los prestadores de servicios de certificación que hayan realizado la comunicación prevista en el artículo 17 de la Ley 6/2020 al Ministerio de Asuntos Económicos y Transformación Digital y que cumplan con los estándares de calidad y niveles de seguridad establecidos por el citado Ministerio.

No obstante, para la validación de los certificados digitales, la Diputación utiliza @firma, una plataforma de la Administración General del Estado. Por este motivo, la aceptación efectiva de certificados estará condicionada por la actualización de los servicios de la plataforma.

La Diputación Provincial de Cádiz deberá dar publicidad, en su sede electrónica, de los certificados digitales admitidos en cada momento.

5.2. Otros sistemas de identidad admitidos

Adicionalmente a la identificación mediante certificado digital la Diputación de Cádiz admitirá los siguientes sistemas de identidad electrónica:

1. **Sistemas de identificación basados en registro previo de la Administración General del Estado**, como Cl@ve Permanente, Cl@ve PIN24h o Cl@ve Firma.

2. **Identidades digitales basadas en claves concertadas** proporcionadas por la Diputación de manera segura y sometidas a su Política de Seguridad de la Información por la cual cada usuario deberá mantener bajo su exclusivo conocimiento.

3. **Identidades digitales generadas en la propia Diputación basadas en registro previo combinadas con mecanismos de doble factor de autenticación,** como contraseñas OTP "One-Time Password" (de un solo uso) o aplicaciones residentes de gestión de identidades mediante la generación de códigos de autenticación con contraseña de un solo uso.

   En este contexto, la Diputación podrá disponer de un Registro de Identidades Digitales en el que se inscriban los datos de aquellos que se relacionen con la misma. Este Registro recogerá los datos necesarios para facilitar los servicios de identificación, como credenciales o claves.

4. **Identidades digitales basadas en número de referencia,** que implican el uso de un número de referencia entregado por la Diputación que el usuario puede emplear para identificarse.

5. **Identidades digitales basadas en información conocida por la Diputación y el ciudadano,** que permiten a la persona interesada identificarse en los sistemas de la entidad a través de la aportación de determinados datos que únicamente son conocidos

por ella y la Diputación.

6. **Sistemas de identificación proporcionados por prestadores de servicios de confianza de acuerdo con el Reglamento eIDAS,** como, por ejemplo, sistemas de videoidentificación, mediante los cuales los prestadores comprueban la identidad de una persona y la acreditan ante la Diputación.

La Diputación Provincial de Cádiz deberá dar publicidad, en su sede electrónica, de los sistemas de identificación admitidos en cada momento.

6. Identidad digital usada por la Diputación

6.1. Certificados digitales usados por la Diputación

La Diputación y su personal deberán usar los siguientes tipos de certificados digitales:

- **Certificados de persona física.** Certificados digitales a título personal sin vinculación con la Diputación y emitido por un prestador incluido en la Lista de prestadores cualificados de servicios electrónicos de confianza, que se emplearán únicamente en aquellos casos en que los miembros de la entidad deban relacionarse con la misma en el marco de su relación laboral.

- **Certificados de empleado público.** Certificados personales de los que puede disponer cualquier persona física empleada del sector público, que contiene el dato de vinculación con la entidad en el que trabaja y emitido por un prestador incluido en la Lista de prestadores cualificados de servicios electrónicos de confianza. De este modo, los empleados y cargos que actúen como órganos unipersonales de la Diputación emplearán este tipo de certificados en el ejercicio de sus competencias laborales. En el caso de la Diputación, será necesario que la Dirección de Área o persona responsable del Área o servicio de la persona interesada autorice su emisión.

- **Certificados de representante.** Certificados personales de los que únicamente pueden disponer las personas que tienen atribuida la competencia de representar a la Diputación frente a terceros, que contienen el dato de capacidad de representación de la institución y son emitidos por un prestador incluido en la Lista de prestadores de servicios electrónicos de confianza.

- **Certificados de sello electrónico.** Certificados que sirven para emitir firmas en el marco de la actuación administrativa automatizada, según el artículo 42 de la Ley 40/2015

- **Certificados de servidor y aplicación.** Certificados que sirven para la identificación de servidores y aplicaciones y que permiten el intercambio seguro de datos entre sistemas de información propios y de terceros. Este tipo de certificado es el requerido para una aplicación que envía mensajes que requieran asegurar su integridad y autenticidad. El uso de este tipo de certificados no produce efecto jurídico alguno.

- **Certificados de página web y sede electrónica.** Certificados que permiten garantizar el acceso seguro en los entornos de tramitación telemática de la institución, estableciendo comunicaciones cifradas con los usuarios del servidor web utilizando la tecnología SSL o TLS. Se podrá aplicar cualquier certificado emitido por autoridades de certificación con un alto nivel de reconocimiento de sus claves públicas en los navegadores web de uso más extendido. El uso de este tipo de certificado no produce efecto jurídico alguno.

La Diputación Provincial de Cádiz dará publicidad, en su sede electrónica, de los certificados digitales de que disponga en cada momento, exceptuando aquellos vinculados con personas físicas.

6.2. Certificados digitales usados por el personal de la Diputación

En aquellos supuestos en que el personal de la Diputación necesite disponer de certificado digital, podrá usar, según lo indicado en el apartado anterior, uno de persona física, de empleado público o de representante, según su cargo y competencias lo requieran. Para el caso de terceros que participen o colaboren puntualmente con la institución, podrán usar uno de persona física o uno de vinculación con la Diputación.

La Diputación, por lo tanto, podrá utilizar los certificados mencionados en los siguientes casos:

- Todo el personal de la Diputación que, en el ejercicio de sus funciones, necesite firmar documentos electrónicos o realizar alguna de las tareas para las que se requiere certificado, podrá usar los certificados de persona física o solicitar un certificado de vinculación con la Diputación. Es responsabilidad de la persona empleada por la Diputación asegurarse de la vigencia de su certificado.

- Todas las personas que, por cargo o designación, puedan representar a la Diputación, deberán tener como mínimo un certificado digital de representante. Mediante decreto de Presidencia se podrán conceder certificados digitales de representante para determinadas actuaciones autorizadas previamente por la Unidad o Área de la Diputación correspondiente. Asimismo, se podrán registrar estas capacidades en Registro Electrónico de Apoderamientos de la Administración General del Estado o REA-AGE para acceder a un subconjunto de información o trámites para los que han sido apoderados.

- El resto de las personas vinculadas a la Diputación o personas que participen o colaboren puntualmente con ella, podrán usar un certificado de persona física u obtener un certificado digital de vinculación con la organización, acompañando la justificación de su necesidad verificada por su superior jerárquico o por el responsable del servicio con el que colabore.

- Todas las personas que formen parte de una entidad de derecho público dependiente o vinculada a la Diputación y que, en el ejercicio de sus funciones, deban relacionarse con la Diputación, podrán disponer de un certificado de pertenencia a la entidad correspondiente.

Los certificados emitidos a favor de los empleados de la Diputación, de acuerdo con su condición de trabajadores de la Diputación, se emiten para usarse exclusivamente en los procedimientos y trámites que deban efectuar de acuerdo con sus funciones. Concretamente, para:

- Autenticarse en los sistemas de información de la Diputación, si corresponde.

- Autenticarse frente los portales de las administraciones públicas con las que se relacione en el ejercicio de sus funciones.

- Firmar electrónicamente documentos generados por la Diputación.

- Firmar electrónicamente documentos generados por un tercero, relacionados con un procedimiento o expediente electrónico en el ámbito de la Diputación.

6.3. Ciclo de vida de los certificados digitales usados por la Diputación

6.3.1. Obtención, renovación y revocación

La Diputación utiliza como prestador de servicios de certificación de referencia la Fábrica Nacional de Moneda y Timbre (FNMT) y su infraestructura de clave pública, así como Firmaprofesional para la obtención de certificados de empleado público, utilizando como Entidad de Registro la que la Diputación tiene constituida al efecto. Sin embargo, atendiendo a requisitos puntuales, se pueden utilizar los servicios de otra Autoridad de Certificación.

La FNMT, Firmaprofesional o la Autoridad de Certificación correspondiente son las responsables de definir las políticas de gestión de los certificados digitales que emiten y, por tanto, quienes definen la vigencia de los certificados, la forma en que se revocan, se renuevan o se validan.

A los efectos de adoptar los procedimientos establecidos por el prestador de servicios de certificación para operar la Entidad de Registro constituida por la Diputación, se han establecido procedimientos internos que identifican las actividades que se realizan y sus responsables, así como los procedimientos a seguir por los usuarios para la solicitud, renovación y revocación de sus certificados digitales.

6.3.1.1. Certificados digitales del personal de la Diputación

Los certificados digitales de empleado público de la Diputación se emiten y revocan en función de las necesidades del puesto de trabajo, y su gestión corresponde a Registro General, bajo la superior dirección de Secretaría General, de acuerdo con las particularidades de las Autoridades de Certificación emisoras de los certificados digitales, requiriéndose la presentación del titular del certificado ante la Entidad de Registro propia de la Diputación o la que la Autoridad de Certificación determine. Es función de Registro General, por lo tanto, la gestión de las solicitudes y de las renovaciones de certificados digitales de empleado público de la Diputación Provincial de Cádiz. En el caso de la Diputación, el certificado de empleado público ha de solicitarse exclusivamente por las personas empleadas públicas que tengan habilitada la firma electrónica o que utilicen herramientas de otras administraciones públicas, como la Plataforma de Intermediación de Datos, Apoder@, la Plataforma de Contratación, el Tribunal de Cuentas, la Base de Datos Nacional de Subvenciones, el Boletín Oficial del Estado/Autonómico o Provincial, la obtención de certificados de la Agencia Estatal de Administración Tributaria de estar al corriente en las obligaciones tributaria, etc. El certificado de empleado público no se expedirá a quienes efectúen trámites de gestión interna o que no precisen interactuar con terceros.

La Diputación ha habilitado un trámite en la Intranet de la entidad para solicitar la expedición del certificado de empleado público. Las personas interesadas que cumplan con los requisitos recién mencionados podrán rellenar el formulario habilitado a tal efecto, previa autorización de la Dirección de Área o persona responsable del Área o servicio, que se acreditará con la firma en el trámite electrónico. Registro General se encargará de tramitar la solicitud y, si todo es correcto, se procederá a la emisión del certificado de empleado público.

Si el certificado digital es de trabajador público con cargo, se acompañará la solicitud con un certificado por parte de Registro General de la Diputación en la que se certifique el cargo de la persona que solicita el certificado.

En caso de que un trabajador de la Diputación o de una entidad dependiente tenga una incidencia como, por ejemplo, la pérdida del certificado, este debe solicitar su revocación directamente a la Autoridad de Certificación emisora del certificado digital y ponerlo en conocimiento del responsable de su servicio o departamento quien, a la vez, debe comunicarlo a Registro General.

Con carácter previo a la caducidad de un certificado digital, su titular recibe un correo electrónico desde la Autoridad de Certificación correspondiente, informando de su próxima caducidad. El usuario debe comunicarlo a Registro General para que haga una nueva solicitud para su renovación, siguiendo el mismo procedimiento establecido para la solicitud de un nuevo certificado digital, siempre y cuando esta renovación no pueda practicarse de forma directa con la Autoridad de Certificación, en cuyo caso se informará igualmente a Registro General. En caso de no realizar ninguna actuación, el certificado digital caducará sin que pueda utilizarse.

Finalmente, los certificados de representante de persona jurídica son asignados a los funcionarios habilitados correspondientes, mediante autorización expedida por Decreto de Presidencia que limite los usos que se podrán dar a estos certificados. Registro General debe llevar un control de la caducidad de estos certificados y sus asignaciones a los trabajadores públicos de la Diputación para garantizar que sean mantenidos en el tiempo aquellos que sean requeridos, así cómo se estén utilizando por las personas autorizadas para los usos autorizados.

6.3.1.2. Certificados digitales de sello electrónico

Para la solicitud de emisión de un certificado digital de sello electrónico (atribuido a un órgano de la Diputación) o de un certificado técnico, el área de la Diputación o de la entidad dependiente que lo necesite deberá solicitarlo a EPICSA, que es la encargada de realizar la solicitud y descarga del certificado digital para su posterior instalación en el servidor y en las aplicaciones correspondientes.

En el caso de los certificados digitales de sello electrónico (atribuidos a un órgano) y de sede electrónica, también se requiere una autorización por parte de Secretaría General. Los usos de los certificados digitales de sello electrónico para los órganos de la entidad podrán limitarse para efectuar funciones determinadas.

Los sellos electrónicos para la actuación administrativa automatizada son diferentes para cada órgano, de manera que estos últimos deberán disponer de los certificados de sello electrónico necesarios para las funciones encomendadas, realizadas como actuación administrativa automatizada, en virtud de lo que establece el artículo 40 de la Ley 40/2015 y los artículos 19 y 20 del Real Decreto 203/2021.

En este caso, es EPICSA quien gestiona un inventario de los certificados de sello electrónico existentes en la Diputación. El inventario de certificados digitales incluye la información necesaria para su gestión, como el tipo de certificado, su emisor, la aplicación que lo gestiona y la fecha de su caducidad, entre otros.

