GIJÓN_IN: ciudad inteligente, innovadora e integradora

Título

POLITICA DE IDENTIFICACIÓN Y FIRMA MUNICIPAL

Política de identificación y firma, de sellos electrónicos, de certificados y de otros sistemas de identificación y firma de la Administración Municipal de Gijón

Autor

Servicio de Planificación y Modernización

Dirección General de Innovación y Promoción de Gijón

Identificación de documento	
Versión	**1**
N.º de revisión	
Estado	**Original**
Fecha	**Junio-2020**

Extracto: El presente documento tiene por objeto fijar los criterios comunes que la Administración Municipal de Gijón establece en relación con la identificación y firma electrónica.

De forma concreta, en esta Política se establecen las directrices referidas al uso de identificación y firma electrónica:

- En clave interna en lo referido al uso de las soluciones de gestión, con la intención de garantizar la integridad, autenticidad y validez jurídica de los documentos sobre los que se realice y aplique una firma electrónica, así como los sistemas de identificación que utiliza el personal municipal, los miembros de la corporación, los órganos que lo componen, las empresas adjudicatarias de los contratos y demás entidades colaboradoras. También, en lo referente al personal municipal, se establece el proceso de provisión de los certificados y gestión del ciclo de vida de los mismos.

- En clave externa, respecto a los certificados y sellos digitales utilizados por la ciudadanía, así como otros sistemas de identificación y firma electrónica que permitan el establecimiento tanto de identidades digitales como la acreditación de la autenticidad de la voluntad que puedan emplearse en el ejercicio de sus derechos.

Esta Política también contempla la preservación de los documentos firmados para garantizar su perdurabilidad y validez jurídica a largo plazo.

Índice

1. Introducción

La entrada en vigor de las Leyes 39/2015 y 40/2015 el 2 de Octubre de 2016, ha definido un nuevo escenario en las relaciones *ad intra* y *ad extra* de las Administraciones Públicas, suponiendo un cambio de paradigma, en el que el salto del papel al ámbito digital implica una importante transformación en la manera de hacer de la administración.

El Ayuntamiento de Gijón, consciente del entorno normativo y del marco de transformación digital que rodea todo ello, lleva desde el año 2009 aplicando firma electrónica en el ámbito de la gestión municipal para la firma de documentos electrónicos administrativos, garantizando la máxima seguridad jurídica, la autenticidad, la integridad y el no repudio.

Para ello, se ha constituido como autoridad delegada de un prestador de servicios de certificación, y tiene emitidos unos 500 certificados para el personal municipal, personal directivo y miembros de la corporación, así como cerca de 15 sellos de órgano para su aplicación en la actuación administrativa automatizada.

De la misma forma, ha dotado a la ciudadanía de un sistema de identificación, la Tarjeta Ciudadana, desde el año 2003. Se utiliza como sistema de identificación ante este Ayuntamiento, y, dotado a través de la *Ordenanza Municipal de Administración Electrónica* (aprobada por el Ayuntamiento Pleno de 12 de febrero de 2010).

El actual ordenamiento jurídico en materia de administración electrónica señala que la aceptación de los sistemas de identificación por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas la identificación electrónica de los interesados en el procedimiento administrativo. Por este motivo, se ha creado el sistema Cl@ve por Orden PRE/1838/2014, de 8 de octubre, (BOE del 9) se publicó el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas. Este sistema es de uso generalizado por las Administraciones Públicas y a partir de Septiembre de 2018 comienza la obligación de reconocimiento mutuo de identidades electrónicas transfronterizas notificadas a la Comisión Europea, por lo que todos los servicios públicos deben poder ofrecer la posibilidad de identificación con medios de identidad electrónicos de otros países.

Por este motivo en esta política de identificación y firma se establece como medio preferente de identificación el sistema Cl@ve. Para ello, las oficinas de asistencia en materia de registro facilitarán a las personas interesadas este sistema permitiendo con ello las relaciones electrónicas con y entre otras administraciones públicas.

Dentro del marco general descrito previamente, cabe destacar 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 (ENI) y, en concreto, dentro de las Normas Técnicas de desarrollo de dicho Esquema, tal como establece la *Resolución de 27 de octubre de 2016* («BOE» núm. 266, de 3 de noviembre 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*, considerando que es necesario dotarse de una política propia que defina el conjunto de criterios comunes asumidos con los cuales operar, para respaldar el correcto uso de la identidad digital y de la firma electrónica que permita la generación con carácter auténtico de documentos electrónicos, expedientes electrónicos y foliados de expedientes electrónicos.

Esta política de firma se fundamenta en los siguientes criterios:

- La actividad administrativa de la Administración Municipal de Gijón se plasma en documentos y expedientes electrónicos auténticos, a fin de dar cumplimiento a la Ley 39/2015 y se aplica tanto al Ayuntamiento de Gijón como al resto de organismos, empresas municipales y otras entidades que estén sometidas a derecho público.
- Los documentos electrónicos firmados electrónicamente en el ámbito de la Administración Municipal de Gijón, en cumplimiento de esta Política, tendrán plena validez y se considerarán documentos electrónicos administrativos de acuerdo con lo dispuesto en el art. 26 de la Ley 39/2015, o bien cuando se realicen copias por parte de la Administración Municipal, como en el caso de la digitalización certificada, de acuerdo al art. 27 de la Ley 39/2015 y demás normativa de desarrollo.
- El nivel de seguridad tecnológica, el tipo de certificado a utilizar, el formato de la firma y del sellado y los mecanismos de preservación, serán fijados de acuerdo con el documento y el acto administrativo al que se refieren.
- Las firmas electrónicas que se generen en la Administración Municipal de Gijón se efectuarán, en origen, con el formato y nivel de seguridad requerida para su conservación durante todo el periodo de vida útil del documento al que se refieren, incluido su posterior archivado electrónico, salvo las excepciones previstas en el apartado 8.1. Del mismo modo, los documentos electrónicos que se reciban firmados se someterán a un proceso de validación de las firmas en el momento de la recepción. En aquellos casos en los que la validación de la firma no sea correcta se aplicará el procedimiento que se apruebe al efecto.

Por tanto, en esta Política se viene a establecer:

1. La finalidad con la que se desarrolla la política de identificación y firma, de los sellos electrónicos, de los certificados y de los demás sistemas de identificación y firma electrónica municipales.

2. Los datos generales de la Política, sus periodos de validez y su transición a nuevas políticas y la asignación de responsabilidades para su gestión.

3. La definición de los conceptos clave en materia de identificación y firma electrónica y que se desarrollan a lo largo de la Política.

4. El uso de certificados digitales:

   - Los certificados digitales e identidades digitales admitidos: qué certificados digitales o identidades digitales (acreditadas a través de un registro previo o el intercambio de información conocida entre ambas partes) pueden utilizar otras personas o entidades para relacionarse electrónicamente con la administración municipal.

   - Los certificados digitales e identidades digitales a utilizar por la Administración Municipal: qué certificados y otras identidades digitales pueden utilizar el personal municipal en el ejercicio de sus funciones y los sellos electrónicos previstos para la actuación administrativa automatizada.

5. El ciclo de vida de los certificados y sellos utilizados por la administración municipal, identificando el procedimiento de solicitud, de renovación, de revocación y de suspensión de los mismos.

6. Las clases, tipos y niveles de firma, es decir, cómo y en qué formato se generan las firmas electrónicas utilizadas en el ámbito municipal y el proceso seguido para su validación. También debe señalarse que se prevén en esta Política las firmas electrónicas basadas en identidades digitales y evidencias electrónicas asociadas a la voluntad de la firma, tal como se recoge en el capítulo segundo de la Ley 39/2015, del procedimiento administrativo común de las Administraciones públicas, incorporando un nivel de identificación y/o firma específico para aquellos colectivos de personas que puedan tener dificultades de acceso a los servicios electrónicos, ponderando previamente las circunstancias concretas.

7. La definición del sello de tiempo como elemento facilitador de la preservación de las firmas electrónicas realizadas, y como evidencia de la fecha y hora en que se ha producido un acto.

8. El mantenimiento y la preservación de firmas electrónicas para garantizar la introducción en los sistemas de gestión documental de la Administración Municipal de documentos auténticos que garanticen la preservación de su validez jurídica a largo plazo.

9. Los criterios de firma electrónica aplicados en un contexto particular que tienen por objetivo determinar la validez de una firma electrónica en una transacción particular identificando qué obligaciones asume la Administración Municipal de Gijón, teniendo en cuenta el uso que se tiene que dar a los objetos firmados electrónicamente, documentos o expedientes electrónicos, y el tipo de actuación administrativa que recoge el acto de firma.

10. La identificación de un subconjunto representativo de casos de uso de la firma electrónica que identifican posibles escenarios en los que los procedimientos municipales pueden requerir el uso de firmas electrónicas vinculado a una normativa de firma electrónica concreta:

    - La firma electrónica de documentos electrónicos dentro de la plataforma de gestión integrada, a través del portafirmas corporativo.
    - La digitalización de documentos en papel.
    - Los procesos de firma mediante la aplicación de la figura de Actuación Administrativa Automatizada.
    - La incorporación de documentación firmada por terceros.
    - La presentación de solicitudes y de todo tipo de documentación sometida a derecho público a través del Registro Electrónico y la presentación de facturas a través de FACe.
    - La identificación y firma electrónica de las personas interesadas en el procedimiento administrativo mediante empleado público municipal utilizando el sistema de firma electrónica del que esté provisto el personal municipal.
    - El resellado de documentos para ampliación de la validez de las evidencias y extensión del plazo de validez de la firma.
    - La identificación ciudadana mediante comparecencia en sede.
    - La firma electrónica con identificación y evidencia electrónica de un documento electrónico.

