AGTIC

ASESORAMIENTO Y GESTIÓN EN TIC

Política de Firma y Sello electrónicos y de Certificados digitales de la Diputación de Almería

DIPUTACIÓN DE ALMERÍA

Mayo de 2020

Control de versiones

Versión	Fecha	Modificaciones introducidas
1	18/12/2017	Primera versión del documento de Política
2	05/01/2018	Segunda versión del documento elaborada por AGTIC a partir de los comentarios recibidos de la Comisión de Administración electrónica en la reunión celebrada el 20 de diciembre de 2017.
3	05/03/2020	Tercera versión del documento elaborada en el marco de la redacción del Modelo de Gestión del Documento y el Expediente electrónico.
4	05/05/2020	Nueva versión incorporando los comentarios realizados por el departamento de Informática.
5	19/05/2020	Versión definitiva tras incorporar los comentarios recibidos de Alicia Mozos y Pilar Giménez.
6	15/06/2020	Nueva versión incorporando comentarios de Alicia Mozos.

ÍNDICE

1. Introducción

La Diputación de Almería, en adelante la Diputación, en su estrategia de implantación del documento y expediente electrónico como elemento de base para evidenciar su actuación administrativa, requiere dotarse de una Política de Firma y Sello electrónicos y de certificados digitales tal y como establece la resolución de 27 de octubre de 2016, del Ministerio de Hacienda y Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de Certificados de la Administración.

Esta Política debe garantizar el correcto uso de las herramientas de firma electrónica, con el objetivo de que permitan generar documentos electrónicos con carácter de autenticidad. Para ello esta política se fundamenta en los siguientes principios:

- La vocación de la Diputación de que su actividad administrativa pueda plasmarse en documentos y expedientes electrónicos auténticos.
- Los documentos electrónicos firmados electrónicamente, en cumplimiento de lo establecido en esta política, tendrán plena validez y se considerarán originales.
- El nivel de seguridad tecnológica, el tipo de certificado a utilizar, el formato de la firma y del sellado de tiempo y los mecanismos de preservación se fijarán en función de la importancia del documento, del acto administrativo a que se refieran y de la tabla de valoración documental aplicable.
- Las firmas electrónicas que se generan en la Diputación se harán con el formato y nivel de seguridad requerido para su conservación durante todo el periodo de vida útil del documento al que hacen referencia.
- Los documentos electrónicos que se reciban firmados serán sometidos a un proceso de validación y compleción de las firmas en el momento de la recepción.

La presente Política desarrolla los siguientes elementos:

1. El **objeto** con el que se desarrolla la Política de firma y sello electrónicos y de certificados digitales de la Diputación de Almería.
2. Los **datos identificativos** de la Política, su periodo de validez y la asignación de responsabilidades para su gestión y aplicación.
3. La identificación de los **actores involucrados** en el proceso de creación y validación de una firma electrónica.
4. El **uso de certificados y otras identidades digitales**:
    - Certificados e identidades digitales admitidos: qué certificados digitales o identidades digitales (acreditadas a través de un registro previo) pueden utilizar otras personas o entidades para relacionarse telemáticamente con la Diputación.

- Certificados digitales empleados: qué certificados digitales pueden utilizar los empleados de la Diputación, en el ejercicio de sus funciones, y los sellos electrónicos previstos para la actuación automatizada.

5. El **ciclo de vida de los certificados digitales** empleados por la Diputación identificándose cómo pueden obtenerse los certificados cuando se necesiten y cómo se llevará el control de los certificados existentes y de su eventual revocación cuando dejen de ser necesarios.
6. Los **certificados digitales de empleado público y de representantes** de la Diputación de Almería y los sellos electrónicos utilizados por la Diputación en la ejecución de sus procedimientos.
7. El establecimiento del **sellado de tiempo** cómo elemento que permite dejar evidencia de la fecha y hora en que se ha producido un acto y facilita la preservación de la validez jurídica de las firmas electrónicas a lo largo del tiempo.
8. Los **sistemas, clases, tipos, niveles y formatos de firma electrónica** que se prevén en el ámbito de la Diputación.
9. El procedimiento de **validación de firmas electrónicas** que se prevé para los documentos que incorporen firma electrónica.
10. El **mantenimiento y la preservación de firmas electrónicas**, para garantizar la introducción en los sistemas de gestión documental de la Diputación de documentos auténticos que garanticen la preservación de su validez jurídica a largo plazo mediante procesos de resellado de tiempo.
11. Los **Códigos Seguros de Verificación (CSV)** como sistema de validación de la autenticidad de los documentos electrónicos.
12. La identificación de los **metadatos de firma** previstos en el Vocabulario de Metadatos de la Diputación de Almería para la gestión efectiva de firmas electrónicas.