Las renovaciones y revocaciones de este tipo de certificados también dependerán de EPICSA. En el momento en que esta detecte que un certificado incluido en el inventario esté a punto de caducar, juntamente con el solicitante del certificado digital y teniendo en cuenta si este sello es uno de los empleados para una actuación administrativa automatizada, procederá a la renovación, si procede. En este caso, iniciará el trámite de renovación correspondiente, siguiendo los mismos procedimientos establecidos para la solicitud de un nuevo certificado digital de sello electrónico.

En el caso de que un certificado digital de sello electrónico u otro tipo de certificado técnico deje de ser necesario para la finalidad para la cual fue emitido, deberá existir un procedimiento para identificarlo y comunicarlo a EPICSA para que esta proceda a su revocación, siguiendo el procedimiento que la Autoridad de Certificación emisora establezca a tal efecto.

6.3.2. Almacenamiento de los certificados digitales

Los certificados digitales que se usen en la Diputación se podrán encontrar en:

- El repositorio de gestión de certificados de los ordenadores de los respectivos puestos de trabajo en los casos de certificados de empleado público y de representante, lo cual permite generar firmas avanzadas. El titular del certificado es responsable de proteger el uso de los certificados almacenados en este repositorio mediante una contraseña o PIN que solo conozca él.

- La tarjeta criptográfica, para certificados de empleado público o de representante en soporte tarjeta criptográfica, que permiten generar una firma cualificada o reconocida.

- El servicio de gestión centralizada de certificados que la Diputación contrate a un prestador de servicios de confianza cualificado, que permita almacenar certificados de empleado público o de representante y hacerlos accesibles de manera segura a los usuarios autorizados dentro de la red de la Diputación, lo que permitirá también generar firmas cualificadas o reconocidas.

- Este servidor centralizado podrá ser operado por EPICSA siempre que actúe como dispositivo seguro de creación de firma electrónica certificado por el Centro Criptológico Nacional (CCN) garantizándose el cumplimiento de la normativa y estándares a nivel europeo en materia de firma electrónica.

- El repositorio de gestión de certificados digitales de sello electrónico de los servidores de la Diputación, debidamente protegidos de cualquier uso no autorizado, para llevar a cabo la actuación administrativa automatizada, los de aplicación o para certificados de servidor web y sede electrónica.

Los certificados de sello electrónico también se podrán usar por parte terceros que presten servicios a la Diputación en el caso en que sea imprescindible para que la Diputación pueda ejecutar tareas automáticas. Estos usos serán realizados mediante certificados de sello electrónico que, o bien estarán instalados en servidores propios de la Diputación, o bien serán cedidos a este tercero y

deberán estar descritos en un contrato o convenio a celebrar entre la Diputación y el tercero, acotados a usos concretos y sujetas a las potestades de verificación propias de la Diputación.

6.3.3. Mantenimiento del inventario de certificados digitales

De acuerdo con el apartado 4.5 de esta Política, el Registro General de la Diputación, bajo la superior dirección de Secretaría General, llevará a cabo el mantenimiento del inventario de certificados digitales de la organización. Asimismo, EPICSA, de acuerdo con el apartado 4.4 de esta Política, será la encargada del mantenimiento del inventario de certificados digitales de sello electrónico de la Diputación.

El inventario de certificados digitales será único para todos los certificados personales, sin distinción de la entidad certificadora que los emita, y deberá mantenerse actualizado a partir de la información de las solicitudes, las renovaciones y las revocaciones. Asimismo, deberá incluir la información necesaria para la gestión de estos, que contendrá, como mínimo:

- La titularidad del certificado.
- La autoridad emisora.
- La tipología de certificado.
- La fecha de caducidad.

Se revisará, de forma proactiva, la vigencia de los distintos certificados digitales con una periodicidad mínima semestral. Tal revisión podrá conllevar la revocación de certificados digitales que ya no sean conformes con la presente Política y sus sucesivas modificaciones.

Los principales motivos que pueden comportar la revocación de los certificados son:

- Que los datos que contiene el certificado ya no sean ciertos.
- Que la persona ya no ostente el cargo que identifica el certificado o no tenga atribuidas las mismas competencias que en el momento de emisión del certificado.
- Que la seguridad del certificado haya sido comprometida.

Por lo que respecta a las políticas de emisión, gestión y vigencia de los certificados, se deberá seguir lo establecido por las autoridades de certificación responsables.

En cuanto a los certificados digitales de sello electrónico de la Diputación, los roles y las responsabilidades en relación con estos se exponen en el apartado 4 de la presente Política.

El inventario será único para todos los certificados de sello electrónico de la Diputación, y también incluirá la información necesaria para su gestión, que deberá contener, como mínimo, los datos referentes a:

- La autoridad emisora.
- La tipología de certificado.
- La aplicación que gestiona el certificado digital.
- La fecha de caducidad.

Los principales motivos que pueden comportar la revocación de los certificados de sello electrónico son:

- Que la motivación por la que fueron creados ya no exista o haya sido modificada sustancialmente.
- Que la seguridad del certificado haya sido comprometida.

6.4. Otras identidades digitales usadas por la Diputación

Adicionalmente a la identificación mediante certificado digital la Diputación de Cádiz podrá proporcionar a su personal los siguientes sistemas de identidad electrónica:

- **Identidades digitales basadas en claves concertadas** proporcionadas por la Diputación de manera segura y sometidas a su Política de Seguridad de la Información por la cual cada usuario deberá mantener bajo su exclusivo conocimiento.

- **Identidades digitales generadas en la propia Diputación basadas en registro previo combinadas con mecanismos de doble factor de autenticación,** como contraseñas OTP "One-Time Password" (de un solo uso) o aplicaciones residentes de gestión de identidades mediante la generación de códigos de autenticación con contraseña de un solo uso.

  En este contexto, la Diputación podrá disponer de un Registro de Identidades Digitales en el que se inscriban los datos de los miembros de la entidad y/o de los terceros que participen, colaboren o se relacionen puntualmente con la misma. Este Registro recogerá los datos necesarios para facilitar los servicios de identificación, como credenciales o claves.

- **Sistemas de identificación biométrica**, basados en registro previo. Cuando el personal de la Diputación deba identificarse, sus datos biométricos se compararán con los que estén almacenados por parte de la Diputación para validar su identidad. Dichos datos de comparación deberán haberse registrado previamente y estar guardados de manera cifrada por parte de la Diputación.

7. Sistemas de firma electrónica

Los sistemas de firma electrónica contemplados en este apartado son los que se podrán usar en las aplicaciones corporativas de la Diputación, tanto por el personal de la Diputación como de aquellos que se relacionen con ella, y tendrán la finalidad de garantizar la autenticidad, integridad, inalterabilidad y conservación de los documentos firmados digitalmente.

La presente Política define el uso de un conjunto de sistemas de firma electrónica y sus correspondientes casos de uso, contenidos en el apartado 9, que deberán facilitar la toma de decisiones sobre qué sistema de firma electrónica emplear en cada caso concreto de aplicación de la presente Política.

Cuando los empleados de la Diputación participen en procedimientos definidos por otra organización, generarán las firmas en los formatos que dicha organización determine. Si fuese necesario añadir copia en el expediente de la Diputación se aplicarán las comprobaciones indicadas en el apartado 10.

La Diputación Provincial de Cádiz deberá dar publicidad, en su sede electrónica, de los sistemas de firma electrónica admitidos en cada momento.

7.1. Firma electrónica con certificado digital personal (de persona física, empleado público o de representante)

La firma electrónica mediante un certificado digital personal es un sistema de firma electrónica en el que, partiendo de la clave privada del certificado de una persona, se cifra el resumen criptográfico del documento a firmar y se incorpora el certificado digital usado para efectuar la firma junto con su clave pública e información adicional como, por ejemplo, la fecha de firma o la referencia a la Política de Identidad y Firma electrónicas.

La Diputación usará este sistema para firmar documentos electrónicos por parte del personal de la Diputación y admitirá documentos electrónicos firmados con este sistema por parte de los terceros que se relacionen con ella.

Los procesos de firma electrónica en los que se use este sistema serán tanto de persona física como de empleado público o de representante de una persona jurídica.

7.2. Firma electrónica con sello electrónico de actuación administrativa automatizada

El sistema de firma electrónica mediante sello electrónico de actuación administrativa automatizada (AAA) permite la firma de documentos electrónicos de la Diputación mediante procesos automatizados, sin intervención directa del personal a su servicio.

A partir de la clave privada de un certificado digital de sello electrónico, se cifra el resumen criptográfico del documento a firmar y se incorpora el certificado digital usado para efectuar la firma junto con su clave pública e información adicional como, por ejemplo, la fecha de firma o la referencia a la Política de Identidad y Firma electrónicas.

Este tipo de firma se podrá usar en las actuaciones administrativas automatizadas previamente establecidas mediante resolución del Presidente o de la Presidenta de la Diputación publicada en la sede electrónica de la Diputación, de acuerdo con el artículo 41.2 de la Ley 40/2015.

7.3. Firma electrónica basada en un Código Seguro de Verificación de actuación administrativa automatizada

El uso del Código Seguro de Verificación (CSV) vinculado a la administración pública, órgano, organismo público o entidad de derecho público como medio de firma electrónica está regulado en el artículo 42.b) de la Ley 40/2015, y en el Reglamento regulador de la Administración Electrónica en la Diputación Provincial de Cádiz, y permite comprobar la integridad del documento electrónico mediante el acceso a la sede electrónica de la entidad emisora del mismo.

De acuerdo con el artículo 41.2 de la Ley referenciada en el párrafo anterior, el uso del CSV en los casos de actuación administrativa automatizada deberá estar previsto en la resolución que autorice la automatización del procedimiento correspondiente.

El sistema de firma electrónica basada en un CSV podrá usarse en las actuaciones administrativas automatizadas que se determinen mediante resolución del Presidente o de la Presidenta de la Diputación publicada en la sede electrónica de la Diputación, de acuerdo con el artículo 41.2 de la Ley 40/2015.

El CSV está compuesto por caracteres alfanuméricos y, como metadato del documento al que se vincula de forma unívoca, se almacenará en un Catálogo, no pudiéndose eliminar ni modificar una vez asignado. Este Catálogo constituye un conjunto de elementos del sistema de información de la Diputación que almacena documentos electrónicos, junto con sus metadatos asociados, y que genera el CSV mediante un algoritmo aleatorio y lo vincula al documento electrónico que se firma. El CSV resultante, vinculado al documento firmado y a la aplicación firmante del mismo, se almacena en el Catálogo, el cual no admitirá la duplicidad de un CSV.

La integridad y conservación de los documentos electrónicos almacenados en el Catálogo y de sus metadatos asociados obligatorios quedará garantizada a través de medidas técnicas que aseguren su inalterabilidad.

Para comprobar la integridad de los documentos electrónicos autenticados mediante CSV, se podrá acceder al verificador habilitado para tal caso, accesible desde la sede electrónica de la Diputación, en tanto no se acuerde la destrucción de dichos documentos según la normativa que resulte de aplicación o por decisión judicial. Antes de su acceso se comprobará que el documento correspondiente al CSV consultado se mantiene inalterado a través de las medidas técnicas implementadas y, en su defecto, no podrá accederse al documento.

En los casos en que se intente cotejar en la sede electrónica un documento emitido con CSV que ya no figure en el Catálogo, sea por decisión judicial o por la aplicación de la normativa vigente, aparecerá un mensaje que informará de esta circunstancia al usuario. En el caso de que el documento que se pretenda cotejar haya sido sustituido por otro, con un nuevo CSV, la respuesta al intento de cotejo contendrá una referencia a la existencia y CSV del nuevo documento.

En el caso de que el destinatario del documento sea otra Administración Pública, el CSV deberá complementarse con la superposición de un sello electrónico de la Diputación, según lo establecido en el artículo 21.3 del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. Previa a esta firma de sello electrónico se deberá efectuar la comprobación de la integridad del documento

mediante las medidas técnicas implementadas al efecto y sólo se realizará si la integridad del documento no se ha visto alterada.

7.4. Firma electrónica basada en claves concertadas proporcionadas por la Diputación junto con evidencias de voluntad de firma

El uso de este sistema de identificación más firma basado en claves concertadas está regulado en el artículo 10.2.c) de la Ley 39/2015 y permite generar firmas electrónicas a partir de la identidad del firmante más su voluntad de firma.

El sistema de firma electrónica consistente en el uso de claves concertadas más las evidencias de voluntad de firma se basa en la identificación de la persona firmante mediante su usuario y contraseña, que han sido previamente proporcionados por la Diputación y que constituye una primera evidencia de autenticación.

La usabilidad de este sistema estará condicionada a la calidad del mecanismo de distribución de identidades de la Diputación. En consecuencia, los procedimientos de obtención de las credenciales a usar para generar este tipo de firmas deberán garantizar:

- Que la identidad de la persona haya sido verificada de forma cierta por una persona empleada de la Diputación con carácter previo a la emisión de las claves concertadas, ya que, en caso de no cumplirse tal condición, no se podrán usar para generar firmas, hecho que quedará acreditado en el sistema de gestión de credenciales, que deberá tener capacidad para dejar constancia de tal circunstancia. La verificación posterior de la identidad permitirá convalidar las claves concertadas para su uso futuro como mecanismo de firma.

- Que los sistemas de gestión de las claves concertadas garanticen su custodia segura, su renovación de acuerdo con los periodos establecidos en la Política de Seguridad de la Información de la Diputación y un control sobre el número máximo de intentos fallidos de identificación que lleven al bloqueo de la credencial para prevenir un uso fraudulento.