La presente Política de identificación y firma electrónica, de sellos electrónicos, de certificados y demás sistemas de identificación y firma municipales está coordinada por la Dirección General de Innovación y Promoción de Gijón con el resto de políticas de innovación tecnológica y de procesos municipales, como la política de gestión de documentos o la política de seguridad de la información corporativas que resulta de la aplicación de los Esquemas Nacionales de Interoperabilidad y de Seguridad atendiendo a prácticas de certificación de la Autoridad de Certificación que en cada momento preste servicios a la administración municipal de los certificados descritos en el presente documento.

Esta política se aplicará a través de resoluciones de la Alcaldía por las que se irán aprobando progresivamente los diferentes procedimientos y cartas de servicio que se definan durante la iniciativa Gijón-IN. Estas podrán incorporar nuevos modos de identificación y firma en el marco de los criterios generales establecidos en la presente política. Las bases de las diferentes convocatorias, pliegos de condiciones administrativas y otros documentos que rijan las relaciones de las personas con el Ayuntamiento podrán incorporar, previo informe motivado de la Dirección General de Innovación y Promoción de Gijón, otros modelos de identificación y firma a los previstos en la presente política.

En aquellos aspectos no contemplados por la presente Política se atenderá a lo descrito en la política de firma de la Administración General del Estado vigente.

2. Consideraciones Generales

Se define, según la Ley 59/2003, la firma electrónica distinguiendo los siguientes conceptos:

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

Para que una firma electrónica pueda ser considerada firma electrónica avanzada en los términos de la Ley 59/2003 se infieren los siguientes requisitos:

- **Identificación:** que posibilita garantizar la identidad del firmante de manera única.
- **Integridad:** que garantiza que el contenido de un mensaje de datos ha permanecido completo e inalterado, con independencia de los cambios que hubiera podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación.
- **No repudio:** es la garantía de que no puedan ser negados los mensajes en una comunicación telemática.

Cuando se firman datos, la persona firmante indica la aceptación de unas condiciones generales y unas condiciones particulares aplicables a aquella firma electrónica mediante la inclusión de un campo firmado, dentro de la firma, que especifica una política explícita o implícita.

Si el campo correspondiente a la normativa de firma electrónica está ausente y no se identifica ninguna normativa como aplicable, entonces se puede asumir que la firma ha sido generada o verificada sin ninguna restricción normativa, y en consecuencia, que no se le ha asignado ningún significado concreto legal o contractual. Se trataría de una firma que no especifica de forma expresa ninguna semántica o significación

concreta y, por lo tanto, hará falta derivar el significado de la firma a partir del contexto (y especialmente, de la semántica del documento firmado).

La finalidad de esta política de identificación y firma es reforzar la confianza en las transacciones electrónicas a través de una serie de condiciones para un contexto dado, el cual puede ser una transacción determinada, un requisito jurídico o un rol que asuma la parte firmante, entre otros.

3. Alcance de esta Política

Esta Política tiene por objeto establecer el conjunto de criterios comunes que, en materia de firma electrónica e identidad electrónica, definen las directrices a seguir en relación con la autenticación y el reconocimiento de firmas electrónicas basadas tanto en certificados como en evidencias electrónicas, en el ámbito de las soluciones de gestión corporativas, garantizando la autenticidad, la integridad y la conservación de los documentos firmados electrónicamente, tanto en lo referido a las firmas como a los sellos electrónicos, siendo de aplicación a:

a) El conjunto de la Administración Municipal y sus organismos públicos, integrando a los órganos administrativos, las áreas y unidades del Ayuntamiento, así como a los organismos autónomos municipales (Fundación Municipal de Cultura, Educación y Universidad Popular, Fundación Municipal de Servicios Sociales y Patronato Deportivo Municipal).
b) Así mismo, será de aplicación a las sociedades y fundaciones en las que sea mayoritaria la participación directa o indirecta del Ayuntamiento en lo relativo exclusivamente a la identificación y firma de las personas interesadas y a las relaciones entre el Ayuntamiento y las citadas entidades.

En adelante, en este documento, cuando se mencione al Ayuntamiento, se estará haciendo referencia al conjunto de entidades definido en los dos puntos anteriores.

A su vez, el objetivo de esta Política es establecer qué identidades y certificados digitales de la ciudadanía (entendiendo como tal a las personas físicas y jurídicas), en sus relaciones con el Ayuntamiento a través de medios electrónicos, son aceptados y qué certificados digitales usan el personal y cargos de dicha entidad, estableciendo el sistema de gestión de su ciclo de vida.

Esta Política también viene a definir la estrategia a seguir por el Ayuntamiento para la preservación a largo plazo de las firmas electrónicas.

3.1 Datos identificativos de esta Política

Nombre del documento	Política de identificación y firma, de sellos electrónicos, de certificados y de otros sistemas de identificación y firma de la Administración Municipal de Gijón
Versión	1.0
Identificador del gestor	Ayuntamiento de Gijón (DIR3: L01330241)
URL:	https://sedeelectronica.gijon.es Puede verificar la autenticidad de este documento en www.gijon.es/cev

Fecha de expedición	Fecha de firma de la resolución de aprobación de la presente Política.
Ámbito de aplicación	Esta política de identificación y firma aplica a: La actividad administrativa del Ayuntamiento, de sus organismos autónomos y de las Empresas Municipales. El personal municipal que presta servicios en alguna de las entidades mencionadas anteriormente, así como los cargos electos o directivos de los mismos. La relaciones electrónicas entre la ciudadanía, personas interesadas de los procedimiento y servicios municipales. La figura denominada actuación administrativa automatizada.
Responsable de la Política y datos de contacto	ección General de Innovación y Promoción de Gijón ail: mailto:administracionelectonica@gijon.es?subject=Política de firma

3.2 Entrada en vigor de la Política

Esta Política de identificación y firma, de sellos electrónicos, de certificados y de otros sistemas de identificación y firma del Ayuntamiento, entrará en vigor en la fecha de su aprobación por resolución del órgano competente, y será válida hasta que sea sustituida o derogada por una eventual política posterior, pudiendo determinarse un periodo de tiempo transitorio en el que convivan ambas versiones que permita la adecuación de los diferentes sistemas de gestión a las especificaciones de la nueva versión.

Este periodo de tiempo de transición se tendrá que indicar en la nueva versión y superado el mismo solo será válida la versión actualizada.

3.3 Gestión de la presente Política

La presente Política de identificación y firma será objeto de aprobación, mantenimiento, actualización y publicación por parte de la Dirección General de Innovación y Promoción de Gijón. Dicho órgano será el encargado de vigilar su correcta actualización atendiendo a:

a) Las modificaciones motivadas por necesidades propias de la organización
b) Los cambios en políticas relacionadas
c) Los cambios en los certificados electrónicos emitidos por los prestadores de servicios de certificación a los que se referencia.
d) Cualquier otro cambio normativo, técnico u operativo que pueda motivar su revisión.

En todo caso, toda modificación o actualización de la presente Política habrá de ser aprobada por resolución de Alcaldía para que surta los efectos oportunos previa motivación razonada de los servicios adscritos a la Dirección General de Innovación y Promoción de Gijón.

De la misma manera, se establecerá en la sede electrónica municipal un repositorio con las distintas versiones de la presente Política, a fin de conservar un histórico y facilitar la consulta y validación de los sistemas de firma/identificación que se hayan ido aprobando en cualquier momento desde su aprobación.

4. Normativa aplicable y estándares internacionales

En este apartado se define aquella normativa aplicable a la presente Política de firma, así como los estándares internacionales que se han tenido en cuenta para la definición del presente documento.

4.1 Normativa aplicable

La normativa en la que se apoya esta política de identificación y firma se concreta a continuación:

- El 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 (eIDAS) y su normativa de desarrollo.
- La 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 anterior.
- La Ley 59/2003, de 19 de diciembre, de Firma Electrónica así como las modificaciones de esta en aplicación del Reglamento eIDAS.
- La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- El Real Decreto 4/2010, de 8 de enero, del Esquema Nacional de Interoperabilidad.
- El Real Decreto 3/2010, de 8 de enero, del Esquema Nacional de Seguridad.
- La Resolución de 19 de julio de 2011, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de Certificados de la Administración.
- La Resolución de 19 de julio de 2011, por la que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico.

4.2 Estándares internacionales

Los estándares internacionales que se han tenido en cuenta para la definición del presente documento se enumeran a continuación:

- Estándares técnicos de firma electrónica compartida bajo licencia de uso BY - NC - SA del Creative Commons de la empresa Astrea La Infopista Jurídica SL: http://astrea.es/web12/biblioesp/_estandares-tecnicos/.

- 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, v.1.7.4 i 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): Gestión de documentos. Formato de fichero de documento electrónico para la conservación a largo plazo. Parte 1: Uso del PDF 1.4.
- 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 i 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 i RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 5652, RFC 4853 i RFC 3852, Cryptographic Message Syntax (CMS).
- ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

5. Roles involucrados

Los diferentes roles que intervienen en el proceso de creación y validación de la firma electrónica son los siguientes:

a. **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, entendiéndose en este caso que actúa a través de la figura de la representación.

b. **Creadora de un sello digital:** persona jurídica que crea un sello electrónico.

c. **Verificadora:** 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 al 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.

d. **Prestador de servicios de firma electrónica incluido en la lista de confianza de servicios de certificación:** persona física o jurídica que expide certificados electrónicos o presta otros servicios relacionados con la firma electrónica incluido en la lista de servicios de certificación del Ministerio de Industria, Comercio y Turismo, o ministerio competente en su caso.

e. **Emisora y gestora de la Política de firma electrónica y de certificados:** entidad que se encarga de generar y gestionar el documento de la Política, que regirá las actuaciones del firmante, el verificador y de los prestadores de servicios, los procesos de generación y validación de firma electrónica.

6. Identificación y firma:

La Administración Municipal está obligada a verificar la identidad de las personas interesadas en los diferentes procedimientos administrativos o servicios de su competencia.

Estas personas interesadas podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento. Se consideran válidos a efectos de firma los sistemas previstos en esta política de identificación y firma electrónica.