Para la elaboración de esta Política se ha tenido en cuenta lo establecido el por el Real Decreto 4/2010 por el que se regula el Esquema Nacional de Interoperabilidad, así como los siguientes elementos de desarrollo:

- Resolución de 27 de octubre de 2016 (BOE de 3 de noviembre), 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.
- Resolución de 29 de noviembre de 2012 (BOE de 13 de diciembre), de la Secretaría de Estado de Administraciones Públicas, por la que se publica el acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente.

- Resolución de 19 de julio de 2011 (BOE de 30 de julio), 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 referente a su proceso de foliado.

Adicionalmente, la presente política toma como referencia para su desarrollo la normativa y estándares internacionales aplicables y que se identifican en el Anexo I.

Finalmente, la Política de Firma y Sello electrónicos y de certificados digitales de la Diputación de Almería nace con la vocación de servir de modelo a las Entidades Locales de la provincia de Almería para el desarrollo de su propia Política.

2. Objeto de la Política

Esta Política de Firma y Sello electrónicos y de certificados digitales tiene por objeto establecer el conjunto de criterios comunes asumidos por la Diputación de Almería con la autenticación y el reconocimiento de firmas electrónicas basadas tanto en certificados digitales como en evidencias electrónicas.

En concreto, establece las directrices a seguir por la Diputación de Almería respecto al uso de la firma electrónica, en el seno de las aplicaciones corporativas, para garantizar la autenticidad, integridad y conservación de los documentos firmados electrónicamente. Es de aplicación tanto a las firmas como a los sellos electrónicos.

Asimismo, el objetivo de esta Política es establecer qué identidades y certificados digitales son aceptados por la Diputación de Almería y qué certificados digitales utilizan sus empleados estableciéndose el ciclo de vida de los certificados digitales.

Por último, la Política establece las estrategias que la Diputación de Almería adopta para la preservación a largo plazo de las firmas electrónicas.

3. Datos de la Política de Firma y Sello electrónicos y certificados digitales

3.1 Identificación de la Política

Los datos identificativos de la Política de Firma y sello electrónicos y de certificados digitales de la Diputación de Almería son los siguientes:

Nombre del documento	Política de firma y sello electrónicos y de certificados digitales de la Diputación de Almería
Versión	3.0
Identificador del Gestor	Diputación Provincial de Almería con código DIR3 L02000004
URI de referencia	DIPALME_ L02000004_politica_firma_sello_electronicos_certificado_v1.0
URL de referencia	A informar cuando esté disponible el enlace web donde se publique la política.
Fecha de expedición	A informar cuando se publique
Ámbito de Aplicación	Gestión de los documentos y expedientes electrónicos producidos y custodiados por la Diputación de Almería, afectando a la totalidad de su personal en grado de dependencia directa, así como a colaboradores externos y proveedores de servicios mediante cualquier modalidad contractual.
Responsable de la Política y datos de contacto	Comisión de coordinación de proyectos para la implantación y mejora de la administración electrónica en la Diputación de Almería. Email: comiteadministracionelectronica@dipalme.org Tel. 950211100

3.2 Entrada en vigor de la Política

La presente Política de firma y sello electrónicos y de certificados digitales entrará en vigor en la fecha de su expedición y será válida hasta que no sea sustituida o derogada por una Política posterior, pudiéndose facilitar un periodo de tiempo transitorio, en el cual convivan las dos versiones, que permita adecuar los diferentes sistemas de firma electrónica y validación utilizados por la Diputación de Almería a las especificaciones de la nueva versión.

Este período de tiempo de transición se deberá indicar en la nueva versión y superado el mismo sólo será válida la versión actualizada.

3.3 Período de transición

La Política de firma y sello electrónicos y certificados digitales que es sustituida por la presente Política tendrá efectos y será válida durante el período establecido en el acuerdo de resolución de la Presidencia de la Diputación de Almería.