- Que las personas usuarias reciban la información oportuna sobre la criticidad del sistema de credenciales y la importancia de la confidencialidad de las claves.

Las aplicaciones que hagan uso de este sistema de firma deberán permitir que la persona usuaria verifique los datos a firmar mediante la inclusión de frases que manifiesten la voluntad de firma de manera inequívoca, como, por ejemplo, mediante la confirmación del botón de la aplicación correspondiente con una expresión clara del documento o contenido que sea objeto de firma.

Se solicitará la autenticación de la persona usuaria en el momento de proceder a la firma con la finalidad de garantizar el no repudio de la misma.

Una vez verificada la identidad, se creará un fichero de evidencias que se almacenará en el mismo documento electrónico. En el caso en que no fuera técnicamente posible, las evidencias se guardarán en los sistemas corporativos de la Diputación identificándose formalmente el lugar concreto en el que se almacenarán en el procedimiento administrativo que regule el procedimiento de firma.

Posteriormente a la incorporación de las evidencias, se procederá a firmar el documento electrónico, o el paquete de evidencias si estas no se han podido consolidar, mediante el uso de un certificado digital de sello electrónico de la Diputación y completado con un sello de tiempo, en cualquier caso, sellos emitidos por prestadores de servicios de confianza.

Las evidencias objeto de captura deberán incluir, como mínimo:

- Nombre, apellidos, cuenta de usuario y código identificador (NIF o similar) de la persona firmante.

- Fecha y hora de la identificación de la persona firmante en la aplicación.

- Identificador del trámite.
- Identificador de la transacción de firma y la aplicación responsable de la transacción de firma.
- Fecha y hora de la transacción de firma.
- Título y resumen digital o *hash* de los datos firmados.
- Datos de navegación: dirección IP del cliente y navegador utilizado.

La validez jurídica del sistema de firma electrónica efectuada mediante claves concertadas más evidencias de la voluntad de firma está vinculada al documento electrónico y a las evidencias del proceso de identificación de la persona firmante que acepta la firma.

Es posible que el documento electrónico contenga más de una firma electrónica basada en claves concertadas más las evidencias de voluntad de firma. Se deberá, en cualquier caso, poder garantizar la posibilidad de verificar la autenticidad de cada una de ellas.

En el caso de conflicto entre las firmas que incorpore el documento electrónico, la Diputación podrá acreditar:

- Que el procedimiento de firma está regulado de forma específica.
- Que se han generado las evidencias en todas las firmas del mismo tipo.
- Que la firma se produjo en un momento determinado mediante la aplicación de un sello de tiempo.
- Que el documento no ha sido modificado mediante la aplicación del *hash* en las evidencias del documento.
- Que se ha aplicado una firma secundaria al documento electrónico consistente en la aplicación de un certificado de sello electrónico de la Diputación que garantiza la integridad del conjunto.

7.5. Firma electrónica basada en identidades proporcionadas por terceros junto con evidencias de la voluntad de firma (sistema Cl@ve)

El uso de este sistema de identificación más firma basado en claves concertadas está regulado en el artículo 10.2.c) de la Ley 39/2015 y permite generar firmas electrónicas a partir de la identidad del firmante más su voluntad de firma.

Se contemplará este sistema de firma como un caso particular de firma electrónica de terceros con claves concertadas más voluntad de firma, pero delegando la generación de las evidencias en el sistema Cl@ve.

Este sistema se basa en el uso de la plataforma Cl@ve, y será esta la que solicitará al firmante que se autentique para, posteriormente, generar las evidencias tanto de identificación como de voluntad de firmar.

Cl@ve genera un fichero con las evidencias de identificación, las cuales se guardarán, como en el caso anterior, en el mismo documento a firmar. En el caso que, por algún motivo técnico, no fuese posible almacenar este fichero de evidencias en el mismo documento, estas se guardaran en los sistemas corporativos de la Diputación. En estos casos, en el mismo procedimiento administrativo que regule el procedimiento de firma se informará del lugar donde se almacenarán las evidencias. Posteriormente, se firmará el documento mediante un certificado digital de sello electrónico de la Diputación y completado con un sello de tiempo, en cualquier caso, sellos emitidos por prestadores de servicios de confianza.

Las aplicaciones que hagan uso de este sistema de firma deberán permitir que la persona usuaria verifique los datos a firmar mediante la inclusión de frases que manifiesten la voluntad de firma de

manera inequívoca, como, por ejemplo, mediante la confirmación del botón de la aplicación correspondiente con una expresión clara del documento o contenido que sea objeto de firma.

Se solicitará la autenticación de la persona usuaria en el momento de proceder a la firma con la finalidad de garantizar el no repudio de la misma.

La validez jurídica del sistema de firma electrónica efectuada mediante claves concertadas más evidencias de la voluntad de firma está vinculada al documento electrónico y a las evidencias del proceso de identificación de la persona firmante que acepta la firma.

Es posible que el documento electrónico contenga más de una firma electrónica basada en claves concertadas más las evidencias de voluntad de firma. Se deberá, en cualquier caso, poder garantizar la posibilidad de verificar la autenticidad de cada una de ellas.

En el caso de conflicto entre las firmas que incorpore el documento electrónico, la Diputación podrá acreditar:

- Que el procedimiento de firma está regulado de forma específica.
- Que se han generado las evidencias en todas las firmas del mismo tipo.
- Que la firma se produjo en un momento determinado mediante la aplicación de un sello de tiempo.
- Que el documento no ha sido modificado mediante la aplicación del *hash* en las evidencias del documento.
- Que se ha aplicado una firma secundaria al documento electrónico consistente en la aplicación de un certificado de sello electrónico de la Diputación.

7.6. Firma electrónica del personal de la Diputación basada en un sistema de identificación y completada con CSV

La Diputación utilizará para la producción de firmas electrónicas de sus empleados públicos un sistema basado en la identificación de la persona firmante completado con CSV.

El uso de este sistema de identificación más firma basado en claves concertadas está regulado en el artículo 10.2.c) de la Ley 39/2015 y permite generar firmas electrónicas a partir de la identidad del firmante más su voluntad de firma.

Este sistema de firma electrónica está reservado únicamente al personal de la Diputación y se basa en la previa identificación del firmante mediante una de las identidades digitales usadas por la Diputación según el apartado 6.4 de esta política.

Solo si el usuario se identifica correctamente mediante este mecanismo de firma se generará un CSV vinculado unívocamente al documento, que se incorporará al documento firmado junto con una mención relativa al valor original del documento y su vinculación con la persona firmante.

La validez jurídica del sistema de firma electrónica efectuada mediante el uso de sistemas de identificación está vinculada al documento electrónico y a las evidencias del proceso de identificación de la persona firmante que acepta la firma y quedará regulado por la Política de Seguridad de la Información de la Diputación.

Las aplicaciones que hagan uso de este sistema de firma deberán permitir que la persona usuaria verifique los datos a firmar mediante la inclusión de frases que manifiesten la voluntad de firma de manera inequívoca, como, por ejemplo, mediante la confirmación del botón de la aplicación correspondiente con una expresión clara del documento o contenido que sea objeto de firma.

Para ello se solicitará la autenticación de la persona usuaria en el momento de proceder a la firma con la finalidad de garantizar el no repudio de la misma.

Una vez verificada la identidad, se creará un fichero de evidencias que se almacenará en el mismo documento electrónico. En el caso en que no fuera técnicamente posible, las evidencias se guardarán en los sistemas corporativos de la Diputación identificándose formalmente el lugar

concreto en el que se almacenarán en el procedimiento administrativo que regule el procedimiento de firma.

Posteriormente a la incorporación de las evidencias, se procederá a firmar el documento electrónico mediante el uso de un CSV.

Las evidencias objeto de captura deberán incluir, como mínimo:

- Nombre, apellidos, cuenta de usuario y código identificador (NIF o similar) de la persona firmante.
- Fecha y hora de la identificación de la persona firmante en la aplicación.
- Identificador del trámite.
- Identificador de la transacción de firma y la aplicación responsable de la transacción de firma.
- Fecha y hora de la transacción de firma.
- Resumen digital o *hash* de los datos firmados.
- Datos de navegación: dirección IP del cliente y navegador utilizado.
- Vínculo con el CSV generado.

Este sistema podrá ser utilizado para cualesquiera actos resolutorios o de trámite que requieran su firma por empleado público. Los documentos así firmados no requerirán la incorporación de una firma electrónica basada en certificado digital.

La validez jurídica del sistema de firma electrónica efectuada mediante claves concertadas más evidencias de la voluntad de firma está vinculada al documento electrónico y a las evidencias del proceso de identificación de la persona firmante que acepta la firma.

No es posible, en este caso, que el documento electrónico contenga más de una firma electrónica basada en claves concertadas más las evidencias de voluntad de firma.

En el caso de conflicto entre las firmas que incorpore el documento electrónico, la Diputación podrá acreditar:

- Que el procedimiento de firma está regulado de forma específica.
- Que se han generado las evidencias en todas las firmas del mismo tipo.
- Que el documento no ha sido modificado mediante la aplicación del *hash* en las evidencias del documento.

7.7. Firma electrónica basada en sistemas de identificación completadas con un segundo factor de autenticación

El uso del sistema de firma electrónica basado en sistemas de identificación basados en claves concertadas consiste, por su naturaleza descrita en los tres apartados anteriores, en un método de firma electrónica relativamente simple. Por ese mismo motivo, se recomienda añadir un complemento de segundo factor de autenticación basado en uno de los siguientes sistemas:

- Sistemas One-Time Password (OTP), que permiten la confirmación de la identidad de la persona firmante mediante el envío de una contraseña de un solo uso proporcionada vía mensaje de texto (SMS) o correo electrónico al teléfono o dirección de correo electrónico, respectivamente, proporcionados a la Diputación con anterioridad. Por lo tanto, no será posible usar este mecanismo si la Diputación, previamente al momento de la firma, no dispone de una dirección de correo electrónico o número de teléfono de la persona firmante o si estos datos se proporcionan en el mismo momento de la firma.

- Sistemas de aplicaciones residentes de gestión de identidades que permiten la confirmación de la identidad de la persona firmante mediante la generación de códigos de autenticación con contraseña de un solo uso en sistemas instalados en los dispositivos de las personas firmantes, como Cl@ve Permanente.

La validez jurídica del sistema de firma electrónica efectuada mediante el uso de sistemas de doble factor de autenticación está vinculada al documento electrónico y a las evidencias del proceso de identificación de la persona firmante que acepta la firma y quedará regulado por la Política de Seguridad de la Información de la Diputación.

Se solicitará la autenticación de la persona usuaria en el momento de proceder a la firma con la finalidad de garantizar el no repudio de la misma.

Una vez verificada la identidad, se creará un fichero de evidencias que se almacenará en el mismo documento electrónico. En el caso en que no fuera técnicamente posible, las evidencias se guardarán en los sistemas corporativos de la Diputación identificándose formalmente el lugar concreto en el que se almacenarán en el procedimiento administrativo que regule el procedimiento de firma.

Posteriormente a la incorporación de las evidencias, se procederá a firmar el documento electrónico, o el paquete de evidencias si estas no se han podido consolidar, mediante el uso de un certificado digital de sello electrónico de la Diputación y completado con un sello de tiempo, en cualquier caso, sellos emitidos por prestadores de servicios de confianza.

Las evidencias objeto de captura deberán incluir, como mínimo:

- Nombre, apellidos, cuenta de usuario y código identificador (NIF o similar) de la persona firmante.
- Título y resumen criptográfico o *hash* de los datos firmados.
- Fecha y hora de la transacción de firma.
- Forma de identificación de la persona firmante (nombre de usuario o identidad alegada)
- En el caso del uso de sistemas OTP, correo electrónico o número de teléfono al que se ha mandado el reto adicional emitido.
- En el caso del uso de sistemas de aplicaciones residentes de gestión de identidades, dirección MAC de identificación del dispositivo, código introducido para identificar al usuario o identificador propio de la aplicación que identifique su instalación en el dispositivo concreto.
- Verificación de que el reto ha sido superado con éxito.
- Identificador de la transacción de firma y la aplicación responsable de la transacción de firma.
- Datos de navegación: dirección IP del cliente y navegador utilizado.

En el caso de conflicto entre las firmas que incorpore el documento electrónico, la Diputación podrá acreditar:

- Que el procedimiento de firma está regulado de forma específica.
- Que se han generado las evidencias en todas las firmas de cualquier tipo.
- Que la firma se produjo en un momento determinado mediante la aplicación del sello de tiempo.
- Que el documento no ha sido modificado mediante la aplicación del *hash* en las evidencias

del documento.

- Que se ha aplicado una firma secundaria al documento electrónico consistente en la aplicación de un certificado de sello electrónico de la Diputación.

7.8. Firma electrónica biométrica

Este sistema de firma electrónica avanzada se genera a partir de los datos biométricos de la persona firmante, que se incorporan, de forma cifrada, al resumen criptográfico de los documentos electrónicos generados, de forma que permiten acreditar la auditoría de la firma aplicada mediante la siguiente información necesaria:

- Datos biométricos de la persona que firma el documento de forma manuscrita, que se recogen mediante elementos específicos de captura que permiten la visualización del documento en el mismo acto de firma, entre ellos:
  - El detalle temporal concretado en el inicio, final y duración en milisegundos del proceso de firma del documento.
  - El detalle del trazado, en relación con la velocidad, aceleración y presión de este en toda su figura.
- Otra información que pueda resultar relevante para el proceso de firma, como puede ser la identificación de las aplicaciones y programas usados para la captura de la firma o la localización GPS de las máquinas usadas para captar la firma.