Cuando se utilice un sistema de firma de los previstos en esta política, la identidad de las personas interesadas se entenderá ya acreditada mediante el propio acto de la firma.

Con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo, será suficiente con que se acredite previamente la identidad a través de cualquiera de los medios de identificación previstos en esta política.

La Administración Municipal solo requerirá el uso obligatorio de firma para:

a) Formular solicitudes.

b) Presentar declaraciones responsables o comunicaciones.

c) Interponer recursos.

d) Desistir de acciones.

e) Renunciar a derechos.

Se prestará asistencia en el uso de medios electrónicos, especialmente a las personas que no están obligadas normativamente a su utilización, principalmente en lo referente a la identificación y firma electrónica, a la presentación de solicitudes y a la obtención de copias auténticas.

Si alguna de estas personas no dispone de los medios electrónicos necesarios, su identificación o firma electrónica, podrá ser válidamente realizada por el personal municipal. En este caso, será necesario que la persona se identifique ante el personal municipal y preste su consentimiento expreso para esta actuación, de lo que deberá quedar constancia para los casos de discrepancia o litigio.

Este soporte y apoyo se realizará preferentemente por medios electrónicos y, a ser posible, con el sistema de cita previa integrado con las soluciones de gestión municipales al objeto de garantizar la integridad de la información.

6.1 Certificados digitales y otras identidades y firmas digitales

En la implantación de las herramientas de Administración Electrónica, es imprescindible asegurar las garantías jurídicas y respeto a los derechos de ciudadanía y empresas en las gestiones que se realicen de forma electrónica.

Los documentos que se generan electrónicamente llevan asociados tres conceptos que son necesarios salvaguardar y que son la confidencialidad, la integridad y la autenticidad:

- La confidencialidad se refiere a la capacidad de mantener un documento electrónico inaccesible a todos, excepto a una lista determinada de personas.

- La integridad garantiza que el documento recibido coincide con el documento emitido sin posibilidad alguna de cambio.

- La autenticidad se refiere a la capacidad de determinar si una lista determinada de personas ha establecido su reconocimiento y/o compromiso sobre el contenido del documento electrónico. La autenticidad en un documento tradicional se garantiza mediante la firma autógrafa. Así, una persona, o varias, manifiestan su voluntad de reconocer el contenido de un documento.

La confidencialidad, integridad y autenticidad (los procesos definidos de firma y cifrado) se aseguran mediante la tecnología llamada criptografía. La aplicación de la criptografía en el envío de mensajes digitales, proporciona las herramientas idóneas para asegurar las cuestiones mencionados. La confidencialidad se relaciona comúnmente con técnicas de cifrado y la integridad y la autenticidad con técnicas de firma digital, aunque ambos en realidad se reducen a procedimientos criptográficos de cifrado y descifrado.

La criptografía asimétrica es el método criptográfico que utiliza un par de claves complementarias, la pública y la privada, para cifrar documentos o mensajes. Lo que está codificado con una clave privada necesita su correspondiente clave pública para ser descodificado. Y viceversa, lo codificado con una clave pública solo puede ser descodificado con su clave privada. La clave privada debe ser conocida únicamente por su propietario, mientras que la correspondiente clave pública puede ser dada a conocer abiertamente.

El hecho de que la clave privada solo sea conocida por su propietario permite que:

- Cualquier documento generado a partir de esta clave necesariamente tiene que haber sido generado por el propietario de la clave (firma electrónica).

- Un documento al que se aplica la clave pública solo podrá ser abierto por el propietario de la correspondiente clave privada (cifrado electrónico).

Un certificado electrónico es un documento emitido y firmado por una autoridad de certificación que identifica a una persona (física o jurídica) con un par de claves y que contiene la siguiente información:

- Datos de identificación del titular del certificado (Nombre del titular, NIF, e-mail,…).

- Distintivos del certificado: número de serie, entidad que lo emitió, fecha de emisión, periodo de validez del certificado, etc.
- Una pareja de claves: pública y privada.
- La firma electrónica del certificado con la clave de la autoridad de certificación (AC) que lo haya emitido.

Toda esta información puede dividirse en dos partes:

- Parte privada del certificado: clave privada.
- Parte pública del certificado: resto de datos del certificado, incluida la firma electrónica de la autoridad de certificación que lo emitió.

La parte privada nunca es cedida por su titular. Esta es la base de la seguridad. Con la pareja de claves se pueden realizar funciones de cifrado con la peculiaridad de que lo que se cifra con la privada solo se puede verificar con la pública y viceversa.

Una firma electrónica es una huella digital de un documento cifrado con una clave. La huella digital se obtiene aplicando un algoritmo a un mensaje. Este algoritmo tiene dos características fundamentales:

- No existe la posibilidad de volver a obtener el mensaje partiendo de la huella digital generada.
- Si se cambia el mensaje, la huella digital que se obtiene es diferente. Estas dos características garantizan la integridad del mensaje. Si se cambia el contenido del mensaje, el que verifica la firma lo va a saber.

La huella digital se cifra con la clave privada del certificado de la persona que firma. Aplicando los mecanismos de verificación, el receptor va a conocer quién firmó y así esa persona no puede repudiar la autoría del mensaje.

La presente política de firma se basa y aplica los requerimientos jurídicos, técnicos y funcionales establecidos por la normativa vigente en materia de administración electrónica, por la Administración General del Estado a través de la Secretaría General de Administración Digital (SGAD) y de la Conferencia Sectorial de Administración Electrónica publicadas en el portal de administración electrónica.

Para profundizar sobre los certificados electrónicos se recomienda consultar el portal firmaelectronica.gob.es

6.1.1 Certificados digitales admitidos por el Ayuntamiento

Los mecanismos de identificación basados en certificado digital se sustentan en la existencia de prestadores de servicios de certificación, incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’, que emiten certificados digitales y permiten comprobar que un certificado concreto ha sido correctamente emitido y que continúa siendo válido en el momento de su uso, es decir, de la firma o sello de un documento. La relación

entre el prestador de servicios de certificación y la entidad que valida el certificado es una relación que se fundamenta en la confianza.

En este contexto, el Ayuntamiento de Gijón, de acuerdo a lo dispuesto en los artículos 9 y 10 de la Ley 39/2015, aceptará todos los certificados digitales incluidos en la Lista de confianza de prestadores de servicios electrónicos de confianza (TSL) del Ministerio de Industria, Comercio y Turismo, o Ministerio que ostente esta competencia en función de los diferentes Decretos de estructura, y validados con la plataforma de validación gestionada por la Administración General del Estado conocida como @firma, la cual establece un listado de entidades y de perfiles de certificados que cumplen con los estándares de calidad y niveles de seguridad establecidos según lo previsto en el artículo 9 de la Ley 40/2015.

De la misma manera, el Ayuntamiento de Gijón, utilizará los servicios de validación de @firma, accesible a través de la red SARA o a través del nodo de @firma del que dispone la Agencia de Tecnología y Certificación Electrónica (ACCV), servicio al que este Ayuntamiento se encuentra suscrito, o cualquier otro que pueda estar disponible.

6.1.2 Otros sistemas de identificación admitidos por el Ayuntamiento

La Administración Municipal fomentará y utilizará como sistema preferente de identificación los mecanismos de identificación admitidos por la plataforma Cl@ve: Cl@ve PIN 24h y Cl@ve permanente, así como el resto de sistemas de identificación que esta plataforma vaya incorporando progresivamente.

Se motiva el uso preferente de Cl@ve al garantizar la seguridad y al permitir la identificación, e incluso firma, ante otras administraciones públicas nacionales y europeas al estar reconocida por las Administraciones Públicas nacionales y por diferentes países europeos ya que está incorporada en el marco europeo de interoperabilidad.

Con ello se garantiza el cumplimiento de lo dispuesto en el artículo 9.4. de la Ley 39/2015 en el que se establece que la aceptación de alguno de los sistemas previstos en el citado artículo por la Administración General del Estado, como sucede con el sistema cl@ve, servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo.

Progresivamente se irá incorporando cl@ve como sistema generalizado de identificación electrónica ante la Administración Municipal.

Con carácter interno, en la plataforma de gestión integrada municipal se recogerá, como figura análoga a la firma electrónica, como acto de revisión sobre documentos electrónicos, el denominado visado que consiste en una validación o visto bueno de documentos durante el proceso-circuito de firma, que si bien no incorpora evidencias, atributos, ni constancia directa sobre los documentos electrónicos, permite la trazabilidad de esta validación al almacenar la información relativa a la validación o no del documento durante el proceso-circuito de firma. Para este tipo de procesos de visado, el personal municipal utilizará el medio de identificación para el acceso a la plataforma de gestión integral que les será asignado de acuerdo a la Política de Seguridad corporativa. La actuación de visado sobre documentos es compatible con otros actos de firma electrónica posteriores o anteriores.

Mención especial merece la incorporación, por parte del Ayuntamiento, del sistema de firma biométrica, que se recoge de forma presencial sobre documentos electrónicos. Dicha operativa facilita, para aquellos casos en que se precisa recoger la voluntad de firmantes externos a la organización, sobre documentos electrónicos, la digitalización del acto de firma manuscrita, con una tableta electrónica, aplicando posteriormente un sello de órgano mediante la figura de la Actuación administrativa automatizada, asegurando con ello la integridad,

autenticidad y el no repudio del contenido del documento. Este sistema se ajustará al contenido del artículo 26 del Reglamento Europeo 910/2014 y demás normativa de desarrollo, para ser reconocido como firma electrónica avanzada.

Igualmente se incorporan en esta política otros sistemas de identificación y firma en aplicación del artículo 9.2.c) de la Ley 39/2015.