3.4 Gestión de la Política de firma y sello electrónicos y de certificados digitales

El mantenimiento, actualización y publicación electrónica de la presente Política corresponderá a la Comisión de coordinación de proyectos para la implantación y mejora de la administración electrónica. Los cambios a la Política serán consensuados con las partes implicadas, así como el periodo de tiempo transitorio para la adaptación de las plataformas a la nueva Política.

Dicha Comisión será responsable de garantizar que en la Sede electrónica de la Diputación de Almería figure tanto la versión actualizada de la Política como el acceso a un repositorio con el historial de las versiones anteriores de la Política de manera que un validador puede encontrar las versiones anteriores para verificar una firma electrónica anterior a la política vigente en el momento de validación.

En el momento de la firma se deberá incluir la referencia del Identificador de la Política (URI) sobre el que se ha basado su implementación, el cual determinará las condiciones que debe cumplir la firma electrónica en un momento determinado. El campo destinado para incluir esta referencia será, sólo para el formato AdES_EPES, la etiqueta *SignaturePolicyIdentifier*,

4. Actores involucrados

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

a) **Firmante:** Una persona física que crea una firma electrónica utilizando datos de creación de firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

b) **Persona jurídica que realiza firma con sello electrónico:** Una persona jurídica que crea una firma electrónica con un sello electrónico mediante un proceso automatizado.

c) **Verificador:** Entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica. Podrá ser una entidad de validación de confianza o una tercera parte que esté interesada en la validez de una firma electrónica.

d) **Prestador de servicios de firma electrónica:** Una persona física o jurídica que expide certificados digitales o presta otros servicios en relación con la firma electrónica.

e) **Emisor y gestor de la política de firma:** Entidad que se encarga de generar y gestionar el documento de política de firma y sello.

En este documento se utilizará el término “firmante”, tanto para referirse al firmante como a la persona jurídica que crea una firma electrónica con un sello electrónico. En el segundo de los casos puede estar sometido a un proceso de actuación administrativa automatizada regulada en la normativa propia de la Diputación.

5. Certificados digitales y otras identidades digitales

5.1 Certificados digitales utilizados por la Diputación de Almería

Podrán utilizar certificados digitales los empleados de la Diputación de Almería que deban firmar documentos electrónicamente o tener acceso a determinados servicios o aplicaciones que requieran autenticación mediante certificados digitales. Los certificados utilizados serán de empleado público lo cual vinculará al titular del certificado con la Diputación de Almería.

Adicionalmente, la Diputación de Almería utilizará:

- Certificados de representante de la Diputación de Almería.
- Certificados de sello electrónico para la actuación administrativa automatizada.
- Certificados de pseudónimo en determinadas circunstancias cuando resulte necesario proteger la identidad personal del firmante y sólo resulta relevante su cargo profesional.
- Certificados de sitio web y sede electrónica para garantizar la no suplantación de identidad de sitios web y sede electrónica titularidad de la Diputación de Almería.

La Diputación de Almería utiliza los certificados digitales emitidos por un prestador reconocido o cualificado de servicios de certificación del cual la Diputación de Almería se constituye como Oficina de Registro para la emisión de certificados digitales de empleado público de la Diputación.

5.2 Certificados admitidos por la Diputación de Almería

El mecanismo de firma o 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 estado correctamente emitido y que continúa siendo vigente en el momento de su uso, es decir de la firma o sellado de un documento. 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 digitales serán aceptados sólo en la medida en que la entidad que lo ha de validar confíe en la honestidad de la Autoridad de Certificación.

La Diputación de Almería debe admitir, a partir de la entrada en vigor de la Ley 15/2014, de 16 de septiembre, de racionalización del Sector Público y otras medidas de reforma administrativa, en la cual en su artículo 24 establece que *"Las Administraciones Públicas deberán admitir todos los certificados reconocidos incluidos en la «Lista de confianza de prestadores de servicios de certificación» (TSL) establecidos en España, publicada en la sede electrónica del Ministerio de Industria, Energía y Turismo"*, todos los certificados digitales emitidos por los prestadores de servicios de certificación que hayan realizado la comunicación

prevista en el artículo 30.2 de la Ley 59/2003 en el Ministerio de Industria, Energía y Turismo y que cumplan con los estándares de calidad y niveles de seguridad establecidos por dicho Ministerio.