Este sistema de firma electrónica avanzada solo se aplica en la biometría de la firma manuscrita, sin usar otras medidas biométricas como el reconocimiento facial o la huella dactilar, que quedan fuera del ámbito de esta Política, sin perjuicio de que se puedan considerar en un futuro. La firma biométrica se realizará presencialmente frente a un funcionario o funcionaria de la Diputación, quien se encargará de comprobar que la firma efectuada por la persona interesada se corresponde con la de su DNI o pasaporte vigente u otro medio que permita verificar su firma original.

El cifrado de la información se lleva a cabo mediante la clave pública de un certificado específico de firma electrónica biométrica que se almacena en los servidores de la Diputación. La clave privada la custodiará un tercero de confianza al que se le podrá requerir cuando sea necesario para que verifique las firmas biométricas en caso de reclamación o litigio.

Un mismo documento podrá incluir más de una firma biométrica, pero siempre de forma paralela entre ellas.

Una vez se hayan realizado todas las firmas biométricas en paralelo y se haya cifrado la información detallada al principio de este apartado, esta se guardará de forma conjunta con el documento y, con el objetivo de garantizar la integridad de este último, se realizará, sobre este, una firma electrónica automática de sello electrónico de aplicación perteneciente a la Diputación completada con un sello de tiempo.

En consecuencia, la validez jurídica de la firma electrónica biométrica estará vinculada al documento y a las evidencias biométricas que se guardan dentro de este mismo de forma cifrada, con la aportación de la firma electrónica y el sello de tiempo para evidenciar su integridad.

En caso de conflicto, una vez descifrados los datos por parte del tercero de confianza que custodia la clave privada del certificado de cifrado, se deberá solicitar un peritaje de los datos biométricos guardados en el documento y cotejarlos con una nueva toma en condiciones similares, por lo que respecta a la maquinaria, aplicaciones y programas usados en la firma controvertida, de datos biométricos de la persona a quien se alega que pertenecen.

Este sistema se podrá utilizar, adicionalmente, como sistema de identificación en el caso de datos sensibles según lo establecido por la normativa de protección de datos. Los datos biométricos se corresponderán a información biométrica del titular de los datos que, partiendo de un registro previo, se almacenarán cifrados de forma irreversible y cuando se utilicen como medio de identificación se compararán con la misma información biométrica obtenida de forma cifrada.

7.9. Firma múltiple

La firma múltiple se produce cuando existen dos o más firmas electrónicas en el mismo documento. Dependiendo de la forma en que estas se han efectuado, se considera que se han realizado de forma secuencial o paralela:

- **Firma secuencial.** Cuando la segunda firma se realiza sobre el objeto digital ya firmado anteriormente. Siempre que sea posible, se evitará su uso para los circuitos de firma en los que los documentos electrónicos se deban firmar a la vez con el mismo objetivo por parte de una pluralidad de personas.

- **Firma paralela.** Cuando las firmas se refieren al mismo objeto digital que tiene un único resumen criptográfico, sea porque se han generado en formato *detached* (separado) o porque el documento está preparado para recibir firmas *attached* (adjuntas) en paralelo.

El uso de la firma múltiple se dará en varias actuaciones en el marco de los diversos procedimientos administrativos de la Diputación, como la firma de documentos electrónicos por parte de más de una persona o el resellado de documentos firmados con carácter previo a que se pueda poner en duda la validez criptográfica de la firma electrónica, con el objetivo de actualizar su validez legal a lo largo del tiempo.

Se procurará que, en todos los casos de firma de documentos electrónicos por más de una persona, se usen tecnologías similares, evitando particularmente que se generen documentos firmados por una parte basándose en certificados y, por la otra, mediante el uso de la firma biométrica.

La combinación de diversos sistemas de firma electrónica será posible en los siguientes casos:

- Firmas electrónicas mediante el uso de certificados digitales, según el apartado 7.1 de esta política, de forma paralela o secuencial para cualquier documento electrónico que requiera más de una firma.

- Firmas electrónicas mediante sistemas basados en claves concertadas, según los apartados 7.4 y 7.5 de esta política, de forma paralela o secuencial, en el caso de documentos electrónicos que requieran más de una firma. El sistema de claves concertadas de la Diputación es uno de estos tipos de firma.

- Firmas electrónicas biométricas, según el apartado 7.8 de esta política, que serán de forma secuencial, para documentos electrónicos que se generen presencialmente frente a terceros y requieran dos o más firmas.

- Firma electrónica mediante un sistema basado en claves concertadas, según los apartados 7.4 y 7.5 de esta política, y, posteriormente, la aplicación de una firma electrónica mediante un certificado digital, según el apartado 7.1 de esta política, de forma paralela o secuencial, para aquellos documentos electrónicos que requieran la firma de más de una persona y se combinen ambos sistemas de firma electrónica.

  Cuando concurran dos sistemas de firma distintos, se conservarán las evidencias de la firma no criptográfica de manera que el sello electrónico o la firma digital que se incorpore en último lugar dé cobertura a todo el contenido del documento junto con las evidencias de la voluntad de firma.

7.10. Sello de tiempo

El sello de tiempo es un tipo de firma electrónica generada por un tercero de confianza basándose en un certificado digital especialmente diseñado a tal efecto que permite acreditar la fecha y hora en la que se ha producido el acto, que puede hacer referencia a:

- El momento de firma del documento. En este caso, el sello de tiempo estará asociado a la firma electrónica aplicada.

- El momento de la creación del documento. En este otro caso, el sello de tiempo estará asociado al documento electrónico.

Este tipo de firma electrónica sella la fecha y hora del instante en que se realiza el acto mediante un proveedor de sellado de tiempo, que podrá ser la Fábrica Nacional de Moneda y Timbre o la Plataforma de Sellado de Tiempo TS@ de la Administración General del Estado, en función de las aplicaciones que use la Diputación.

Se podrá disponer de un proveedor de sellado de tiempo alternativo para garantizar la disponibilidad de los procedimientos de sellado de tiempo, que deberá estar sincronizado con fuentes fiables de tiempo como, por ejemplo, la Real Armada Española, reconocida como tal por el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

El procedimiento de uso del sello de tiempo consiste en la creación de una evidencia sobre una firma electrónica mediante el cálculo del resumen criptográfico del documento y/o de las firmas electrónicas en caso de resellado. Es decir, se realiza una operación matemática que se aplica al conjunto de información sobre la que se emitirá el sello de tiempo que resulta en una cadena de bits llamada *hash* y que se cifra con la clave privada del certificado de sello de tiempo usado para tal operación.

El resultado de la aplicación del certificado de sello de tiempo da como resultado la incorporación de la fecha y hora de la operación en el documento electrónico, así como información del certificado de sello de tiempo usado para su firma.

En caso de que sea necesario generar un sello de tiempo y el proveedor no esté proporcionando el servicio, la firma debe generarse sin sello de tiempo y la fecha será la que indiquen los servidores de la Diputación. Este caso, distinto al caso explicado en los puntos anteriores, recibe el nombre de "Marca de tiempo". Los servidores de la Diputación están sincronizados en cuanto a tiempo con el organismo nacional encargado de determinar el patrón de tiempo. Una vez se restablezca el servicio de sellado de tiempo, se añadirá el sello de tiempo a aquellas firmas y documentos que hayan quedado únicamente con una marca de tiempo.

7.11. Firma de nivel alto de acuerdo con el Esquema Nacional de Seguridad

De acuerdo con los requisitos de la firma electrónica establecidos por el ENS, esta Política reconoce un sistema de firma electrónica de nivel alto para aquellos servicios y activos de información que sean categorizados como de nivel alto, según la categorización de sistemas de información y la correspondiente declaración de aplicabilidad de medidas de seguridad del ENS realizada por la Diputación.

En el caso de que la Diputación requiera firmar un documento de nivel alto de seguridad, la firma deberá ser, de acuerdo con el ENS, o bien firma electrónica cualificada basada en un certificado digital cualificado asociado a la persona que realiza el acto, empleando productos certificados conforme a lo establecido en el epígrafe 4.1.5 del Anexo II del ENS, o bien usando la firma electrónica avanzada basada en certificado digital cualificado asociado a la persona que realiza el acto, complementada con una verificación de identidad mediante claves concertadas, tal y como se detalla en el apartado 7.4 de la presente Política.

El certificado digital para este segundo tipo de firmas podrá estar emitido en soporte software, pero la plataforma donde se encuentra el documento a firmar debe incorporar un control de acceso con usuario y contraseña o clave de un solo uso, y conservar las evidencias de esta autenticación en el documento firmado o vinculado al mismo.

Este sistema de firma cumple con el Refuerzo R4 previsto en el epígrafe 5.7.3 del Anexo II del ENS y, por tanto, puede aplicar a cualquier tipo de documento, incluso a aquellos que tengan riesgos de nivel alto asociados con su autenticidad o integridad. A los efectos que interesan a la Diputación Provincial de Cádiz, esta firma avanzada complementada con un refuerzo aporta una garantía de autenticidad y no repudio comparable a la de la firma cualificada. La firma cualificada se podrá seguir empleando, pero no será la única solución disponible para firmar los documentos de mayor nivel alto según el ENS.

Cuando un usuario de la Diputación Provincial de Cádiz acceda al sistema empleado para la tramitación de los documentos electrónicos o la emisión de las firmas electrónicas, se identificará

con credenciales concertadas (usuario y contraseña). Una vez autenticado, podrá consultar la documentación y firmar la que le corresponda utilizando el certificado digital cualificado, que podrá tener tanto en soporte tarjeta como instalado en su ordenador.

El sistema de tramitación guardará sistemáticamente, juntamente con el documento firmado, la información del registro de auditoría con todos los eventos en la tramitación del documento. Este paquete de datos incluye la información de cuándo y cómo se autenticó en el sistema el usuario que ha firmado el documento. Esta evidencia, junto con un sello de tiempo que se añadirá tras la firma, serán suficientes para dar cumplimiento al requisito R4 del ENS mencionado anteriormente, siempre y cuando se cumpla lo siguiente:

- La identificación del usuario debe haberse producido con una credencial diferente del propio certificado digital con el que ha firmado.
- La evidencia de identificación se guarda como complemento de seguridad de la firma, pero la firma propiamente dicha es la que genera el certificado, sin que sea estrictamente necesario que incluya la evidencia del segundo factor.
- Se debe guardar el registro de auditoría de las identificaciones en todos los casos de documentos que deben requerir firma de nivel alto.

8. Formato de las firmas electrónicas basadas en certificados digitales

Varios de los sistemas analizados en el apartado anterior se basan en el uso de certificados digitales. Siempre que la firma se base en un certificado digital, se deberán atender las siguientes recomendaciones comunes.

Cuando se usen firmas basadas en certificados digitales, estas serán preferentemente del tipo PAdES cuando se puedan generar como una firma *attached* (adjunta) a un documento en formato PDF; en otros casos, se usará la firma *detached* (separada) en formato XAdES.

En general, se preferirá que las firmas incorporen sello de tiempo, siempre que no se haya determinado que para el procedimiento concreto no se requiera de acuerdo con el tiempo de custodia de los documentos.

A continuación, se adjunta una tabla que detalla los formatos de firma a usar:

	Generalmente, con sello de tiempo	Cuando no sea necesario sello de tiempo
Cuando sea posible, firma attached (adjunta) sobre PDF	PAdES-LTV	PAdES-BES
En otros casos, firma detached (separada)	XAdES-B-T	XAdES-B-B

9. Casos de uso de la firma electrónica

A continuación, se presentan los posibles casos de uso de los sistemas de firma electrónica descritos en el apartado 7, caracterizándolos jurídicamente, recomendando el uso de uno u otro en función del caso analizado y determinando sus requisitos de seguridad.

9.1. Firma electrónica de un documento interno

Este caso de uso hace referencia a los documentos producidos internamente por la Diputación, firmados por el personal en ejercicio de sus funciones o por parte de terceros que participen o colaboren puntualmente con la Diputación, que tengan como destinatario otro usuario interno o el simple cumplimiento de un paso más en el procedimiento. En ningún caso aplica a documentos que vayan a surtir efectos jurídicos ante terceros.

En este caso se permitirá aplicar la firma electrónica en documentos electrónicos en cualquier momento de su ciclo de vida.

Sus principales características son:

- La firma electrónica se realiza sobre un documento original en soporte electrónico.
- El documento original y las firmas deben incorporarse al sistema de firma.
- La firma electrónica deberá ser validada mediante un servicio o autoridad de validación con la finalidad de asegurar su integridad y autenticidad.
- Siempre que sea necesaria la preservación del documento electrónico a lo largo del tiempo, este deberá estar en cualquiera de los formatos admitidos por la Diputación en su política de gestión documental, preferiblemente en PDF/A y XML.