6.2 Certificados digitales utilizados por el Ayuntamiento

Los tipos de certificados que se emiten por el Ayuntamiento, como autoridad de registro delegada del prestador de servicios de certificación, para su utilización por el personal municipal, altos cargos, personal electo, otras personas colaboradoras y para el adecuado funcionamiento de los servicios electrónicos serán los siguientes:

i. **Certificado Digital de Empleado Público**: de uso para el personal municipal, cuya actividad esté regulada por el Texto Refundido del Estatuto Básico del Empleo Público (TREBEP) y normas de desarrollo, se le proveerá de un certificado digital provisto por la Autoridad de Certificación con la que el Ayuntamiento de Gijón, en cada momento, haya establecido un contrato o convenio para su provisión. Con carácter general, la emisión de estos certificados se realizará a los empleados municipales, bien sean personal funcionario o bien personal laboral del Ayuntamiento.

   La emisión de estos certificados se hará para el ejercicio de las funciones y potestades atribuidas por razón del puesto, en ningún caso deberán utilizarse para fines personales.

ii. **Certificado de Pertenencia a Entidad**: para perfil análogo al anterior que será utilizado para el personal de las Empresas Municipales, así como los cargos electos de la Corporación y demás colectivos cuya relación de prestación de servicios no esté regulada por el TREBEP, quedando fuera de esta Política aquellos usos de carácter personal que se le puedan dar.

iii. **Sellos Electrónicos**: se aplicarán en aquellos procesos en los que se pueda emplear la figura de la actuación administrativa automatizada**,** de acuerdo a lo dispuesto en el Art. 41 de la Ley 40/2015 y cuyo uso será aprobado mediante resolución de la Alcaldía para cada uno los procesos que se determinen. Para ello el Ayuntamiento utilizará los sellos de los prestadores de servicios de certificación con los que exista contrato o convenio para su provisión, según lo mencionado en los párrafos anteriores.

   La relación de los sellos electrónicos empleados por el Ayuntamiento se publicará en su Sede Electrónica.

iv. **Certificados de Servidor Seguro**: el Ayuntamiento podrá utilizar diferentes certificados digitales de distintos prestadores de servicios de certificación. La decisión sobre qué certificados se utilizarán vendrá condicionada en cada momento por las necesidades técnicas y organizativas del Ayuntamiento y la difusión y nivel de confianza de estos prestadores de servicios de certificación en los navegadores utilizados por el conjunto de la sociedad.

   La relación de certificados de servidor seguro empleados por el Ayuntamiento se publicarán en su Sede Electrónica.

v. **Certificado de Sede Electrónica:** igual que en el caso anterior, la sede electrónica del Ayuntamiento se identificará a través de un sello electrónico que identifica de forma segura el dominio sedeelectronica.gijon.es. La clave pública de este certificado será publicada en la propia sede para las comprobaciones que los usuarios deseen realizar a través del mismo y pueda ser agregado con el nivel de confianza adecuado por las personas usuarias de la sede municipal.

vi. **Certificados de Representación:** se emiten en el ámbito de la Administración Municipal e identifican a las personas que ostenten la representación de tales entidades, habilitándoles entre otras funciones, la representación para la realización de trámites ante otras Administraciones, en función de la correspondiente Resolución de la Alcaldía o Acuerdo de órganos competente

vii. **Firma Electrónica de Transmisiones de Datos**: en aquellos casos en los que el Ayuntamiento utiliza servicios interoperables de otras Administraciones o entidades, donde la firma se asociará al protocolo de transporte, formando parte de los mecanismos de cifrado a implementar en una comunicación segura.

La firma electrónica de transmisiones de datos estará basada en los estándares recogidos en la Norma Técnica de Interoperabilidad de Catálogo de estándares. La firma de transmisiones de datos proporciona integridad, autenticación y no repudio entre dos servidores (punto a punto). En este caso, la firma está asociada al protocolo de transporte, formando parte de los mecanismos de cifrado a implementar en una comunicación segura. Cuando se implementen mecanismos de transmisión firmada de datos entre el Ayuntamiento y otras entidades, que deban cifrarse en una comunicación segura, se hará bajo las especificaciones SOAP, Simple Object Access Protocol, aceptándose al menos en su versión 1.1., tal y como especifica la Norma Técnica de Interoperabilidad de Catálogo de estándares. Para transmisiones firmadas de datos basadas en Servicios Web, se aplicarán las firmas electrónicas según el estándar WS-Security: SOAP Message Security de OASIS, versiones 1.0, 1.1 o superiores y, en particular, cumpliendo con la especificación estándar X.509 Certificate Token Profile.

En circunstancias excepcionales debidamente motivadas, y previa aprobación por Resolución de la Alcaldía, se podrán aplicar otras especificaciones diferentes a las citadas especificaciones SOAP.

De forma extraordinaria, en caso de que los certificados provistos por la Autoridad de Certificación que en cada caso provea al Ayuntamiento, independientemente de su perfil, presentasen algún tipo de incidencia o inconveniente de carácter técnico, aceptación en determinados portales, etc. se podrá obtener un certificado de firma electrónica/sello electrónico de cualquier otra Autoridad de Certificación que permita corregir la situación, pudiendo encontrarse distintas autoridades de certificación prestando servicios al Ayuntamiento simultáneamente en un determinado momento.

En aquellos casos en que el certificado se provea a los usuarios y cargos del Ayuntamiento, se emplearán aquellos formatos de certificados que faciliten la operativa de firma municipal, siendo los formatos preferentes de los certificados:

- Software (en formatos .p12 y .pfx)
- HSM (Hardware Security Module)
- Hardware (Tarjeta Criptográfica o Token USB)

Por Resolución de la Alcaldía se determinará el procedimiento de emisión de los certificados electrónicos al personal municipal, altos cargos, personal electo y demás personal colaborador que incluirá un documento electrónico en el que se establecen las condiciones de uso de los sistemas de identificación y firma así como las demás prescripciones en relación con la utilización de los sistemas de información municipales, apertura de cuentas en el dominio y protección de datos de carácter personal.

6.3 Sistemas de identificación provistos por el Ayuntamiento a sus empleados, altos cargos y otros tipos de personal

El Ayuntamiento pondrá en marcha progresivamente la identificación, con carácter general, a través del certificado electrónico que se provee a las personas usuarias de las soluciones de gestión.

Para ello el Ayuntamiento provee a todo su personal que haya de tener acceso a determinados servicios o aplicaciones, de un nombre único de usuario y una contraseña dentro del dominio municipal. De acuerdo a las políticas de seguridad acordes al Esquema Nacional de Seguridad de aplicación en el entorno municipal, y la Política de Seguridad que a dicho respecto, emita el Ayuntamiento, la contraseña provista habrá de ser renovada por el usuario periódicamente, en el plazo definido a tal efecto. Además, a dicha contraseña se le añadirán determinados niveles de complejidad, como es la inclusión obligatoria de mayúsculas/minúsculas, números y/o símbolos, un número mínimo de caracteres, etc.

De la misma manera, en determinados aplicativos corporativos, el identificador del usuario y la contraseña podrán ser sustituidos por otros identificativos, como puede ser el número de empleado, pin de acceso u otros.

A su vez, en determinadas ocasiones para trabajar con aplicativos de terceros, o con otras herramientas externas al Ayuntamiento, fuera del entorno municipal, se facilitarán al usuario unas credenciales distintas a las descritas previa mente, que le serán comunicadas de forma segura y adecuada, acorde a la Política de Seguridad de este Ayuntamiento, para la realización de las labores que precisen.

7. Ciclo de vida de los certificados digitales entregados por el Ayuntamiento

La Autoridad de Certificación emisora de los certificados digitales que en cada momento provea al Ayuntamiento, será la responsable de definir las políticas de gestión de los certificados emitidos, definiendo:

a) Periodo de vigencia de los certificados electrónicos y sellos emitidos, en función del perfil de los mismos.
b) Casos, modo y motivación de la revocación de los certificados en caso de pérdida de control sobre los mismos, olvido de la clave de protección de los mimos, etc., comprendiendo como revocación la finalización de la validez del certificado con carácter previo a la fecha de caducidad que se establezca en el mismo.
c) Plazo y motivación en que opera la suspensión de la validez del certificado, entendida como situación temporal, pero que en caso de superar el plazo estimado o vuelve a situación activa o deviene en una revocación definitiva del certificado.
d) Modo de renovación de cada certificado.
e) Proceso de validación para la emisión del certificado.
f) El modo en que se recoge la voluntad del solicitante (mediante contrato, aceptación de condiciones…).
g) Resto de documentación que se precisa para la emisión (acreditación de identidad, nombramiento, poderes…).

En función de la Autoridad de Certificación que en cada caso provea al Ayuntamiento de Gijón de los distintos tipos de certificados (Empleado Público, Pertenencia, Sello Electrónico, Sede Electrónica o de Servidor Seguro, Representación, etc.) y de acuerdo a la declaración de prácticas de certificación y las políticas de firma asociadas a los certificados de los que se provea al Ayuntamiento, se definirá un procedimiento para la emisión, renovación, revocación y suspensión de certificados y sellos electrónicos, donde se dejará constancia de las comprobaciones y labores a realizar, así como la gestión posterior de la documentación generada. Dicho procedimiento será aprobado mediante resolución de Alcaldía.

7.1 Gestión interna del ciclo de vida de los certificados de firma electrónica, sellos y otros sistemas de firma basados en certificados expedidos por el prestador de servicios de certificación

La Dirección General de Innovación y Promoción de Gijón será la responsable de la gestión interna de los certificados y, con el apoyo del Servicio de Sistemas de Información, de las labores de:

i. Solicitud de emisión e instalación de los certificados y sellos
ii. Control del ciclo de vida de los certificados, sellos, etc.:
    a. Labores de solicitud de suspensión o de revocación de los certificados emitidos.
    b. Gestión de las renovaciones de los certificados.
iii. Gestión de la documentación obtenida de la emisión de los certificados, copias y demás documentación relativa a los certificados
iv. Seguimiento de las prácticas de certificación y aquellos otros trabajos relacionados con la misma.