La Diputación de Almería utiliza la plataforma @firma del Ministerio de Hacienda y Administraciones Públicas tanto para la validación de sus certificados digitales como para certificados de terceros, por lo que la aceptación efectiva de certificados digitales vendrá condicionada por la actualización de los servicios de dicha plataforma.

A través de la plataforma @firma se podrán admitir los certificados reconocidos incluidos en la "Lista de confianza de prestadores de servicios de certificación" (TSL) establecidos en España, publicada en la sede electrónica del Ministerio de Industria, Energía y Turismo.

5.3 Otras identidades digitales admitidas por la Diputación de Almería

En virtud del artículo 9.2 de la Ley 39/2015, la Diputación admite, además de certificados digitales, cualquier otro mecanismo de identificación y firma que sea aceptado por el sistema Cl@ve que está orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos.

En particular, la Diputación utilizará el sistema de firma electrónica basada en evidencias de la voluntad de firma.

6. Ciclo de vida de los certificados digitales utilizados por la Diputación de Almería

Tal y como se ha indicado en el apartado anterior, la Diputación de Almería utiliza los certificados digitales emitidos por un prestador reconocido o cualificado de servicios de certificación de la que se ha constituido como Oficina de Registro para la emisión de certificados digitales de empleado público de la Diputación.

Corresponde a este prestador de servicios de certificación la responsabilidad de definir las políticas de gestión de los certificados digitales que emite y, por tanto, es quien define la vigencia de los certificados, la manera como se emiten, revocan y renuevan y las correspondientes normativas de uso.

Al efecto de adoptar los procedimientos establecidos por el prestador de servicios de certificación para operar la Oficina de Registro de la Diputación, se han establecido procedimientos internos en la Diputación que identifican las actividades que se realizan y sus responsables, así como los procedimientos a seguir por los usuarios para la solicitud, renovación, revocación, etc. de sus certificados digitales. Todo ello sujeto estrictamente a las directrices que el prestador de servicios de certificación establece al efecto.

Adicionalmente, corresponde al prestador de servicios de certificación proveer el acceso a un inventario de certificados emitidos en el seno de la Diputación que permite disponer de información actualizada sobre el número de certificados digitales emitidos, el tipo de certificado, su estado y la fecha de caducidad, entre otros datos

6.1 Certificados digitales de empleado público

La emisión de los certificados digitales se realiza en función de las necesidades del puesto de trabajo y se revocan en el momento de la desvinculación del personal de la Diputación o bien por incidencias en el certificado.

Corresponde a la Diputación de Almería, como Oficina de Registro del prestador de servicios de certificación que emite los certificados, la verificación de la identidad de la persona para la que se emite el certificado digital y su vinculación con la Diputación siempre de acuerdo con las instrucciones de la Autoridad de Certificación siendo esta última quien finalmente emite el certificado digital.

En el momento de la entrega del certificado a su titular éste es informado de la normativa de uso y del procedimiento que debe seguir en caso de que tenga una incidencia, como puede ser la pérdida del certificado.

De forma automática, en el momento en que un certificado digital de empleado público esté a punto de caducar, el prestador de servicios de confianza informará al titular de dicho certificado sobre este hecho para que pueda iniciar el trámite de renovación del certificado digital siguiendo los mismos procedimientos establecidos para la solicitud de un nuevo

certificado digital. Con carácter previo se evaluará de nuevo la vinculación de la persona con la Diputación.

6.2 Certificados digitales de representante

Los certificados digitales de representante de la Diputación son asignados a los empleados públicos que los requieren para el desempeño de sus funciones mediante la correspondiente autorización limitando mediante resolución de la presidencia de la Diputación los usos que podrá realizar con el certificado. Adicionalmente, son revocados en el momento en que la persona deja de tener otorgada la capacidad de representar a la Diputación.

Corresponde a la Diputación de Almería, como Oficina de Registro del prestador de servicios de certificación que emite los certificados, la verificación de la identidad de la persona para la que se emite el certificado digital y su capacidad de representación de la Diputación siempre de acuerdo con las instrucciones del prestador de servicios de confianza siendo éste quien finalmente emita el certificado digital.

En el momento de la entrega del certificado a su titular éste es informado de la normativa de uso y custodia y del procedimiento que debe seguir en caso de que tenga una incidencia, como puede ser la pérdida del certificado.