Los sistemas de firma aplicables a este caso son:

- Firma con certificado digital personal, de acuerdo con lo descrito en el apartado 7.1.
- Firma basada en sistemas de identificación, de acuerdo con lo descrito en los apartados 7.4 y 7.6 complementadas, en su caso, con un segundo factor de autenticación, de acuerdo con lo descrito en el apartado 7.7.
- Firma de nivel alto, de acuerdo con lo descrito en el apartado 7.11.
- Firma múltiple, de acuerdo con lo descrito en el apartado 7.10.

9.2. Firma electrónica de un documento con valor para terceros

Este caso de uso se refiere a documentos producidos internamente en la Diputación que han de estar firmados por alguien del personal, o por terceros que colaboren puntualmente con la Diputación, que generan derechos y/u obligaciones a terceros.

Se permitirá aplicar la firma electrónica en documentos electrónicos en cualquier momento de su ciclo de vida.

Sus principales características son:

- La firma electrónica se realiza sobre un documento original en soporte electrónico.
- El documento original y las firmas deben incorporarse al sistema de firma.
- La firma electrónica deberá ser validada mediante un servicio o autoridad de validación con la finalidad de asegurar su integridad y autenticidad.
- El documento electrónico deberá estar en cualquiera de los formatos admitidos por la Diputación, preferiblemente en PDF, PDF/A y XML, con el objetivo de garantizar su preservación a lo largo del tiempo.
- Se expedirá una copia auténtica del documento electrónico que ocultará los datos del DNI de la persona firmante y las evidencias de la firma –en aquellos casos en que la firma se haya efectuado mediante usuario y contraseña y complemento de segundo factor de autenticación–, para garantizar la protección de los datos de carácter personal, y se añadirá un Código de Seguro de Verificación. Esta será la copia que se facilitará a terceros.

Los sistemas de firma aplicables a este caso son:

- Firma con certificado digital personal, de acuerdo con lo descrito en el apartado 7.1.
- Firma basada en sistemas de identificación, de acuerdo con lo descrito en los apartados 7.4 y 7.6 complementadas, en su caso, con un segundo factor de autenticación, de acuerdo con lo descrito en el apartado 7.7.

- Firma de nivel alto, de acuerdo con lo descrito en el apartado 7.11.
- Firma múltiple, de acuerdo con lo descrito en el apartado 7.10.

9.3. Firma electrónica de documentos por parte de terceros

Este caso de uso hace referencia a aquellos documentos electrónicos producidos por la Diputación o terceros y que son firmados por estos últimos en un entorno controlado por la Diputación. En el caso en que este tipo de documentos electrónicos se firme en entornos fuera del control de la Diputación, habrá que atenerse al caso de uso presentado en el apartado 9.7.

Concretamente, este caso aplica en la firma de documentos en el momento de su presentación ante un registro electrónico, o en aquellas situaciones en que el tercero ha de firmar documentos electrónicos en momentos posteriores en su participación en un procedimiento administrativo de la Diputación.

Sus principales características son:

- La firma electrónica se realiza sobre un documento original en soporte electrónico.
- El documento original y las firmas deben incorporarse al sistema de firma.
- La firma electrónica deberá ser validada mediante un servicio o autoridad de validación con la finalidad de asegurar su integridad y autenticidad.
- Siempre que sea necesaria la preservación del documento electrónico a lo largo del tiempo, este deberá estar en cualquiera de los formatos admitidos por la Diputación, preferiblemente en PDF, PDF/A y XML.

Los sistemas de firma aplicables a este caso son:

- Firma con certificado digital personal, de acuerdo con lo descrito en el apartado 7.1.
- Firma basada en sistemas de identificación, de acuerdo con lo descrito en los apartados 7.4, 7.5 y 7.6 complementadas, en su caso, con un segundo factor de autenticación, de acuerdo con lo descrito en el apartado 7.7.
- Firma electrónica biométrica, de acuerdo con lo descrito en el apartado 7.8.
- Firma de nivel alto, de acuerdo con lo descrito en el apartado 7.11.
- Firma múltiple, de acuerdo con lo descrito en el apartado 7.10.

9.4. Firma electrónica de contratos, convenios o acuerdos con otras partes

Este caso de uso aplica a los documentos de carácter contractual multilaterales en los que participa la Diputación de forma conjunta con una o más partes, que se firmarán en entornos controlados por la Diputación. En el caso en que este tipo de documentos electrónicos se firmen en entornos fuera del control de la Diputación, habrá que atenerse al caso de uso presentado en el apartado 9.7.

Sus principales características son:

- La firma electrónica se realiza sobre un documento original en soporte electrónico.
- El documento original y las firmas deben incorporarse al sistema de firma.
- La firma electrónica deberá ser validada mediante un servicio o autoridad de validación con la finalidad de asegurar su integridad y autenticidad.
- El documento electrónico deberá estar en cualquiera de los formatos admitidos por la Diputación, preferiblemente en PDF, PDF/A y XML, con el objetivo de garantizar su

preservación a lo largo del tiempo.

- El documento electrónico se podrá firmar más de una vez, por parte de diversas personas usuarias y de forma paralela o secuencial.

Los sistemas de firma aplicables a este caso para las firmas emitidas por personal de la Diputación son:

- Firma con certificado digital personal, de acuerdo con lo descrito en el apartado 7.1.
- Firma basada en sistemas de identificación, de acuerdo con lo descrito en los apartados 7.4 y 7.6 complementadas, en su caso, con un segundo factor de autenticación, de acuerdo con lo descrito en el apartado 7.7.
- Firma de nivel alto, de acuerdo con lo descrito en el apartado 7.11.
- Firma múltiple, de acuerdo con lo descrito en el apartado 7.10.

Los sistemas de firma aplicables a este caso para las firmas emitidas por terceros son:

- Firma con certificado digital personal, de acuerdo con lo descrito en el apartado 7.1.
- Firma basada en sistemas de identificación, de acuerdo con lo descrito en los apartados 7.4, 7.5 y 7.6 complementadas, en su caso, con un segundo factor de autenticación, de acuerdo con lo descrito en el apartado 7.7.
- Firma electrónica biométrica, de acuerdo con lo descrito en el apartado 7.8.
- Firma de nivel alto, de acuerdo con lo descrito en el apartado 7.11.
- Firma múltiple, de acuerdo con lo descrito en el apartado 7.10.

9.5. Firma electrónica automatizada

Este caso de uso permite la firma de documentos electrónicos de forma automática con plenas garantías jurídicas mediante el uso de certificados de sello electrónico sin la intervención de personas firmantes en el proceso.

Este supuesto está pensado para aquellas tareas en las que se deben firmar documentos de forma automatizada con plenas garantías jurídicas. Para su ejecución, se usará un certificado digital que firmará los documentos en nombre de la aplicación en cuestión y de la Diputación.

Sus principales características son:

- La firma electrónica se realiza sobre un documento original en soporte electrónico de forma automática.
- El documento electrónico podrá estar en cualquiera de los formatos admitidos por la Diputación (preferiblemente PDF, PDF/A y XML), aunque se preferirá el uso del formato PDF/A para documentos que deban remitirse a las personas interesadas.
- Los certificados digitales y las claves privadas que permiten generar procesos de firma automatizada basadas en certificados digitales se guardarán en un repositorio seguro en los servidores de la Diputación o en un servidor de una tercera entidad prestadora de servicios, siempre que esa cesión esté limitada y controlada de acuerdo con lo dispuesto en el apartado 6.3.2.
- Los sistemas de firma aplicables a este caso son:
- Firma con sello electrónico de actuación administrativa automatizada, de acuerdo con lo descrito en el apartado 7.2.

- Firma basada en un CSV de actuación administrativa automatizada, de acuerdo con lo descrito en el apartado 7.3.

9.6. Firma de personas no nacionales ni residentes

Con carácter general, la Diputación admite todos los certificados digitales reconocidos por las autoridades homologadas por el Ministerio correspondiente, de acuerdo con el Reglamento eIDAS.

Dicha admisión puede quedar limitada por las capacidades de las herramientas de interpretación y validación de certificados que use la Diputación, Cl@ve según lo indicado en el apartado 5.1 de esta política, u otras herramientas que puedan utilizarse según lo identificado en el apartado 10.

Se establecen las siguientes directrices con relación a la identificación y firma de personas no nacionales ni residentes en el ámbito de la Diputación y de sus organismos autónomos y entes dependientes:

- Las personas físicas y jurídicas, en su relación con la Diputación deberán obtener un certificado digital de los descritos en el apartado 5.1, que podrá obtenerse por parte de una entidad de certificación de su país. En el caso de ciudadanos residentes en la UE, el reconocimiento será automático de acuerdo con los prestadores de servicios de confianza electrónica cualificados reconocidos por el Reglamento eIDAS, mientras que, en el caso de emisores de certificados situados fuera de la UE, será necesario verificar la solvencia de la Autoridad de Certificación.

- Adicionalmente podrán identificarse alegando sus datos personales, a partir de los cuales se elaborará una identidad mediante el sistema de clave concertada descrito en el apartado 7.4 de la presente Política, que podrá complementarse con el uso del segundo factor de autenticación descrito en el apartado 7.7. En el caso en que se requiera un nivel de firma más alto que el requerido para la firma con claves concertadas, se deberá requerir el uso de un certificado digital.

9.7. Incorporación de documentos electrónicos firmados de fuentes externas

En lo referente a las firmas provenientes de plataformas ajenas a la Diputación, se procederá a su validación, y, una vez validadas, se incorporarán al expediente correspondiente con las correspondientes evidencias de validación.

El apartado 10 contempla las comprobaciones a realizar para proceder a la validación de firmas de terceros.

10. Comprobaciones para tener en cuenta en la validación de firmas electrónicas de terceros realizadas con certificado digital

Para validar las firmas, siempre que sea posible, se implementarán controles de validación automáticos, así como se capacitará al personal de la Diputación para que también puedan realizarlos de forma manual, haciendo uso de los sistemas de validación que se identifican en los apartados 10.1 y 10.2 de la presente Política.

Para garantizar la validez jurídica de los documentos electrónicos firmados digitalmente, cualquier documento que entre en la Diputación y que contenga una firma o un sello de tiempo, previamente a su almacenamiento en el gestor documental, debe ser validado de forma automática. Para ello, se puede emplear alguno de estos sistemas:

- **Verifirma**, la aplicación de validación de firma y certificados que se incluye con Portafirmas. Está instalada en las instalaciones de la propia Diputación y se conecta con Portafirmas y @firma. Esta aplicación es accesible a través de Internet para todos los usuarios de la organización, y únicamente sirve para verificar firmas que se hayan efectuado con el Portafirmas de la Diputación.
- **VALIDe,** una aplicación online de la Administración General del Estado (AGE) que permite determinar la validez de firmas y certificados digitales.

- **Adobe Acrobat Reader,** un programa a través del cual los documentos firmados en formato PAdES también pueden evaluar la validez de una firma digital comprobando sus propiedades. Cuando se obtiene el documento pdf firmado, es posible validar su firma para verificar el firmante y el contenido firmado.

  Dependiendo de cómo se haya configurado la aplicación, la validación puede efectuarse automáticamente. La validez de la firma está determinada por la verificación de la autenticidad del estado del certificado digital y la integridad del documento de la firma.

  La verificación de la autenticidad confirma que el certificado del firmante o sus certificados principales existen en la lista de identidades de confianza del validador. También confirma si el certificado de firma es válido según la configuración de Acrobat Reader del usuario.

  La verificación de integridad del documento confirma si el contenido firmado ha cambiado después de su firma; si cambia, la verificación de integridad del documento confirma si el contenido ha variado de un modo permitido por el firmante.

Para las firmas electrónicas avanzadas y reconocidas, únicamente en aquellos casos en los que el proceso, automático o manual, de validación de todas las firmas electrónicas y de los sellos electrónicos sea satisfactorio, debe almacenarse el documento electrónico dentro del gestor documental de la Diputación.

Para las firmas a través de acreditación de la identidad y de evidencias de la voluntad de firma y biométricas, debe almacenarse el documento electrónico con sus firmas en el gestor documental directamente, sin ninguna validación adicional, ya que los sistemas de firma de ese tipo son seguros y no cuentan con un proceso automatizado de validación.

Para las firmas a través de acreditación de la identidad y de evidencias de la voluntad de firma y las firmas biométricas, se procederá a la firma electrónica del documento con un certificado de sello electrónico en formato -T. En este caso, solo debe realizarse el completado en la firma secundaria y se comprobará su validez igual que se acaba de expresar para las firmas electrónicas realizadas con certificado digital.

10.1. Comprobaciones manuales de la validez de la firma electrónica

En el caso que las comprobaciones automáticas de las firmas electrónicas descritas en el apartado anterior sean incorrectas, se deberá proceder a su verificación mediante comprobaciones manuales, tal y como se expone en los siguientes apartados.

10.1.1. Verificación de la fecha de firma

La fecha de firma de un documento electrónico es relevante para gestionar la validez del certificado de la persona firmante.

Es posible que el documento electrónico tenga una fecha de firma en su contenido, pero que esta no coincida con la fecha de la firma electrónica. En consecuencia, se deberá verificar que la fecha en la que se ha firmado el documento y diferenciar si la fecha de firma se ha establecido mediante un sello de tiempo o usando el reloj del dispositivo de la persona firmante.

Solo en el caso de que la fecha de la firma electrónica provenga de un sello de tiempo, existirá una seguridad fidedigna del momento en que se produjo la firma, con independencia de la fecha que conste en el contenido del documento electrónico.