El Servicio de Gestión de Recursos Humanos realizará las gestiones necesarias para la correcta gestión del ciclo de vida de los certificados de acuerdo con el procedimiento se apruebe al efecto.

Se tendrá especial atención al control de los certificados del personal que, por razón de cese o cambio de puesto, deban revocarse, así como aquellos casos en los que se produzcan cambios en el equipo de gobierno del Ayuntamiento y sus distintos altos cargos, así como en las gerencias de las entidades empresariales dependientes.

Para desarrollar esta operativa, dentro del marco de las relaciones que se establezcan con la Autoridad de Certificación correspondiente, se establecerá una Autoridad de Registro desde la que se cursen, a través de los operadores corporativos que se nombren al efecto mediante resolución de Alcaldía, aquellas labores detalladas en el punto anterior y de acuerdo al procedimiento que para desarrollar estas labores, se hubiese aprobado

Dentro de dicha Autoridad de Registro, las personas responsables gestionarán:

- El inventario de los distintos certificados emitidos que contemple, al menos, el código de identificación del certificado, el tipo de certificado, el emisor del mismo, la persona o aplicación que gestiona el certificado, la fecha de emisión, fecha de caducidad del mismo, el estado del mismo.
- En las soluciones de gestión municipales, en un expediente electrónico, se almacenará el contrato de prestación de servicios de firma y aceptación de la política de firma de la Autoridad de Certificación que de cada usuario se obtenga. A través de dicha herramienta, se definirá la forma más adecuada de comunicar a la Autoridad de Registro copia de dicha documentación.
- Cualquier otra función que por la política de firma de la Autoridad de Certificación, o por la operativa de seguridad tecnológica corporativa del Ayuntamiento, acorde al Esquema Nacional de Seguridad, se precise.

Todas estas funciones se realizarán de acuerdo a la operativa definida en la Declaración de prácticas de certificación de la Autoridad de Certificación que en cada momento provea al Ayuntamiento de sus servicios de certificación.

8. Sellado de tiempo

El sellado de tiempo será la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

Se suprimirá la utilización de sellos de caucho en cualquier tipo de documento en soporte papel antes de su digitalización para evitar confusiones. Por Resolución de la Alcaldía se aprobará la aplicación del sellado de tiempo y la no aplicación en documentos de soporte papel de sellos de caucho.

Las características principales del sello de tiempo son:

- El sello de tiempo es un sello electrónico generado por un tercero de confianza sobre la base de un certificado digital especialmente destinado a estos efectos.
- Da evidencia de la fecha y hora en que se ha producido un acto. Se utiliza conjuntamente con un documento en cualquier formato y que puede estar firmado electrónicamente.
- Mediante un proveedor de sellado de tiempo, se sellará la fecha y hora del instante en que se ha realizado el acto.
- El proceso consiste en crear una evidencia electrónica sobre una firma electrónica: se calcula el resumen criptográfico del documento y/o sus firmas electrónicas (en el caso del resellado), es decir, una operación matemática que se aplica al conjunto de información sobre el cual emitir el sello de tiempo y obtiene una cadena de bits denominada *hash*, que se cifra con la clave privada del certificado de sello de tiempo utilizado para hacer la operación. Se devuelve esta firma conjuntamente con la fecha y hora de la operación, así como información sobre el certificado de sello de tiempo utilizado para hacer la firma.
- El sello de tiempo se incorporará a las firmas electrónicas, preferentemente en el formato especificado en el estándar XAdES-T, CAdES-T y PAdES-LTV.
- El sellado de tiempo se realizará a través de los servicios proporcionados por la plataforma @firma, accesible a través de la red SARA o por el prestador de servicios de certificación que el Ayuntamiento pueda contratar en cada momento.

9. Sistemas y clases de firma o sello

En el presente apartado se recopilan los aspectos relacionados con la firma electrónica en el marco del Ayuntamiento, determinando los distintos usos de la firma y sello en el ámbito de los sistemas empleados por la Administración Municipal.

Se persiguen los siguientes objetivos:

- Dotar al Ayuntamiento de un sistema para el control, el uso y la conservación de la documentación original firmada electrónicamente, cuyo origen es el desarrollo habitual de su actividad política y administrativa, en el ejercicio de sus competencias.
- Garantizar la gestión documental adecuada en el ámbito del Ayuntamiento, asegurando su autenticidad, fiabilidad e integridad, así como la disponibilidad futura a lo largo del ciclo de vida, a través de la plataforma de gestión integrada municipal, contemplando desde el registro, el expediente y su posterior archivo electrónico.
- Dar cumplimiento al marco normativo establecido por:
  - Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas.
  - Ley 40/2015 de Régimen Jurídico del Sector Público.
  - Real Decreto 4/2010 por el que se establece el Esquema Nacional de Interoperabilidad y las Normas Técnicas de Interoperabilidad (Documento Electrónico, Expediente Electrónico…) que lo desarrollan.
  - Demás normativa de administración electrónica sobre identificación y firma electrónica.

9.1 Tipos de firma a utilizar en el ámbito del Ayuntamiento

Los tipos de firma que se utilizan en el ámbito municipal son los siguientes:

i. **Firma electrónica basada en el uso de un certificado digital dentro de la plataforma de gestión integrada municipal**. Es el sistema de firma electrónica en el que, partiendo de la clave privada de un usuario, se cifra el resumen criptográfico del documento a firmar, y se añade a esta firma información del certificado utilizado para la firma, la fecha de la firma, la política de firma, etc. Una vez firmado, el documento quedará almacenado en el gestor documental corporativo, accediendo al mismo desde la propia plataforma de gestión integrada, a través del denominado Código Electrónico de Verificación (CEV) que permite la consulta de un mismo documento desde las diferentes soluciones de gestión: expedientes, económico-financiero, tributaria, padrón, registros, etc. El documento podrá remitirse a una persona interesada o a otra administración en formato electrónico, mediante notificación o comunicación electrónica para acceder a la copia auténtica del documento, para permitir con ello su verificación por la persona receptora, o mediante copia en papel del mismo, en cuyo caso, la verificación del documento original se realizará, en todo caso, mediante el Código Electrónico de Verificación (CEV).

   Se incluye en este tipo la firma electrónica mediante un sello digital para aplicar la figura de actuación administrativa automatizada cuya utilización será preferente frente a otros tipos para aquellos procesos y subprocesos en los que no exista intervención de empleado público motivándose esta preferencia en la normalización y celeridad de la actuación administrativa.

ii. **Firma electrónica por parte de personal funcionario habilitado para su aplicación en la identificación y firma de las personas interesadas en los procedimientos administrativos**. El personal municipal utilizará la firma electrónica basada en certificados digitales, descrita en el apartado anterior, en aquellos supuestos en los que alguna de las personas interesadas en los procedimientos administrativos no disponga de los medios electrónicos necesarios, consiguiendo con ello la identificación y firma electrónica de ésta en el procedimiento administrativo.

iii. **Firma basada en la identificación más voluntad de firma.** En los procedimientos que se determine, y con las condiciones que se establezcan se podrán establecer otros mecanismos de firma, basada en la identificación de la persona que ha participado en el proceso y la plasmación de su voluntad de firma, a través de

evidencias electrónicas que cuentan con un registro previo fruto de las potestades, prerrogativas y competencias municipales. Este registro previo permite garantizar la identidad en base al intercambio de información conocida entre ambas partes y que consta en un registro previo.

Se establecerá este tipo de firma en casos excepcionales y para sujetos no obligados que precisen condiciones especiales de identificación y firma que favorezcan el acceso y uso de los servicios electrónicos aplicando para ellos una clase de firma simple de las previstas en el apartado siguiente.

En este supuesto las personas interesadas que utilicen este tipo de firma entenderán acreditada su identidad mediante el propio acto de la firma.

iv. **Firma electrónica ordinaria:** es aquella que utiliza el personal municipal fuera del entorno de la plataforma de gestión integrada municipal, como puede ser la firma que se produzca mediante herramientas de ofimática o análogas, que permiten la gestión de identidades electrónicas, así como la producción de firma sobre documentos. Dicha operativa dota de autenticidad, fiabilidad e integridad al documento firmado, si bien no contempla su ulterior gestión, ni la obtención de sellos de tiempo ni firmas de conservación a largo plazo.

Por estos motivos, el Ayuntamiento no se responsabiliza de su seguridad y conservación recayendo esta responsabilidad en el personal municipal que los genera.

v. **Firma biométrica:** ya mencionada, incorporada en aquellos casos en que se precisa firma externa, producida en unidad de acto con un firmante interno, como puede ser la firma de un convenio o de un contrato. Dicha firma biométrica será de utilización mediante sellado posterior, por Actuación administrativa automatizada, que acredita la autenticidad, fiabilidad e integridad del documento. Este sistema debe cumplir el contenido del artículo 26 del Reglamento Europeo 910/2014, para ser reconocido como firma electrónica avanzada.

En aquellos supuestos que por su especificidad se motive se utilizará una combinación de los tipos de firma descritos en los apartados i, ii e iii.

9.2 Clases de firma electrónica

De acuerdo a lo dispuesto en el Reglamento (UE) n.º 910/2014, el Parlamento Europeo y del Consejo, de 23 de julio de 2014 (también denominado Reglamento eIDAS), relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, se definen las distintas clases de firma electrónica:

- Firma electrónica simple: agrupa los datos en formato electrónico, anejos a otros datos electrónicos o asociados de manera lógica con ellos, que utiliza el firmante para firmar.
- 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 que hace referencia y que ha sido 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 sido generada mediante un dispositivo seguro de creación de firma, según

establece el artículo 3.15 del Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del 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.

El Ayuntamiento regulará para cada procedimiento administrativo la clase de firma a aplicar, el nivel de seguridad de firma, así como el rol que debe tener el firmante y, por tanto, qué sistema de firma se utilizará, así como en caso de que sea preciso realizar una firma criptográfica, qué certificados digitales se emplearán, de acuerdo a la Política de Gestión Documental del Ayuntamiento, y que en cada caso será aprobado a través de resolución de la Alcaldía.