De forma automática, en el momento en que un certificado digital de representante esté a punto de caducar, el prestador de servicios de confianza informará al responsable de dicho certificado sobre este hecho para que pueda iniciar el trámite de renovación del certificado digital siguiendo los mismos procedimientos establecidos para la solicitud de un nuevo certificado digital. Con carácter previo se valorará si dicha persona sigue teniendo la capacidad de representación de la Diputación.

6.3 Certificados de sello electrónico para la actuación administrativa automatizada

Para las actuaciones administrativas automatizadas la Diputación de Almería dispondrá de certificados de sello electrónico. Por Resolución del Presidente se podrán crear sellos electrónicos de órganos de la Diputación para las actuaciones administrativas automatizadas en el ámbito de sus competencias o para superponer a documentos firmados, a fin de garantizar la interoperabilidad y asegurar la integridad, inalterabilidad y el no repudio de los mismos.

Para la generación de este tipo de certificados, la Diputación ha establecido los procedimientos internos necesarios para que, dada una necesidad concreta, se proceda a autorizar su adquisición la cual se trasladará al prestador de servicios de confianza de acuerdo con los procedimientos y requerimientos que éste tenga establecidos al efecto.

Los sellos electrónicos podrían ser distintos para cada actuación administrativa automatizada de la Diputación y serán instalados y custodiados de forma segura de manera que se garantice

que sólo puedan ser utilizados por actuaciones administrativas automatizadas autorizadas para cada sello.

La Diputación de Almería, en el ejercicio de sus competencias, podrá utilizar este tipo de certificados para su identificación y autenticación en los siguientes tipos de actuaciones administrativas automatizadas:

- Intercambio de información con otras Administraciones Públicas, corporaciones, entidades e instituciones públicas.
- Procesos de sellado de documentos electrónicos, al objeto de facilitar su interoperabilidad, conservación y legibilidad.
- Comunicaciones electrónicas con personas físicas y jurídicas.
- Generación y emisión de certificados y documentos administrativos electrónicos.
- Generación y emisión de copias electrónicas auténticas a partir de documentos electrónicos y de documentos en soporte no electrónicos.
- Inscripciones, anotaciones registrales y archivo de documentos electrónicos registrales.
- Generación y emisión de acuses de recibo, incluyendo los generados por el registro electrónico.
- Cambios de formato de documentos electrónicos y posibles refirmas o resellado de documentos.
- Firma de boletines o diarios oficiales.

Cada actuación administrativa automatizada llevada a cabo por la Diputación de Almería será aprobada formalmente de acuerdo con lo establecido en el Reglamento de Actuación Administrativa Automatizada determinándose el sello electrónico utilizado en cada actuación.

Cada sello electrónico dispondrá de una persona en la Diputación responsable de su custodia, revocación o renovación de acuerdo con los procedimientos indicados por la Autoridad de Certificación emisora del certificado de sello electrónico.

El uso de los sellos electrónicos estará sometido a un control periódico por parte de cada uno de sus responsables para garantizar que son utilizados para las finalidades para las que fueron creados. Igualmente, el responsable del sello electrónico será el responsable de solicitar la revocación del certificado en caso de dejar de ser necesario.

6.4 Certificados digitales para la identificación de sitios web

Los dominios web de la Diputación de Almería se identifican mediante un certificado digital cualificado de sitio web, expedido por un prestador de servicios de confianza y que es distinto para cada sitio web titularidad de la Diputación.

En concreto, la sede electrónica de la Diputación de Almería se identifica mediante un certificado digital de sitio web que responderá a la URL https://sede.dipalme.org.

La gestión de estos certificados se llevará a cabo del mismo modo que se ha indicado en el caso de certificados de sello electrónico.

7. Sellado de tiempo

Todos los documentos firmados electrónicamente por parte de la Diputación de Almería incluyen sello de tiempo evidenciando así la fecha y la hora en la que han sido firmados, así como que no han sido modificados desde ese momento.

La Diputación utilizará el sellado de tiempo que provea la plataforma @firma.

8. Sistemas, clases, tipos, niveles y formatos de firma electrónica

8.1 Sistemas de firma electrónica

Los objetivos que persigue la Diputación de Almería con la implantación de la firma electrónica son fundamentalmente tres:

- Dotar a la Diputación de Almería de un sistema para el control, el uso y la conservación de la documentación original firmada electrónicamente, gestionada en el desarrollo habitual de su actividad política y administrativa.
- Garantizar la gestión adecuada de los documentos de la Diputación de Almería, asegurando la autenticidad, la fiabilidad, la integridad y la disponibilidad futura a lo largo de su ciclo de vida, basado en un software informático que ofrece una capa de gestión de documentos y archivo común.
- Dar respuesta a las exigencias en materia de archivo electrónico de la Ley 39/2015 y del Esquema Nacional de Interoperabilidad.