Si bien estas comprobaciones se realizarán de forma automática mediante la aplicación de captura del documento, también se podrán efectuar manualmente por parte del personal de la Diputación.

10.1.2. Identificación de la titularidad y la cadena de confianza

La generación de una firma electrónica requiere el uso de un certificado digital reconocido, que deberá ser necesariamente emitido por parte de una entidad prestadora de servicios electrónicos de confianza cualificados. Este hecho permite acreditar que la firma electrónica usada es segura y garantizar la identidad de la persona firmante.

Si la verificación del emisor del certificado digital falla, sea automática o manualmente, la Diputación

no depositará su confianza en la firma del documento electrónico y este será rechazado y devuelto al firmante, indicando que no puede ser admitido debido a que la firma electrónica no ha sido realizada con un certificado digital emitido por un prestador de servicios electrónicos de confianza cualificado.

10.1.3. Verificación de la vigencia del certificado

Los certificados digitales podrán caducar de acuerdo con la fecha fijada en el momento de su emisión, o incluso ser suspendidos o revocados antes de tal fecha por varios motivos, como, por ejemplo, la pérdida de vigencia de los datos de los certificados o la pérdida de la tarjeta criptográfica.

Teniendo en cuenta lo expuesto en el párrafo anterior, la Diputación deberá comprobar la validez de las firmas emitidas de acuerdo con los datos aportados por el certificado o la autoridad de certificación siguiendo los siguientes procedimientos:

- Verificación de las listas de revocación de certificados (CRLs), implementada automáticamente por la mayoría de las aplicaciones que permiten la visualización de los documentos firmados del mercado, pese a que no generen pruebas concretas.

- Solicitud de un informe de verificación (OCSP), por parte del prestador de servicio de certificación, pero que se deberá solicitar mediante un sistema informático de la Diputación.

Es posible que el certificado caduque después de la firma de un documento. Por este motivo, es importante que la Diputación sea capaz de acreditar que el certificado era vigente en la fecha de emisión de la firma mediante la aplicación de un sello de tiempo emitido por una autoridad de sellado de tiempo (TSA), según lo expuesto en el apartado 7.10.

10.1.4. Verificación de la vinculación criptográfica del documento con la firma

Esta verificación se lleva a cabo para validar que la firma electrónica hace referencia al documento que se alega haber firmado, ya que es posible que el documento pueda haber sufrido modificaciones posteriores al momento de su firma, por lo que la firma ya no se corresponderá con el contenido del documento, delatando un problema de integridad del mismo.

En los procesos de incorporación del documento en el sistema de gestión documental de la Diputación, la verificación se llevará a cabo mediante un procedimiento de validación automática. No obstante, esta comprobación también se podrá efectuar manualmente mediante el uso de aplicaciones ofimáticas que permitan la visualización de documentos firmados electrónicamente y la interpretación de la validez de su firma.

Cuando este proceso de verificación falle, se considerará que la firma es defectuosa y se procederá a la devolución del documento electrónico a su emisor, informando del motivo de rechazo.

10.2. Comprobaciones manuales de la validez de la firma electrónica en relación con el firmante y su contenido

En cualquier caso, tras las comprobaciones automáticas y manuales anteriores deberán realizarse una serie de comprobaciones manuales relacionadas con la capacidad de firma por parte del firmante y el contenido del documento que se detallan a continuación.

de las firmas electrónicas descritas en el apartado anterior sean incorrectas, se deberá proceder a su verificación mediante comprobaciones manuales, tal y como se expone en los siguientes apartados.

10.2.1. Identidad del titular del certificado

Teniendo en cuenta que un certificado digital proporciona información para identificar a la persona física o jurídica que se compromete con el contenido del documento, verificar su identidad mediante las referencias que se puedan extraer del certificado digital resulta clave para poder establecer que un documento ha sido firmado por la persona que debe.

En el caso de firma mediante representación, deberá constar información del representante y de la

persona representada en el campo correspondiente.

Si el titular del certificado coincide con la persona que consta como firmante del documento o su representante, se puede dar la verificación por válida, mientras que en el caso en que el titular del certificado no coincida con la identidad de la persona que debería firmar el documento, se deberá rechazar el documento por no poder admitirse su firma.

10.2.2. Validación de las facultades del firmante

Es posible que algunas veces se firme en nombre de un tercero. En ese caso, la Diputación deberá comprobar que el firmante está capacitado para ejercer la representación alegada, en el caso en que esas facultades no consten en el propio certificado digital o no se puedan comprobar como, por ejemplo, el nivel de capacidad de representación según el importe de una transacción económica.

Es por ello por lo que, en algunos casos, puede resultar adecuado requerir la presentación de documentación adicional que permita acreditar la representación u optar por la opción de verificar su identidad mediante el acceso a registros externos.

Cuando no sea posible verificar la suficiencia de poderes de representación de la persona firmante, se deberá retornar el documento a su emisor.

10.2.3. Verificación del contenido del documento propuesto por la Diputación para firma de un tercero

La verificación del contenido de un documento electrónico es tan esencial como la de un documento en papel, aunque en el caso del documento electrónico, las comprobaciones se centrarán en el análisis sobre la adecuación del contenido y si se ajusta a los requisitos necesarios para gozar de validez jurídica.

En el caso de que el documento se haya producido en origen por la propia Diputación, se recomienda hacerlo firmar al tercero, previa firma mediante un sello de órgano de la Diputación, con tal de automatizar la verificación del retorno mediante la comprobación de la firma electrónica de sello electrónico, tal y como se ha expuesto en el apartado 10.1.4.

Si no se puede verificar de forma automática, se deberá revisar manualmente el contenido del documento para garantizar que no se ha producido ningún cambio entre la versión mandada al firmante y la versión que se devuelve firmada.

Si la verificación falla, se procederá a la devolución del documento firmado por el tercero.

11. Estrategia de preservación de documentos y firmas electrónicas

Pese a que la firma electrónica permite acreditar la autenticidad de la expresión de la voluntad en documentos electrónicos, existen ciertos riesgos para su plena validez que deben gestionarse debidamente para garantizar la validez jurídica indefinida del documento electrónico.

Tales riesgos son:

- La caducidad o revocación del certificado digital o del sello electrónico mediante el cual se firma un documento electrónico.
- La ausencia de validez del certificado digital o del sello electrónico en el momento en que se genera la firma electrónica.
- La posible obsolescencia tecnológica de la longitud de las claves criptográficas contenidas en los certificados digitales mediante los cuales se generan firmas electrónicas.

Para garantizar la validez de las firmas electrónicas recibidas y emitidas por la Diputación, la estrategia adoptada se basa en un modelo de evidencias de integridad que ofrece el sistema de gestión de documentos electrónicos cuando almacena los documentos una vez hayan sido correctamente firmados. Por este motivo, todas las firmas electrónicas de documentos recibidos deben validarse antes de su incorporación en el sistema de gestión de documentos electrónicos y rechazarse en caso de que no sean válidas.

Para garantizar el mantenimiento y la preservación de las firmas electrónicas, y contrarrestar así los riesgos ya mencionados, la Diputación se dota de dos mecanismos que se podrán emplear indistintamente o de manera complementaria: la preservación de documentos y firmas electrónicas mediante resellado de tiempo, y la preservación de documentos y firmas electrónicas mediante evidencias seguras del sistema de gestión documental.

11.1. Preservación de documentos y firmas electrónicas mediante resellado de tiempo en entornos propios

El proceso de resellado consiste en la renovación del sello de tiempo aplicado al documento electrónico, mediante la incorporación de un nuevo eslabón en la cadena de evidencias electrónicas a las firmas electrónicas que el documento ya contiene. El objetivo principal del proceso es garantizar la conservación, integridad y autenticidad del documento electrónico a lo largo del tiempo.

El resellado se aplicará a aquellos documentos electrónicos aún no transferidos al Archivo Electrónico Único o al documento índice de los expedientes electrónicos que hayan sido transferidos al Archivo Electrónico Único de la Diputación en el momento en que esté a punto de caducar el último sello de tiempo aplicado a la firma electrónica a preservar y, de forma excepcional, cuando se haya detectado la obsolescencia tecnológica de los algoritmos o claves que firman el documento en cuestión.

Este proceso requiere que las firmas del documento sean del formato XAdES-A o PAdES-LTV, que son los tipos de firma que admiten añadir evidencias temporales. En el caso en que la firma no esté en uno de estos dos formatos, antes de llevar a cabo el proceso de resellado habrá que completar la firma de los documentos en uno de los formatos indicados.

Por lo tanto, se deberá añadir un nuevo sello de tiempo a las firmas XaDES-A o PAdES-LTV, que deberá:

- Estar generado con un certificado reciente.
- Tener periodo de validez superior a las firmas a resellar.
- Tener una longitud de clave suficiente con el objetivo de que no pueda resultar comprometida.
- Aplicar un algoritmo o clave que no esté sujeto a la obsolescencia criptográfica del mismo en el momento en que se emite.

Por lo que respecta a las firmas realizadas mediante la acreditación de la identidad y la recogida de evidencias de la voluntad de firma, se procederá al resellado de la firma secundaria.

Cuando la Diputación pretenda revisar la validez de las firmas electrónicas, llevará a cabo los siguientes pasos para cada tipo de firma:

- En el caso de firmas electrónicas generadas dentro del entorno de la Diputación, se procederá a la generación de las firmas en formatos que permitan garantizar su preservación durante la fase de tramitación del procedimiento administrativo. En consecuencia, para los documentos en formato XML, las firmas se transformarán al formato XAdES-A y, para los documentos PDF, al formato PAdES-LTV.
- Cuando las firmas electrónicas provengan de plataformas externas, se procederá a completarlas en un momento posterior al cierre y foliación del expediente administrativo. En consecuencia, para los documentos en formato XML, las firmas se transformarán al formato XAdES-A y, para los documentos PDF, al formato PAdES-LTV.
- Cuando por cualquier motivo no sea posible generar firmas electrónicas con garantías de preservación, se procederá, lo más brevemente posible, a generar una copia electrónica auténtica del documento original. Tal proceso resultará en la aplicación de una firma en formato que garantice la preservación de la copia electrónica auténtica, que substituirá al

documento original.

- En lo que se refiere a las firmas electrónicas basadas en la identidad más la voluntad de firma, se generará la firma mediante la aplicación del sello electrónico en un formato que garantice la preservación, preferentemente PAdES-LTV.

- En el caso de las firmas electrónicas basadas en Códigos Seguros de Verificación (CSV), se mantendrá una versión del documento electrónico guardada en los repositorios de consulta, con las firmas electrónicas en formatos que garanticen su preservación.

- En referencia a las firmas biométricas, se generará firma electrónica mediante la aplicación de un sello electrónico en formato que garantice su preservación (PAdES-LTV).

11.2. Preservación de documentos y firmas electrónicas mediante evidencias seguras del sistema de gestión documental

Este mecanismo de preservación de documentos y firmas electrónicas supone la utilización de evidencias seguras del sistema de gestión de documentos electrónicos de la Diputación. Este método implica, en primera instancia, la confianza en el sistema de gestión documental empleado por la Diputación, ya que es el propio sistema el que garantiza la integridad de los documentos incorporados en el sistema. De este modo, aquellos documentos que no presenten una firma electrónica válida no serán incorporados en el gestor documental.

En aplicación de esta estrategia de preservación, siempre que se almacene un documento, se generará y guardará el *hash* o resumen criptográfico asociado al mismo en forma de metadato de gestión documental y como medida para garantizar su integridad. Asimismo, y con la finalidad de asegurar la validez del *hash*, la Diputación aplicará las medidas de vigilancia necesarias en el sistema que se utilice, según las soluciones tecnológicas disponibles en cada momento, garantizando en todo momento la integridad e inviolabilidad de la información sobre *hash* y su vinculación con el documento correspondiente.

Asimismo, procederá a una actualización del método de cálculo del *hash* en caso de que el anterior pueda verse comprometido, generando un nuevo *hash* y guardando al mismo tiempo el *hash* anterior como medida adicional que permita garantizar la integridad del documento. Al consultar un documento almacenado en el sistema de gestión de documentos electrónicos de la Diputación, se deberán comprobar las evidencias de integridad mediante el cotejo del *hash* obtenido y el almacenado en el sistema de gestión documental para ese documento. En el caso de que coincidan, se podrá obtener una copia auténtica para su consulta generada mediante actuación administrativa automatizada y firmada electrónicamente con CSV, de acuerdo con lo expuesto en el apartado 7.3 de la presente Política y/o firma con sello electrónico de actuación administrativa automatizada según lo expuesto en el apartado 7.2.

La copia auténtica generada no será almacenada en atención a que puede volver a ser generada en cualquier momento, ya sea porque exista una nueva consulta o porque se introduzca un CSV para su comprobación. Por lo tanto, el CSV quedará vinculado al documento de forma inequívoca, de manera que para cada nueva consulta se genere con el mismo CSV o pueda comprobarse su integridad a partir del CSV.

Cuando se emplee este sistema de preservación no será necesario el resellado de las firmas electrónicas, ya que es el sistema el que aporta las garantías y la certeza de que las firmas no han sido modificadas o alteradas desde su almacenamiento, gracias a las medidas de seguridad que aplique la Diputación.