9.3 Modalidades de firma electrónica utilizados en el Ayuntamiento

Se establecen las siguientes modalidades de firma electrónica:

Desde una perspectiva técnica, el Ayuntamiento utilizará con carácter general, en los procesos de firma sobre documentos ofimáticos generados desde sus aplicativos corporativos, la conversión del documento a formato PDF y su firma en formato PADES. En los casos que no sea posible la conversión a formato PDF se realizará la firma en el formato XAdES Embedded. A través de esta modalidad, la firma se incrusta en el documento ofimático, haciendo que toda la información que permite la comprobación de la autenticidad e integridad del documento, así como la validación de la propia firma se incorpore igualmente al documento.

En determinadas circunstancias, por motivo de algunas particularidades del Esquema Nacional de Interoperabilidad en lo referido a la Norma Técnica de Expediente Electrónico y la Norma Técnica de Documento Electrónico, y en concreto para la interoperabilidad de los expedientes y documentos electrónicos, a través de aplicaciones como INSIDE, que permite el intercambio de expedientes electrónicos, u otros servicios comunes gestionados por la Administración General del Estado, el Ayuntamiento empleará el formato enveloping (envolvente) en el que el documento firmado es la firma electrónica del documento a firmar, y dentro de dicha firma está el propio documento.

En el Ayuntamiento se podrá realizar *firma simple*, por la cual en un documento existe una única firma electrónica, o bien firma múltiple, por la que sobre un documento se producen varias firmas consecutivas, definiéndose circuitos de firma para que se produzcan las distintas firmas, ya sea en paralelo o en cascada.

9.4 Formatos de firma utilizados en el ámbito del Ayuntamiento

Según el Reglamento eIDAS previamente indicado, las especificaciones para el formato de firmas electrónicas avanzadas para documentos en formato PDF (estándar de facto, en la generación de documentos ofimáticos en el ámbito del Ayuntamiento) se establecen en el PAdES (PDF *Advanced Electronic Signature*, por sus siglas en inglés).

Debido a que los documentos PDF pueden almacenarse durante mucho tiempo, es necesario tener herramientas disponibles que garanticen que los documentos firmados electrónicamente seguirán siendo válidos durante largos períodos de tiempo. Especialmente para documentos relevantes, la validez de la firma debe permanecer incluso si la clave/certificado de firma ha caducado o ha sido revocado, la Autoridad de Certificación emisora ya no existe, o los algoritmos criptográficos que se usaron para crear la firma electrónica ya no son confiables.

Para resolver estas eventualidades hay varias normas, como la especificación técnica ETSI TS 103 172 - Firmas e infraestructuras electrónicas (ESI); *PAdES Baseline Profile*, que se estableció para definir cómo archivar PDF bajo el estándar PAdES.

La especificación TS 103 172 define los perfiles de partida de PAdES que se utilizan para describir diferentes firmas de PAdES, estando definidos en las especificaciones técnicas los siguientes perfiles relevantes:

i. Nivel B: define un perfil para firmas electrónicas a corto plazo. Debe incluir una firma electrónica y el certificado de firma.

ii. Nivel T: al igual que el Nivel B, pero agrega una marca de tiempo, que demuestra que la firma existía en una fecha y hora determinadas.

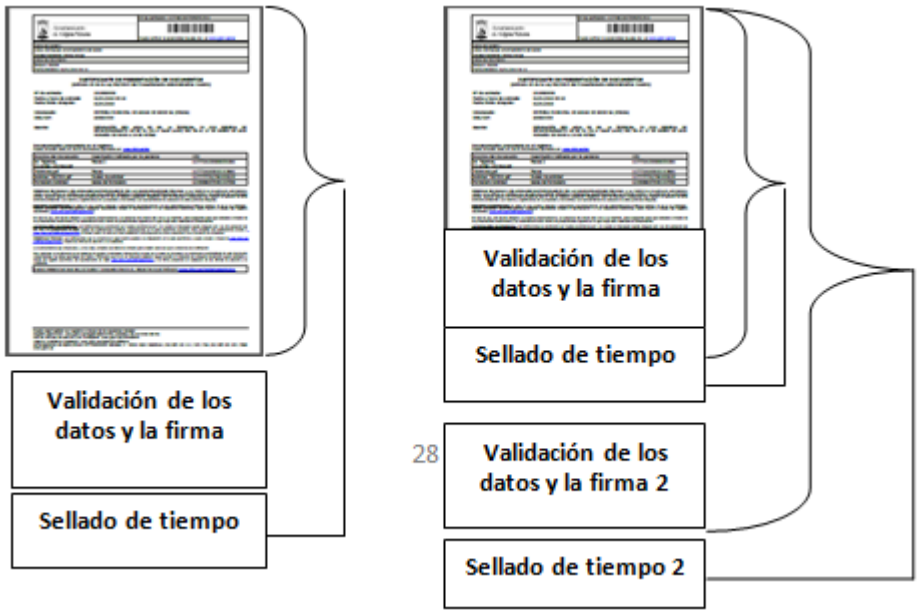
iii. Nivel LT: al igual que el nivel T, pero agrega datos VRI (información relacionada con la verificación) al DSS (Document Security Store), como respuestas OCSP o CRL y todos los certificados de la cadena de certificados, desde el certificado de usuario hasta el certificado de CA raíz. En resumen, este perfil permite validar la firma de un documento, incluso después de un largo período de tiempo, cuando el entorno de firma (por ejemplo, firma de la Autoridad de Certificación) ya no está disponible. El nivel LT se recomienda para las firmas electrónicas avanzadas, sin embargo, las leyes nacionales deben verificarse caso por caso.

iv. Nivel LTV: al igual que el Nivel LT, pero agrega una marca de tiempo de documento y datos VRI para la TSA (Autoridad de sellado de tiempo) al DSS. Se podrá validar la firma de un documento firmado en nivel LTV, más allá de cualquier evento que pueda limitar su validez. Este es el perfil que se ajusta a las regulaciones de eIDAS y respalda los requisitos que la normativa presente y futura pueda imponer.

Para el cumplimiento del nivel LTV, se deben cumplir los requisitos de los niveles B, L y LT además de los propios requisitos de dicho nivel. Las firmas que se ajustan al nivel LTV deben tener al menos un sello de tiempo del documento aplicado a su perfil. Antes de que el atributo de sello de tiempo del documento se genere e incorpore al perfil de firma, se debe incluir todo el material de validación que se requiere para la verificación de la firma. Este material incluye todos los certificados y la información de estado de OCSP o CRL perteneciente a esos certificados.

Este perfil incorporará al documento almacenado un Diccionario de Almacén de Seguridad del Documento, que incorporará la información adjunta a un documento PDF relacionada con su seguridad, incluida la información relacionada con la validación (VRI: referencias indirectas a los datos de validación utilizados para validar una firma específica) y referencias indirectas a los valores de los datos de validación para todas las firmas (datos que pueden ser utilizados por un verificador de firmas electrónicas para determinar que la firma es válida –por ejemplo, jerarquía de certificados, CRL, respuestas OCSP–).

La estructura de un PDF al que se ha aplicado LTV se ilustra en la siguiente figura:



En la imagen superior se observa un proceso por el cual, sobre un documento firmado (izquierda) con su sellado de tiempo, se aplica un proceso, mediante la incorporación de una nueva firma que incorpore un nuevo sellado de tiempo, y permita su comprobación posterior, más allá del final de la validez de la primera firma (derecha).

Esta estructura del documento firmado con Nivel LTV, permite sucesivos sellados de tiempo para favorecer que la documentación sea verificable a lo largo del tiempo, mediante procesos de resellado.

Una vez definidos los niveles que contempla el formato PAdES, se establecen los siguientes criterios:

- En el ámbito del Ayuntamiento, el formato de firma electrónica avanzada será nivel LTV (*Long Term Validation* o validación a largo plazo), e incluye documentos PDF firmados digitalmente que se almacenan durante largos períodos de tiempo.

  Por tanto, en los procesos de firma en que los usuarios del entorno municipal realicen firmas electrónicas sobre documentos PDF en el ámbito de los aplicativos municipales (plataforma de gestión integral), el acto de firma electrónica del propio documento implicará, de forma automatizada, la asociación del resto de atributos, incluyendo toda la jerarquía de certificados (intermedios y raíz) y el posterior sellado de tiempo (TSA) incluyendo su jerarquía así como la constancia de la validación de la firma.

- En la presentación de solicitudes a través del registro electrónico mediante firma electrónica por parte de la ciudadanía, el formato que se obtendrá de la transacción será un documento XML firmado, como resumen de los datos cubiertos, en el formulario correspondiente es XAdES-LT (nivel básico, para recoger firma en el

lado del cliente), recibiendo el resto de documentos adjuntos un sello mediante Actuación administrativa automatizada, con sellado de tiempo del acto de firma (PAdES-LTV).

- En el caso de utilización de Factura Electrónica, se admitirán las firmas XAdES enveloped, de acuerdo con el formato Facturae regulado en la Orden PRE/2971/2007; es decir, la firma se considera un campo más a añadir en el documento de factura. El formato será XAdES LT.
- En materia de archivo electrónico, atendiendo a lo que se disponga en la Política de Gestión Documental del Ayuntamiento cuando un expediente haya finalizado, transcurrido el plazo para ser remitido al Archivo Municipal definido por la Serie Documental correspondiente del cuadro de clasificación del Ayuntamiento, se remitirán:
  - Documentos aportados bien en presentación electrónica o bien incorporados mediante digitalización certificada de los documentos en papel aportados presencialmente, que llegarán en formato PAdES-LTV, mediante la aplicación de un sello electrónico más sellado de tiempo, a través de la figurad de la Actuación administrativa automatizada.
  - Documentos electrónicos generados y firmados en la plataforma de gestión integral municipal, también en formato PAdES-LTV.