Para ello la Diputación podrá usar distintos **sistemas de firma electrónica**:

- Firma electrónica basada en el uso de un certificado digital.
- Firma electrónica basada en la identificación más las evidencias de la voluntad de la firma y cualquier otro mecanismo de firma electrónica proporcionada por el sistema Cl@ve.

La Diputación se ajustará a las condiciones de uso de los mecanismos de firma electrónica proporcionada por el sistema Cl@ve custodiando debidamente las evidencias que éste devuelva de los procesos de firma electrónica realizados con este sistema.

Es por ello que, a continuación, sólo se procede a establecer las clases, tipos, niveles y formatos de firma electrónica utilizados por la Diputación de Almería.

8.2 Clases de firma electrónica

Por lo que respecta a las **clases de firma electrónica** desde un punto de vista jurídico la Diputación utilizará las siguientes:

- **Simple u Ordinaria**: es el conjunto de datos en forma electrónica, consignados juntamente con otros o que están asociados, que pueden ser utilizados como medio de identificación del firmante.
- **Firma electrónica avanzada**: es la firma electrónica que permite identificar al firmante y detectar cualquier cambio posterior de los datos firmados, que está vinculada al

firmante de manera única y a los datos a los que hace referencia y que ha estado creada por medios que el firmante puede mantener bajo su control exclusivo.

- **Firma electrónica reconocida o cualificada**: es la firma electrónica avanzada que se basa en un certificado reconocido o cualificado y que ha estado generada mediante un dispositivo seguro de creación de firma, según lo establecido en la normativa aplicable a la firma electrónica (ver Anexo I).

En cualquier caso, se utilizarán certificados digitales reconocidos o cualificados emitidos por un prestador de servicios de certificación, que cumplen con los requisitos establecidos en la normativa aplicable a firma electrónica (ver Anexo I) en cuanto a la comprobación de la identidad y el resto de circunstancias de los solicitantes, y la fiabilidad y las garantías de los servicios de certificación que presten.

8.3 Tipos de firma electrónica

A continuación, se muestran las diferentes definiciones de **tipos de firma electrónica** desde un punto de vista técnico:

- **Firma attached:** los datos de la firma residen en el documento firmado. Por lo tanto, el mismo documento dispone de toda la información para comprobar la autenticidad e integridad del documento, así como la información necesaria para la validación de la firma. Hay que diferenciar entre dos tipos diferentes de firma attached:
  - **Enveloped (incrustada).** El documento firmado está compuesto por el contenido del documento a firmar más la firma de este contenido.
  - **Enveloping (envolvente).** El documento firmado es la firma electrónica del documento a firmar y dentro de esta firma está el propio documento a firmar.

  Este es el tipo de firma electrónica que se usará de forma preferente siempre que el formato del documento a ser firmado lo permita.
- **Firma detached:** los datos de firma residen fuera del documento a firmar, pero están asociados a éste. Los datos de la firma se mantienen por separado durante todo el ciclo de vida del documento. Para validar la firma hay que crear un documento de evidencia electrónica que contenga de forma conjunta el documento y sus datos completos de la firma.

8.4 Niveles de firma electrónica

Por lo que respecta a **niveles de firmas electrónicas** la Diputación prevé el uso de los siguientes:

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

- **Firma múltiple:** el documento contiene dos o más firmas. Esta firma múltiple consiste en que varios firmantes firmen el documento consecutivamente. Esta firma se puede aplicar sobre el documento original cada vez, lo que se identifica como firma paralela, o sobre el documento firmado, que se identifica como firma anidada.

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

8.5 Formatos de firma electrónica

La Diputación de Almería empleará los formatos admitidos en la Política de Firma y Sello electrónicos y de Certificados de la Administración General del Estado.