11.3. Preservación de documentos y firmas electrónicas en expedientes transferidos al Archivo Electrónico Único

11.3.1. Selección de formatos documentales de conservación

Las actuaciones que permiten la preservación del formato del documento, sus elementos de seguridad, firmas electrónicas y sellos de tiempo son necesarias para garantizar la inteligibilidad e integridad de los documentos electrónicos a largo plazo.

De acuerdo con el párrafo anterior, el sistema de preservación de documentos electrónicos debe realizar controles periódicos sobre estos mismos para garantizar su accesibilidad, la posibilidad de recuperarlos y su validez jurídica, que comprobarán:

- La accesibilidad de sus soportes.
- La capacidad de lectura de sus formatos.
- La validez jurídica de las firmas electrónicas.
- La integridad de los documentos.
- La integridad de los expedientes.

En el caso en que los documentos provengan de una fuente externa a la Diputación y no se encuentre en uno de los formatos admitidos por la entidad –según su Catálogo de Formatos Documentales–, estos se convertirán mediante un proceso de copia auténtica a uno de los formatos admitidos.

En cualquier caso, con la finalidad de garantizar la validez de la firma electrónica, se aplicará el criterio establecido previamente, que consiste en completar las firmas existentes en formatos que permitan garantizar su preservación a lo largo del tiempo, concretándose estos en:

- XAdES-A para los documentos en formato XML con firmas XAdES.
- PAdES-LTV para los documentos en formato PDF o PDF/A.

Partiendo de estas firmas y en el momento en que el sello electrónico caduque, se procederá al resellado de las firmas electrónicas mediante la aplicación de un nuevo sello, con una caducidad suficiente y con los algoritmos o claves de firma actualizados.

El formato aplicado al foliado del expediente será XML, puesto que es el formato que permite una mejor actuación administrativa automatizada garantizando la integridad del expediente.

Alternativamente o de forma complementaria, en el caso de optar por la estrategia de preservación basada en evidencias seguras del sistema de gestión documental con carácter previo al ingreso de los documentos en el Archivo Electrónico Único, se comprobará la integridad del *hash* de los documentos ingresados que solo serán ingresados si la comprobación no falla. En tal caso, el Archivo Electrónico Único almacenará como metadato el *hash* y garantizará en todo momento su integridad y vinculación con el documento correspondiente y, en caso de que una función *hash* pueda verse comprometida, la sustituirá por una nueva generando y guardando de forma segura el nuevo *hash*, así como el anterior.

11.3.2. Requisitos de los elementos a transferir al Archivo Electrónico Único

Los elementos seleccionados para su transferencia a la herramienta de archivo longevo deberán cumplir con los siguientes requisitos:

- Los expedientes deberán estar en la herramienta de gestión documental, cerrados y foliados de forma íntegra con los documentos que forman parte de este y con los resúmenes criptográficos de los mismos.
- Los metadatos obligatorios de los documentos, expedientes y firmas deberán estar informados de forma correcta de acuerdo con el vocabulario de metadatos de gestión documental propio de la Diputación.
- Los documentos electrónicos deberán estar en un formato reconocido, gestionable y no obsoleto según la herramienta de archivo longevo usada.
- Las firmas electrónicas de los documentos y expedientes deberán estar completadas en formatos que garanticen su preservación o deberán incorporar evidencias seguras basadas

en *hash* que garanticen de forma segura la integridad del documento.

11.3.3. Mantenimiento y migración de formatos

A pesar de que en origen se determinen los formatos que puedan garantizar una mayor preservación de los documentos a lo largo del tiempo, hay que tener en cuenta la posibilidad de que tales formatos puedan acabar quedando obsoletos, sea por motivos de seguridad o por su substitución por otras tecnologías que provocan que los formatos dejen de ser estándares comúnmente aceptados.

Los documentos en formato obsoleto o en proceso de obsolescencia deberán migrarse a nuevos formatos más adecuados que permitan cumplir con las funciones de preservación.

La Diputación considera que la migración es la opción más recomendable para poder garantizar el acceso a la documentación con independencia del tiempo transcurrido, mediante la aplicación de las recomendaciones de los estándares internacionales ISO 18493:2018 y el modelo OAIS (Sistema de información de archivo abierto) definido en el estándar ISO 14721:2003.

La implementación tecnológica de la migración dependerá de las soluciones tecnológicas disponibles en cada momento. No obstante, se contemplan dos alternativas:

- Definir un procedimiento de migración certificado dentro del propio sistema de gestión de documentos electrónicos o del archivo electrónico de la Diputación, siempre que el procedimiento sea capaz de garantizar la equivalencia funcional entre el documento original y el resultante del proceso, y certificar la migración mediante una actuación administrativa automatizada que genere una copia auténtica del documento.

- Delegar el proceso de migración a un tercero de confianza mediante el uso de una plataforma que permita transferir y recuperar los documentos de forma segura, siempre que el documento resultante cumpla con los mismos requisitos anteriores.

Siempre que el documento resultante contenga firmas electrónicas criptográficas vinculadas al resumen criptográfico del documento original, la firma y documento original se conservarán con la finalidad de poder seguir acreditando su autoría, pese a que la consulta e inteligibilidad del documento estarán garantizadas en el documento copia auténtica resultante de la migración.

En cualquier caso, antes del proceso de copia auténtica se deberá comprobar la integridad del documento y de sus firmas electrónicas a partir de:

- La validez de las firmas electrónicas del documento o la del documento índice del expediente, si la estrategia de conservación está basada mediante el resellado de tiempo.

- La integridad del *hash* del documento almacenado como metadato en comparación con el *hash* obtenido aplicando la misma función criptográfica justo antes del proceso de migración del formato, si la estrategia de conservación está basada en evidencias seguras del sistema de gestión documental.

12. Mantenimiento de la Política

12.1. Despliegue de la Política de Identidad y Firma Electrónicas

La actualización de la presente Política requerirá que se lleve a cabo la adecuación de las diversas aplicaciones, herramientas informáticas y procesos que se usen en la Diputación. En ese caso, la UTAE coordinará la actualización de todos los sistemas afectados para adecuarlos a lo que dispone la presente Política y EPICSA ejecutará dicha actualización y se encargará de fijar anticipadamente los plazos de ejecución para ello

Los servicios y sistemas que se pongan en funcionamiento con posterioridad a la entrada en vigor de la Política de Identidad y Firma Electrónicas de la Diputación estarán sujetos a estos desde el momento en que empiecen a operar.

EPICSA deberá examinar, con una periodicidad bienal y con la finalidad de comprobar el estado de cumplimiento de la Política, su adecuación a las necesidades reales del personal de la organización y su alineación con las tecnologías disponibles, informando de ello a Secretaría General.

12.2. Situaciones transitorias

Los métodos de identificación y firma contemplados en la presente Política se empezarán a usar de forma progresiva, conforme a que la Diputación disponga de las aplicaciones, herramientas y procesos necesarios para su uso.

12.3. Derogación de Políticas obsoletas

La aprobación de la presente Política de Identidad y Firma Electrónicas supone la derogación de la Política de Firma Electrónica de la Diputación Provincial de Cádiz, aprobada por Decreto número SINFO-00017-2017 de fecha 8 de mayo de 2017, publicado en el Boletín Oficial de la Provincia de Cádiz el 24 de mayo de 2017.

ANEXO I DE LA PIFE-DPCA

Aprobada la Política de identidad y firma electrónicas, se pretende su puesta en práctica, siendo para ello imprescindible el desarrollo de las siguientes actuaciones:

Primero.- Presentación de documentación por Sede

Vista la práctica habitual de las diferentes Administraciones Públicas, en la que los formularios presentados por Sede Electrónica se firman con sello de órgano, se acuerda mantener el sistema actual, mediante el cual la documentación presentada por Sede se firma con sello de órgano de Diputación.

No obstante, se va a eliminar del cajetín la referencia a que se firma por la Diputación, incluyéndose en el mismo, exclusivamente, que está presentado por el interesado y el CSV.

También se procederá a eliminar el acceso alternativo a la Sede Electrónica, que conlleva la autenticación mediante certificado digital.

Segundo.- Formato de firma

A la fecha, la Diputación utiliza los siguientes formatos de firma:

- PAdES.- Para los sellos electrónicos.
- XAdES.- Para la firma con certificado digital.

Tras la aprobación de la PIFE-DPCA se plantea la unificación del formato y del tipo de firma que, entre otras cosas, facilitará la automatización de actuaciones, valorándose las siguientes opciones:

- PAdES.- Cuyas ventajas son que la firma se incrusta en el propio documento, genera un único archivo y se trabajaría con documentos originales en TR@DIZ, tramitador de expedientes electrónicos de la Diputación Provincial de Cádiz. La desventaja es que la firma aunque es visible dentro del Panel de firmas del lector de PDF, no se estampa en las propias páginas del documento información alguna sobre la firma del mismo y, además, si el documento es abierto desde un navegador web este tipo de firma no es visible, dando la impresión de no estar firmado. Para poder evitar en la medida de lo posible esta confusión, se confirma que antes de la firma puede estamparse una leyenda para informar que el documento está firmado.

- XAdES.- Es el formato más usado. Su ventaja principal es que el informe de firma genera un cajetín de firmas que se estampa en el documento y el usuario puede ver claramente los firmantes del documento. Entre las desventajas destacamos que la firma electrónica no queda incrustada en el documento generado, y por tanto, lo que se genera es una versión amigable, un informe de firma del documento, y no el original del mismo, pues el original consta de dos ficheros: el del propio documento y el de la firma electrónica. Mantener su uso, además, impide actuaciones automatizadas cuando es precisa una firma con certificado previa al sello, pues no procede el uso conjunto de los dos sistemas de firmas electrónicas que se emplean en la Diputación, el tipo XAdES, para firma con certificado, y el tipo PAdES, para la firma con sellos electrónicos.

- Código Seguro de Verificación para actuaciones automatizadas.- Entre sus ventajas se encuentra que no precisa resellado y que es más rápida. Entre sus desventajas está la necesidad de que su uso ha de ser regulado previamente y que, para su posterior remisión a otras administraciones, sería preciso firmarlo con sello de órgano.

A la vista de las ventajas y desventajas, se entendió por el grupo que procede normalizar la firma en formato PAdES para toda la documentación que se genere en la Diputación Provincial de Cádiz.

De cada documento firmado se generará un hash que, cuando haya que remitir el documento a otra

administración o ponerlo a disposición del ciudadano/interesado, nos permitirá obtener una copia auténtica del documento firmado. Esta copia auténtica, que se firmará con sello y a la que se le incorporará un CSV, será la que se traslade, no el original, de forma que no se puedan ver los datos del firmante y así cumplir con la ley de protección de datos.

Para la generación del CSV referido se plantean diferentes posibilidades que se utilizan, para diferentes actuaciones, en el Servicio de Recaudación:

- Encriptar un código de barras.
- Incluir una secuencia interna de encriptado.
- Utilizar el mismo esquema que Notific@.

Dado que esta sistemática está debidamente tasada y es acorde con el esquema de Notific@, se decide extender este mecanismo de Noticadiz de generación de CSV en la firma PAdES, de forma general en Diputación.

La decisión adoptada conlleva la modificación del Esquema Institucional de Metadatos, pues se hace preciso implementar un nuevo metadato que recoja el CSV. La modificación del Esquema se realizará cuando corresponda sin perjuicio de su utilización una vez consensuado.

Tras la puesta en práctica de esta medida será necesario impartir la correspondiente formación a los usuarios, dado que dejarán de ver el cajetín de firma en los documentos generados.

No procede, a la fecha, la calendarización del proyecto pues supone un cambio importante ya que requiere comprobar todos los aplicativos que generan firmas (Portafirmas, Gestión de decretos, Registro, Registro de bienes y actividades, etc.) para adaptarlos a la firma PAdES, si bien es un trabajo que depende exclusivamente de EPICSA.

Tercero.- Firma longeva

Definido el formato de firma, se opta por incorporar la firma longeva dado que este sistema garantiza la autenticidad de la firma aportando mayor seguridad al sistema.

Para su puesta en práctica se elevó consulta al Ministerio desde donde nos informan que con las librerías Integr@, que permiten realizar firmas con sello de tiempo en una sola transacción de firma, no es posible incluir en la firma la información de no caducidad y no repudio de los certificados usados que proporciona el protocolo OCSP que se está comprobando en dicho proceso.

Por esa razón, se ha decidido que EPICSA, para las firmas PAdES con sellos de órgano, realice un cliente que, a la vuelta de la firma, con las librerías de Integr@ incluya en el fichero de firma la información que proporciona el protocolo OCSP. De esta forma, las firmas conformadas de esta manera serían PAdES LT-Level y, por lo tanto, longevas. Tras las consultas efectuadas y pruebas realizadas, la firma con sello se realizará a través de @firma v6.4 federado, es decir, instalado en EPICSA, y posteriormente con el TSA (sello de tiempo) se conformará la firma del sello como longeva.

En cuanto a la documentación firmada por nuestro actual cliente de firmas electrónicas, Portafirmas, que actualmente realiza firmas electrónicas en formato XAdES T-Level, habría que configurar el cambio de formato de firma a nivel de aplicación para que fuera PAdES LT-Level. Dado que las firmas se inician y finalizan en el mismo formato, aquellas que se encuentren iniciadas en formato XAdES T-Level continuarán así hasta su finalización. Mientras que las firmas que se inicien a partir del cambio, se realizarán ya con el nuevo formato configurado a nivel de aplicación, es decir, PAdES.