  En ambos casos, los documentos remitidos al archivo tendrán asegurada la verificación de las firmas que sobre los mismos se hubiesen realizado. Se definirá la operativa, de acuerdo a la Política de Gestión Documental del Ayuntamiento, que será aprobada por resolución de Alcaldía, para aquellos documentos y anejos sobre los que en el momento del traslado al Archivo no figure ninguna firma o sello alguno, que a dichos documentos se aplicarán procesos de sellado en formato PAdES-LTV, al menos.

9.5 Firma electrónica a través de acreditación de la identidad cuando acredite la voluntad y consentimiento

Se establecen los siguientes sistemas de acreditación de la identidad de evidencias de la voluntad de firma:

i. En determinados procedimientos en los que las personas interesadas se correspondan con sujetos no obligados a relacionarse electrónicamente con la administración municipal se aplicará una combinación del tipo de firma basado en la voluntad de identificación más la voluntad de firma, incorporando un sello digital para aplicar la figura de actuación administrativa automatizada del subproceso de registro de solicitudes presentadas.

   Para ello se aplicará la identificación de la persona y la plasmación de su voluntad de firma, a través de evidencias electrónicas que cuentan con un registro previo en ejercicio de las potestades, prerrogativas y competencias municipales previstas en normas con rango legal o su correspondiente desarrollo reglamentario.

ii. En este apartado se contempla igualmente la utilización de la tarjeta ciudadana exclusivamente para su utilización por los sujetos no obligados, de acuerdo con la regulación prevista en el artículo 14 de Ley 39/2015, como sistema de identificación firma en tanto en cuanto se vaya sustituyendo por el sistema Cl@ve.

9.6 Firma con la plataforma Cl@ve

Este será un sistema específico de firma electrónica avanzada para los documentos electrónicos que firme electrónicamente un tercero a través de la plataforma Cl@ve de la Secretaría General de Administración Digital de la Administración General del Estado.

El proceso de firma se realiza de la siguiente manera:

i. La persona deberá identificarse en la Sede Electrónica del Ayuntamiento, para lo que se validará en la plataforma Cl@ve con certificado digital o con alguno de los sistemas previstos para esta plataforma: Cl@ve PIN, Cl@ve permanente, etc.

ii. Cumplimentará el formulario a firmar y pulsará el botón de firma (incluyendo los datos y adjuntos pertinentes). Esta acción redirigirá a la plataforma Cl@ve. Se generará una evidencia (XML) firmada por MINHAP (firma primaria), donde hay información sobre esta segunda identificación. Esta evidencia se incorporará a la anotación que se genere en el Registro del Ayuntamiento de Gijón y quedará vinculada al resto de documentos presentados/generados.

iii. Acto seguido, sobre la documentación presentada, se realizará una copia electrónica mediante Actuación administrativa automatizada, aplicando un sello electrónico sobre el conjunto de documentos.

Por lo tanto, la validez jurídica de la firma electrónica a través de Cl@ve está vinculada al documento y fundamentada en las evidencias del proceso de firma del firmante (firma primaria).

9.7 Validación de firma basada en un código electrónico de verificación (CEV)

El artículo 42.b de la Ley 40/2015 regula el uso del código seguro de verificación como medio de firma, vinculado a la Administración pública, órgano, organismo público o entidad de derecho público, y permite en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Este tipo de validación está dirigido a permitir la validación de documentos, que puedan ser remitidas a la ciudadanía, como pueden ser, por ejemplo, las notificaciones y comunicaciones que realiza el Ayuntamiento.

El Ayuntamiento ha previsto el uso de este sistema que permita la comprobación de la autenticidad e integridad de los documentos autenticados mediante CEV, que se encuentra publicado en www.gijon.es/cev, y que permite la validación de aquellos documentos generados en el ámbito del Ayuntamiento, así como aquellos documentos aportados por la ciudadanía a los cuales se incorpora un Código Electrónico de Verificación durante el proceso de copia electrónica. Dicho servicio, una vez introducido un Código Electrónico de Verificación válido, permitirá acceder al documento, así como la descarga del fichero en formato PDF, por lo que será posible utilizar las herramientas de verificación del visor de PDF utilizado por el usuario de este servicio, donde se podrán validar las firmas o sellos que en cada caso puedan existir sobre el documento.

La diferenciación entre copia auténtica de documento y copia de documento se determinará conforme al procedimiento previsto al efecto. La calificación como copia auténtica se realizará conforme a lo establecido en la política de gestión documental municipal y lo dispuesto en el artículo 27 de la Ley 39/2015.

9.8 Firma en otros aplicativos

En el entorno del Ayuntamiento, se podrá utilizar la firma electrónica para producir documentos firmados en aplicativos ofimáticos con carácter genérico, que permitan obtener ficheros confiables, acreditar identidad de la persona firmante y que el contenido de lo firmado no ha sido modificado con posterioridad, etc.

Este tipo de firma, aún siendo válido hacia el exterior, en el ámbito de funcionamiento de esta entidad, por defecto solo aplica el formato PAdES-BES de firma, ignorando el proceso de Sellado de Tiempo posterior, con lo que supone una diferencia importante respecto al funcionamiento de generación de documentos establecida en la Política de Gestión Documental y la presente Política de Firma. Además, los documentos generados por esta vía no podrán ser verificados mediante CEV, ya que su almacenamiento a priori, no se realizará en el gestor documental corporativo y al no ser firma PAdES LTV no se garantiza la conservación a largo plazo.

10. Validación de firmas o sellos

Para garantizar la validez jurídica de los documentos electrónicos firmados digitalmente, cualquier documento generado o aportado al Ayuntamiento puede ser susceptible de ser validado, a través de alguno de los siguientes sistemas:

i. La plataforma de validación de la Administración General del Estado, @firma, también por medio dela aplicación web VALIDe, como sistema de verificación de documentos firmados y certificados, a través de https://valide.redsara.es/ publicada por Ministerio de Política Territorial y Función Pública a través de la Secretaría General de Administración Digital.

ii. Para la validación de documentos PDF, cuando sea preciso, se utilizará la validación de firmas que incorporan las herramientas informáticas de visualización de tal extensión de fichero, como por ejemplo, el Adobe Acrobat Reader.

iii. Mediante el proceso de comprobación de las evidencias de voluntad de firma en el uso de otros medios de identificación y firma.

iv. Mediante comprobación en sede electrónica del organismo emisor del documento del Código Electrónico de Verificación.

v. Cualquier otro sistema que permita la correcta verificación de la validez de la firma electrónica, la identidad del firmante, y acreditar que el documento firmado no ha sido modificado en momento posterior a la firma practicada.

Se debe tener en cuenta, como ya se ha mencionado previamente, que se aplicará el proceso de digitalización a todo documento presentado en soporte papel ante el Registro del Ayuntamiento y el formato papel se devolverá en el ato. En el proceso de digitalización se aplicará Actuación administrativa automatizada, mediante sello electrónico, y posterior sellado de tiempo del acto de sellado. Dicho sello permite incorporar firma de carácter longevo (PAdES-LTV) sobre la documentación, lo que permite su validación más allá del fin de la validez del certificado empleado para firmarlo.

Acto seguido será almacenado en el Gestor Documental corporativo, se le asignará un Código Electrónico de Verificación y, dependiendo de su tipología, el sistema dejará constancia visible del CEV sobre el propio documento. Estos procesos se harán de acuerdo a lo establecido en la Política de Gestión Documental del Ayuntamiento.

11. Mantenimiento y preservación de las firmas y sellos electrónicos

La aplicación de una firma o sello electrónico sobre un documento otorga validez jurídica a los documentos electrónicos. Sin embargo, esta validez está sujeta a ciertos riesgos que se tienen que gestionar debidamente para garantizar una validez indefinida del documento en soporte electrónico. Estos riesgos son:

1. **Caducidad del certificado digital con el que se firma un documento electrónico.** Puede cuestionarse la validez de un documento electrónico a partir de la fecha de caducidad del certificado digital que se utilizó para la firma, que será posterior a la fecha de emisión del certificado digital o, en su caso, a la revocación del certificado. Para garantizar el momento en que se generó la firma electrónica, esta se puede completar con un sello de tiempo emitido por una Autoridad de Certificación. El Ayuntamiento utiliza firmas PAdES-LTV en documentos PDF, lo que incorpora sellado de tiempo y constancia de la validez. En el caso de ficheros con otro formato, actualmente se utiliza el formato XAdES-LT que cumple los requisitos legales de la Directiva para firma electrónica avanzada.

2. **Validez del certificado digital en el momento de generar la firma electrónica**. Puede cuestionarse la validez de un documento electrónico si no existe evidencia suficiente de que el certificado digital estaba vigente el día en que se generó la firma electrónica, es decir, de que no estaba revocado. Para guardar la evidencia de que un certificado digital, en la fecha de la firma, no estaba revocado, hay que completar la firma con la información de la validación de este aspecto contra la Autoridad de Certificación emisora del certificado. Al respecto, hay que tener en cuenta que las autoridades de certificación, en el momento en que un certificado digital caduca, eliminan las evidencias de revocación de su lista de revocados, por lo que si no se guarda la mencionada evidencia una vez caducado el certificado no existirá la certeza de que el certificado con el que se generó la firma no estaba revocado en aquel momento. Como se ha señalado, el Ayuntamiento, garantiza esta comprobación con el uso de PAdES-LTV.

3. **Obsolescencia tecnológica de la longitud de las claves criptográficas contenidas en el certificado digital y con las que se generan las firmas electrónicas.** Un documento electrónico puede dejar de tener validez jurídica a partir del momento en que se pone en entredicho la seguridad de las claves criptográficas con las que se firmó. Ante este escenario, habrá que tomar medidas para no continuar generando firmas con ese problema y asegurar las firmas anteriores que tuvieran ese problema. El Ayuntamiento, para dar respuesta a este problema de obsolescencia tecnológica de las claves criptográficas, procederá a generar certificados de mayor longitud de claves y utilizar algoritmos de *hash* más actualizados, y generar sucesivas refirmas a partir de firmas que permitan incorporar estos sellos de tiempo. En el caso del Ayuntamiento, la aplicación del formato PAdES-LTV resuelve esta problemática.