Dentro de las distintas clases de los formatos XAdES, CAdES y PAdES, deberá adecuar sus sistemas de información para la generación de, al menos, la clase básica de uno de esos formatos de firma electrónica, añadiendo información sobre la Política (clase EPES) y un sellado de tiempo, y la verificación de las especificaciones de la clase básica de los siguientes formatos:

- XAdES internally detached signature
- XAdES envoloped signature
- CAdES detache/expicit signature
- CAdES attached/implicit signature
- PAdES

En este sentido, las distintas clases, tipos y niveles de firma electrónica se utilizarán de forma combinada según las necesidades de Diputación en cada caso mediante los siguientes **formatos de firma electrónica**:

- **Firma electrónica con política de firma y con sello de tiempo:** se identificará como AdES-T y se utilizará en los documentos electrónicos y foliado de expedientes que se tengan que guardar menos que el tiempo de caducidad del certificado digital utilizado para generar el sello de tiempo asociado a la firma electrónica. En el caso de múltiples firmas, se tendrá en cuenta la primera fecha de caducidad del sello de tiempo dentro de las distintas firmas en caso de realizarse en paralelo o la fecha de caducidad del sello de tiempo de la última firma en caso de anidadas.
  - Para documentos PDF o PDF/A se usará la firma PAdES con sello de tiempo.

- Para documentos XML (facturas electrónicas, índice del expediente (resultante del proceso de foliado) u otros documentos recibidos vía interoperabilidad) se usarán firmas XAdES-T preferiblemente attached enveloping.
- Para el resto de los documentos se usarán firmas XAdES-T dettached.
- Adicionalmente será posible utilizar el formato de firma electrónica CAdES-T attached o dettached según corresponda al formato del documento.

- **Firma electrónica de archivo:** se identificará como AdES-A y se utilizará para los documentos electrónicos y foliado de expedientes que se tengan que guardar más del tiempo de caducidad del certificado digital utilizado para generar el sello de tiempo asociado a la firma electrónica. En el caso de múltiples firmas, se tendrá en cuenta la primera fecha de caducidad del sello de tiempo dentro de las distintas firmas en caso de realizarse en paralelo o la fecha de caducidad del sello de tiempo de la última firma en caso de anidadas.
  - Para documentos PDF o PDF/A se usará la firma PAdES-LTV.
  - Para documentos XML se usarán firmas XAdES-A preferiblemente attached enveloping.
  - Para el resto de los documentos se usarán firmas XAdES-A dettached.
  - Adicionalmente será posible utilizar el formato de firma electrónica CAdES-A attached o dettached según corresponda al formato del documento.

9. Validación de firmas electrónicas

Para garantizar la validez jurídica de los documentos electrónicos firmados electrónicamente, cualquier documento que entra o se genera en la Diputación de Almería y que contiene una firma o sello electrónico y/o un sello de tiempo, previamente a su almacenaje en el gestor documental, es necesario validarlo.

Para ello se utilizará los servicios de la Aplicación de VALIdación de firma y certificados Online y Demostrador de servicios de @firma denominada VALIDe, en caso de realizarse manualmente, y la plataforma @firma, en caso de realizarse de forma automatizada. Se usará de forma preferente la validación automática mediante los servicios de la plataforma @firma.

En los casos de las firmas electrónicas validadas con @firma, sólo en aquellos casos en los que el proceso de validación de todas las firmas electrónicas y de los sellos electrónicos es satisfactorio, se procede a almacenar el documento electrónico en el gestor documental siempre que sea posible completando la firma electrónica con las evidencias resultantes de la validación y un sello de tiempo del momento en que se realiza la validación. Este proceso se realizará sólo con carácter previo a la incorporación de un documento en los sistemas de la Diputación.

Para las firmas a través de acreditación de la identidad y de evidencias de la voluntad de firma u otras firmas generadas con los mecanismos facilitados por la plataforma Cl@ve, se procede a almacenar el documento electrónico con sus firmas electrónicas en el sistema de gestión documental directamente, sin ninguna validación adicional, ya que los sistemas de firma de este tipo ya son seguros y no existe un proceso automatizado de validación.

Sólo en el caso de que sea necesaria la preservación de la validez jurídica del documento más allá del tiempo de vida del certificado digital utilizado para generar cualquier firma asociada, o del sello de tiempo asociado a la firma electrónica, se procede a completar la firma o las firmas electrónicas si estas no son firma de archivo, es decir -A o -LTV.