Cuarto.- Garantizar la autenticidad de los documentos tras la caducidad de la firma

A fin de garantizar el mantenimiento y la preservación de las firmas electrónicas generadas por la Diputación Provincial de Cádiz, a la fecha de aprobación del presente documento se plantean dos estrategias:

- Preservación de documentos y firmas electrónicas mediante resellado de tiempo. Consiste en el resellado de toda la documentación firmada cuando caduque el certificado con el que se firmó. Entre sus ventajas, la seguridad jurídica extra que otorga al documento. Entre las desventajas está el volumen de documentación duplicada que se generaría, la necesidad de seguir resellando de forma continua y el volumen de trabajo que generaría.

- Preservación de documentos y firmas electrónicas mediante evidencias seguras del sistema de gestión documental (sistema criptográfico a demanda). Evita las desventajas del resellado, si bien garantiza exclusivamente la seguridad jurídica de aquellos documentos que necesitan ser contrastados pero no de la totalidad de los documentos que obran en el gestor documental.

Analizadas ambas estrategias se opta por lo siguiente:

- Para los documentos cuya firma ya esté caducada, se establecerá entre EPICSA y Secretaría General un protocolo que permita garantizar la inalterabilidad del documento. Garantizada la autenticidad del documento con la firma caducada, se procederá de forma automatizada (a través del sello de Secretaría) a expedir una copia auténtica del documento. Se subirá a G-EDE el documento original, con la firma caducada, y la copia auténtica, sobre la que se generará el hash.

- Respecto de los expedientes y documentos que consten en TR@DIZ, dado que G-EDE, por el momento, no cuenta con sistema de resellado de documentos, se firmarán con sello longevo antes de su transferencia al Archivo Electrónico Único, lo que garantiza 10 años más de garantía de autenticidad. Además de ello, antes de subir a G-EDE se generará un hash que se incluirá en el documento como metadato.

- Sin perjuicio de ello, a partir de la aprobación de la PIFE-DPCA se implementará el sistema criptográfico a demanda, de forma que no se precise el resellado ni de los documentos ni del índice.

Para ello a la firma del documento se generará de forma automática un hash antes de su envío a G-EDE, de forma que el trabajo depende exclusivamente de EPICSA y cuyo desarrollo no genera dificultades.

La decisión adoptada conlleva la modificación del Esquema Institucional de Metadatos, pues se hace preciso implementar un nuevo metadato que recoja el hash. La modificación del Esquema se realizará cuando corresponda sin perjuicio de su utilización una vez consensuado.

ANEXO II DE LA PIFE-DPCA

Glosario

Se ha considerado adecuado incorporar un anexo con las definiciones de algunos de los conceptos utilizados en este documento, con la finalidad de contribuir a una mayor comprensión de los contenidos que se exponen en la presente Política de Identidad y Firma Electrónicas:

- **Casos de uso de la firma electrónica.** Posibles escenarios de generación de documentos electrónicos firmados. Por cada caso de uso se identifican los formatos de firma electrónica aplicables, los posibles niveles de firma…

- **Clases de firma electrónica.** Este documento se refiere a las clases de firma electrónica y a su validez jurídica siguiendo las definiciones establecidas en el Reglamento eIDAS, según el cual las firmas electrónicas se clasifican en firma simple, avanzada y cualificada.

- **Código Seguro de Verificación (CSV).** Código que se incluye en los documentos electrónicos que puedan ser impresos y que permite que un tercero pueda verificar su autenticidad e integridad. La persona interesada deberá comprobar dicho código a través del servicio habilitado a tal efecto (validador de documentos con CSV) en la sede electrónica de la Diputación.

- **Firma biométrica**. Firma electrónica avanzada realizada en tabletas gráficas específicas para firmar documentos generados presencialmente ante un tercero. En el proceso de firma, el dispositivo especializado capta las evidencias biométricas del firmante (presión del lápiz, velocidad de escritura y aceleración) y el contexto de la firma. La información obtenida se cifra con una clave púbica de un tercero de confianza y se almacena en el mismo documento firmado o en un repositorio de firmas.

- **Formato de firma electrónica.** La forma en la que se codifican las firmas electrónicas, siendo sus formatos más comunes S / MIME, CMS, XAdES, CAdES y PAdES.

- **Nivel de firma**. Indica si el documento tiene una única firma o múltiples firmas y, en este último caso, si estas se generan de forma paralela o secuencial.

- **Sellado de tiempo.** Acreditación de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos a cargo de un tercero de confianza.

- **Sistema de firma.** Forma de firma de un documento electrónico, sea mediante un certificado digital de la persona firmante, por medio de un sistema de identificación más evidencia electrónica del acto de firma, firma biométrica o mediante un Código Seguro de Verificación (CSV).

- **Tipo de firma.** Forma de relación de la firma electrónica con el documento firmado, dentro del mismo documento, pudiendo ser dentro del mismo documento, como un documento aparte o dentro de estructuras XML.

Los actores involucrados en el proceso de creación y validación de una firma electrónica son los siguientes:

- **Firmante.** Persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica.

- **Creador de un sello.** Persona jurídica que crea un sello electrónico.

- **Verificador.** Entidad, sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por la política por la que se rige la plataforma de relación electrónica, o el servicio concreto en el que se está invocando. Podrá

ser una entidad de validación de confianza o una tercera parte que esté interesada en la validez de una firma electrónica.

- **Prestador de servicios de firma electrónica.** Una persona física o jurídica, que expide certificados digitales cualificados o presta otros servicios relacionados con la firma electrónica cualificada.

Este documento usa el concepto "firmante" para referirse tanto a la persona que firma como al creador de un sello. En este último caso, se puede tratar de un proceso de actuación administrativa automatizada.

Conceptos de firma electrónica

Definición jurídica de la firma electrónica

Desde una perspectiva jurídica, las diferentes clases de firma se definen como:

- **Firma electrónica ordinaria.** Conjunto de datos en forma electrónica, consignados juntamente con otros o que están asociados, que pueden ser usados como medio de identificación de la persona firmante. Entendiendo identificación como autenticación por entidades.

- **Firma electrónica avanzada.** Conjunto de datos en forma electrónica que permiten identificar al firmante y detectar cualquier cambio posterior de los datos que se hayan firmado, vinculada al firmante de forma única y a los datos a los que hace referencia, creada por medios que el firmante puede mantener bajo su control exclusivo.

- **Firma electrónica cualificada.** Firma electrónica avanzada basada en un certificado reconocido y que ha sido generada mediante un dispositivo seguro de creación de firma.

El concepto de certificado reconocido al que se hace referencia en las definiciones del presente apartado se refiere a aquellos certificados digitales emitidos por un prestador de servicios de certificación cualificado, que cumplen con los requisitos establecidos en lo referente a la comprobación de la identidad y el resto de las circunstancias de los solicitantes y a la fiabilidad y garantías de los servicios de certificación que prestan.

Fundamentos técnicos de la firma electrónica

Desde un punto de vista técnico, los tipos de firma se definen como:

- **Firma *attached*:** los datos de la firma electrónica residen en el documento firmado. Por lo tanto, el mismo documento dispone de toda la información necesaria para comprobar la autenticidad e integridad de este, así como la información necesaria para validar la firma. Existen dos tipos diferentes de firma *attached*:
  - ***Enveloped* (incrustada):** el documento electrónico firmado posee el contenido y su firma.
  - ***Enveloping* (envolvente):** el documento electrónico es la firma electrónica del documento a firmar y, dentro de esta firma, se encuentra el mismo documento a firmar.
- **Firma *detached***: los datos de la firma electrónica se localizan fuera del documento a firmar, pero se encuentran asociados al mismo. Los datos de la firma se mantendrán por separado durante todo el ciclo de vida del documento. Para validar la firma, se deberá crear un documento de evidencias electrónicas que contenga conjuntamente el documento y los datos completos de la firma electrónica.

En relación con el nivel de firma electrónica, se puede distinguir entre:

- **Firma simple:** El documento contiene una única firma.

- **Firma múltiple:** El documento contiene dos o más firmas. La firma múltiple consiste en que varios firmantes firmen el documento de forma consecutiva. Este tipo de firma se puede aplicar sobre el documento original cada vez (firma paralela) o sobre el documento firmado (firma secuencial).

La firma múltiple se usará en diversas actuaciones en el marco de los procedimientos de la Diputación, como, por ejemplo, en la firma de documentos electrónicos por más de una persona o el resellado de documentos ya firmados para actualizar su validez legal a lo largo del tiempo, antes que la validez criptográfica de la firma electrónica pueda quedar en entredicho.

ANEXO III DE LA PIFE-DPCA

Normativa aplicable y estándares internacionales y otras convenciones

El cambio de paradigma que ha supuesto el uso del documento electrónico es el resultado de la aparición de cambios normativos que han impulsado las herramientas telemáticas y que, en determinadas circunstancias, han equiparado los documentos electrónicos a los documentos en formatos más tradicionales. Por otro lado, las organizaciones encargadas de la estandarización técnica han definido y documentado los criterios y formatos que se usarán para la gestión de los documentos digitales en todos sus aspectos, garantizando su validez jurídica.

El contenido del presente apartado contempla el marco normativo y los estándares internacionales y otras convenciones de referencia para la aplicación de la presente Política de Identidad y Firma Electrónicas de la Diputación Provincial de Cádiz.

Normativa de ámbito europeo

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Reglamento de Ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Reglamento (UE) 910/2014 del Parlamento Europeo y Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Normativa de ámbito estatal

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital, por la que se establecen las condiciones de uso de firma electrónica no criptográfica, en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos.
- Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones

Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.
- Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico, especialmente, en lo que se refiere al su proceso de foliado.
- Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

Normativa de ámbito autonómico

- Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.

Normativa propia de la Diputación Provincial de Cádiz

- Política de Gestión de Documentos Electrónicos de la Diputación Provincial de Cádiz (PGDE-DPCA), aprobado por Decreto de 5 de marzo de 2021 (SECRE-00018-2021) y publicada en el apartado de “Normativa” de la Sede electrónica de la Diputación Provincial de Cádiz.
- Reglamento Regulador de la Administración Electrónica en la Diputación Provincial de Cádiz, publicado en el Boletín Oficial de la Provincia de Cádiz núm. 118, de 24 de junio de 2019.
- Decreto de ampliación AAA – Sello electrónico de la Diputación Provincial de Cádiz, aprobado el 24 de abril de 2019 (Decreto SECRE-00029-2019) y publicado en el apartado de “Normativa” de la Sede electrónica de la Diputación Provincial de Cádiz.
- Decreto de aprobación de los sellos electrónicos de la Diputación Provincial de Cádiz, aprobado el 3 de julio de 2017 (Decreto SINFO-00024-2017) y publicado en el apartado de “Normativa” de la Sede electrónica de la Diputación Provincial de Cádiz.
- Ordenanza de transparencia, acceso a la información y reutilización de la información de la Diputación Provincial de Cádiz, publicada en el Boletín Oficial de la Provincia de Cádiz núm. 21, de 2 de febrero de 2016.

Estándares internacionales y otras convenciones

Para el desarrollo de la presente Política, se han contemplado los estándares internacionales y otras convenciones que definen los distintos formatos, tipos de firma y sello electrónico y el resto de las tecnologías, que se relacionan a continuación:

- ETSI RFC 2315 (1998), ETSE RFC 2630 (1999), IETF RFC 3369 (2002), IETF RFC 3852 (2004): PKCS # 7: Cryptographic Message Syntax (CMS).
- ETSI TS 101 733. v.1.6.3, v1.7.4 y v.1.8.1: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).
- ETSI TS 119 122-3: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures: Part 3: incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES.
- ETSI TR 119 124-1: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.
- ETSI TS 119 124-2: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of CAdES baseline signatures.
- ETSI TS 119 124-3: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended CAdES signatures.
- ETSI TS 119 124-4: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of CAdES baseline signatures.
- ETSI TS 119 124-5: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended CAdES signatures.
- ETSI TR 119 134-1 Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.
- ETSI TS 119 134-2: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of XAdES baseline signatures.
- ETSI TS 119 134-3: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended XAdES signatures.
- ETSI TS 119 134-4: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of XAdES baseline signatures.
- ETSI TS 119 134-5: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended XAdES signatures.
- ETSI TS 119 142-3: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS).
- ETSI TR 119 144-1 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.
- ETSI SR 019 020: The framework for standardization of signatures; Standards for AdES digital signatures in mobile and distributed environments.
- IETF RFC 5280 (2008): Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

- IETF RFC 2560 (1999): X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP.
- IETF RFC 3126 (2001): Electronic Signature Formats for Long Term Electronic Signatures.
- ISO 19005 (2008): Formato del fichero / A-1.
- ISO / TR 18492: 2005- Long-term preservation of electronic document-based Information.
- UNE - ISO / TR 13008: 2010 – Información y documentación. Conversión de documentos digitales y procesos de migración.
- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
- ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- ETSI TS 101.861 V1.3.1 Time stamping profile.
- ETSE TR 102.038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.
- ETSE TR 102.041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.
- ETSE TR 102.045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.
- ETSE TR 102.272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.
- IETF RFC 2560, X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP.
- IETF RFC 3125, Electronic Signature Policies.
- IETF RFC 3161 actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 5652, RFC 4853 y RFC 3852, Cryptographic Message Syntax (CMS).
- ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

La Presidenta