10. Mantenimiento y preservación de las firmas y sellos electrónicos

La firma o sello electrónico otorga validez jurídica a los documentos electrónicos. No obstante, esta validez está sujeta a ciertos riesgos que deben gestionarse debidamente para garantizar una validez jurídica durante el tiempo que sea requerido. Estos riesgos son los siguientes:

1. Caducidad del certificado digital con el que se firma un documento electrónico.
2. Validez del certificado digital en el momento de generarse la firma electrónica.
3. Obsolescencia tecnológica de la longitud de las claves criptográficas contenidas en el certificado digital con el que se generan las firmas electrónicas.

Para superar estos riesgos la Diputación aplicará la estrategia de resellado de tiempo de las firmas electrónicas. El proceso de resellado consiste en añadir un nuevo sello de fecha y hora a la firma electrónica.

Para poder aplicar dicho proceso es necesario que las firmas estén en un formato que permita añadir dichas evidencias de tiempo. Estas son las firmas del tipo XAdES-A, CAdES-A o PAdES-LTV. En caso de que una firma no esté en uno de estos formatos, debe completarse la firma previamente al resellado que, en cualquier caso, estará como mínimo en un formato AdES-T, a uno de los formatos anteriormente definidos.

Este es un proceso que se llevará a cabo:

- En el momento en que esté a punto de caducar el último sello de tiempo aplicado a la firma electrónica a preservar.
- Excepcionalmente, cuando se detecte una posible obsolescencia tecnológica de los algoritmos o de las claves utilizadas para firmar el documento.

11. Código Seguro de Verificación

La Diputación de Almería utiliza el Código Seguro de Verificación (en adelante CSV) como un mecanismo a través del cual se puede comprobar la integridad, no la autoría, de una copia auténtica de un documento permitiendo la localización y consulta de este y verificación de su integridad.

El Código Seguro de Verificación consiste en una secuencia de letras y números generada de manera pseudoaletoria y asociada unívocamente al documento al que pertenece.

Para el acceso a documentos con CSV, los interesados se dirigirán a la Sede Electrónica de la Diputación de Almería mediante el enlace https://ov.dipalme.org/csv. Tras introducir el CSV se podrá acceder al documento sólo si este existe o sigue vigente la posibilidad de su consulta.

12. Metadatos de firma

Los Metadatos de firma que utilizará la Diputación de Almería pueden consultarse de forma actualizada en el Vocabulario de Metadatos publicado en la Sede electrónica de la Diputación de Almería. Este vocabulario se somete a lo establecido por el Esquema de Metadatos de Gestión del Documento Electrónico o eEMGDE.

Los metadatos de firma electrónica se recogen bajo la codificación eEMGDE17.

Anexo I: Normativa aplicable y estándares internacionales

La reciente revolución en el uso del documento electrónico es el resultado de la aparición de cambios normativos que han dado impulso a las herramientas telemáticas y han equiparado, en determinadas circunstancias, los documentos en formato electrónico a los documentos en formatos más tradicionales.

Además, tanto a nivel nacional como en la Unión Europea o internacionalmente, las organizaciones de estandarización técnica han definido y documentado los criterios y formatos que se utilizarán para la gestión de los documentos digitales en todos sus aspectos, garantizando su validez jurídica.

En este Anexo se identifican el conjunto de normativas y estándares internacionales que se han tenido en cuenta para la definición de la Política de firma y sello electrónicos y de certificados digitales de la Diputación de Almería.

Normativa aplicable

- Ley 39/2015, 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 15/2014, de 16 de septiembre, de racionalización del Sector Público y otras medidas de reforma administrativa.
- Ley 25/2015, de 28 de julio, de mecanismo de segunda oportunidad, reducción de la carga financiera y otras medidas de orden social.
- Ley 59/2003 de 19 de diciembre de Firma Electrónica.
- Real Decreto 3/2010 de 8 de enero del Esquema Nacional de Seguridad.
- Real Decreto 4/2010 de 8 de enero del Esquema Nacional de Interoperabilidad.
- Resolución de 19 de julio de 2011 de la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.
- Resolución de 19 de julio de 2011 de la Norma Técnica de Interoperabilidad de Expediente Electrónico.
- 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.
- 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 en conformidad con los artículos 27, apartado 5 y 37 apartado 5 del anterior Reglamento.

Estándares internacionales y otras convenciones

- ETSI RFC 2315 (1998), ETSI 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 de fichero PDF/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: Resumen criptográfico 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.
- ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.
- ETSI TR 102 041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.

- ETSI TR 102 045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.
- ETSI 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".