11.1 Resellado de firmas electrónicas

El objetivo principal de esta función es garantizar la firma electrónica a lo largo del tiempo. El proceso de resellado consiste en renovar el sello de fecha y hora añadiendo un nuevo eslabón a la cadena de evidencias electrónicas en la firma electrónica del documento.

Para poder aplicar este proceso, es necesario que las firmas estén en un formato que permita añadir estas evidencias de tiempos. Estas son las firmas del tipo XAdES-LT, CAdES-A o PAdES-LTV. En el supuesto de que una firma no esté en estos formatos, previamente al resellado se debe completar la firma, que en cualquier caso deberá estar como mínimo en un formato AdES-T, en uno de los formatos anteriormente definidos.

Partiremos, tal y como se ha comentado en el punto anterior, del supuesto de que los documentos tengan ya una firma de tipo longevo como ya hemos mencionado para el Ayuntamiento, que estará en formato PAdES-LTV. Sobre estas firmas se incorporará un nuevo sello de tiempo, puesto que su estructura permite esta posibilidad. Este nuevo sello de tiempo estará ya generado con un certificado reciente, con un periodo de validez superior al actual en la firma a resellar, con una longitud de clave que no estará comprometida y con un algoritmo que no esté sujeto a la obsolescencia criptográfica del algoritmo en el momento de su emisión.

Para el caso de las firmas a través de acreditación de la identidad y de evidencias de la voluntad de firma solo se realizará el resellado de la firma secundaria.

En definitiva, el resellado consiste, pues, en mantener la validez de la firma incorporando nuevo material criptográfico, concretamente sellos de fecha y hora, a la propia estructura de la firma electrónica.

11.2 Mantenimiento de la validez jurídica de las firmas vigentes

El proceso de mantenimiento de las firmas electrónicas dentro del Ayuntamiento, para el caso de aquellos documentos que sea necesario preservar, será el siguiente:

a. Como ya se ha mencionado, en el caso de firmas generadas en el entorno del Ayuntamiento, mediante las herramientas habilitadas a tal fin (ERP-plataforma de gestión integrada: Expediente Electrónico y Firma Electrónica) se procederá en fase de tramitación a la generación de las firmas electrónicas ya en formato preservable, es decir, en formato de firma de archivo. Para documentos XML, se deberán de transformar a formato XAdES-LT, como podría ser el caso del foliado electrónico del expediente, y para los documentos PDF se generará una firma electrónica en formato PAdES-LTV.
b. Como ya se ha indicado, en el caso de firmas que provengan de plataformas externas, como pueden ser otras Administraciones, herramientas de cliente, etc., se procederá en su caso a resellar la firma para completar la firma. Este resellado se realizará previo cierre y foliado del expediente. Para documentos XML, se deberán transformar a formato XAdES-LT, como podría ser el caso del foliado electrónico del expediente, y para los documentos PDF se generará una firma electrónica en formato PAdES-LTV.
c. En aquellos casos en que no sea posible generar para algún documento una firma preservable, se procederá al foliado electrónico del expediente con un índice en formato XML con una firma que habrá de ser XAdES-LT, de forma que sea el propio foliado el que garantice la validez jurídica de la firma electrónica del documento.

Todas estas operativas descritas se realizarán de acuerdo de los procedimientos que establezca la Política de Gestión Documental del Ayuntamiento.

12. Casos de uso de firma electrónica del Ayuntamiento

Contenido	La tabla muestra los usos y aplicaciones más comunes de los medios de identificación y firma, a modo ilustrativo.		
	Firma electrónica de documento electrónico dentro del ERP – Sistema de firma electrónica del Ayuntamiento de Gijón	Copia electrónica de documentos en papel	Procesos de firma mediante Actuación Administrativa Automatizada
Descripción	Permite firmar electrónicamente documentos en soporte electrónico en cualquier momento de su ciclo de vida.	Permite la transformación de los documentos en formato papel en documentos electrónicos mediante copia electrónica de los mismos, aplicando la política de gestión documental.	Dentro del sistema de gestión municipal ERP (Expediente y Firma Electrónica) existen procesos de generación de documentos, que son aprobados mediante actuación administrativa automatizada.
Características	i. Se realiza firma dentro del entorno del sistema de firma municipal (ERP-plataforma de gestión integrada). ii. El original y la firma aplicada se incorporan al sistema. iii. Durante el proceso de firma, se validará contra el sistema @firma el certificado utilizado por el firmante. iv. Las evidencias de la validación se incorporarán a la firma *embedded*. v. La firma se produce sobre documentos ofimáticos, siendo el estándar de facto el formato Portable Document File (PDF) vi. Podrá hacerse firma simple o firma múltiple (una o más firmas, en paralelo o en cascada). vii. Por defecto, se aplica PAdES-LTV viii. Sobre los documentos generados dentro del ERP municipal, se plasmará un CEV, que permite la verificación del documento.	i. Consiste en firmar electrónicamente un documento digitalizado en formato PDF. ii. La firma aplicada dotará de integridad y autenticidad al documento, añadiéndole los metadatos de documento necesarios. iii. Durante el proceso de firma, se validará contra el sistema @firma el certificado utilizado por el firmante. iv. Se utiliza Actuación administrativa automatizada, mediante sello electrónico, identificando correctamente a la unidad responsable del proceso. v. Además se utilizará un sellado de tiempo que permita extender la validez jurídica del documento más allá de las evidencias del sello empleado. vi. Se recogerá una sola firma, por lo que será firma simple. vii. Por defecto se aplicará el formato PAdES-LTV. viii. El procedimiento se aprobará por resolución de la Alcaldía. ix. En este proceso de incorporación y digitalización, en función del tipo de documento aplicado, se le añadirá un CEV, que permite la verificación del documento.	i. Consiste en firmar electrónicamente un documento generado en el ERP en formato PDF/XML. ii. La firma aplicada dotará de integridad y autenticidad al documento, añadiéndole los metadatos de documento necesarios. iii. Se utiliza Actuación administrativa automatizada, mediante sello electrónico, identificando correctamente a la unidad responsable del proceso. iv. Durante el proceso de firma, se validará contra el sistema @firma el certificado utilizado por el firmante. v. Además, se utilizará un sellado de tiempo que permita extender la validez jurídica del documento más allá de las evidencias del sello empleado. vi. Puede llevar firma simple o firma múltiple, por poder albergar una firma o varias, realizadas en paralelo sobre el documento. vii. Por defecto, se aplicará PAdES-LTV sobre los ficheros PDF y XAdES-LT sobre los ficheros XML. viii. Sobre los documentos generados dentro del ERP municipal, se plasmará un CEV, que permite la verificación del documento. ix. El procedimiento será aprobado por resolución de Alcaldía.
Tipo de firma	Clase de firma: Reconocida Tipo de certificado: certificado de empleado público/pertenencia a entidad (descritos en el punto 5.3 a) Formatos: PAdES-LTV Sello de tiempo: Sí Tipo de firma: Enveloped	Clase de firma: Reconocida Tipo de Certificado: sello electrónico de órgano. (descritos en el punto 5.3 c) Formatos: PAdES-LTV Sello de tiempo: Sí Tipo de firma: Enveloped	Clase de firma: Reconocida Tipo de Certificado: sello electrónico de órgano. (descritos en el punto 5.3 c) Formatos: PAdES-LTV, XAdES-LT Sello de tiempo: Sí Tipo de firma: Enveloped/ Enveloping

Datos del expediente:	Asunto:
24430C/2020 **Impulso del procedimiento electrónico** Datos del documento: Tramitador: Emisor: **01008485** Fecha Emisor: **24/06/2020**	**Puesta en marcha de la sede electrónica municipal**

	Incorporación de documentación firmada por terceras personas	**Presentación de solicitudes a través del Registro Electrónico/Presentación de facturas a través de FACe o Registro Electrónico de Facturas**	**Resellado de documentos para ampliación de la validez de las evidencias y extensión del plazo de validez de la firma**
Descripción	En caso de que una persona interesada presente documentación firmada electrónicamente, ante los registros electrónicos municipales	En caso de que una persona interesada presente solicitud firmada electrónicamente, ante los registros electrónicos municipales.	Proceso de resellado sobre la documentación albergada en los sistemas municipales ERP de expediente electrónico para ampliar validez de los mismos en el tiempo o su traslado a Archivo Electrónico.
Características	i. Se validan las firmas electrónicas del documento. ii. Se incorporan a la anotación de registro electrónico, y son susceptibles de ser incorporadas en un paso posterior al ERP-plataforma de gestión integrada. iii. Los documentos aportados por esta vía podrán ser verificados desde el ERP-plataforma de gestión integrada, que permitirá consultar las firmas presentes sobre el documento o bien desde el visor de documentos PDF, que permitirá su validación.	i. Se va a validar la firma electrónica utilizada como sistema de identificación y en el acto de firma contra @firma. ii. La firma de la solicitud se plasma sobre documento XML generado a partir del formulario de registro de entrada cubierto la persona interesada. iii. En el caso de factura electrónica, el documento se descarga en el ERP-plataforma de gestión integrada desde el portal FACe.	i. Consiste en resellar electrónicamente un documento almacenado en el ERP-plataforma de gestión integrada en formato PDF/XML. ii. La firma aplicada ampliará el periodo de validez de los documentos sellados. iii. Se utiliza Actuación administrativa automatizada, mediante sello electrónico, identificando correctamente a la unidad responsable del proceso. iv. Durante el proceso de firma, se validará contra el sistema @firma el certificado utilizado por el firmante. v. Además, se utilizará un sellado de tiempo que permita extender la validez jurídica del documento más allá de las evidencias del sello empleado. vi. Llevará firma múltiple, albergando varias firmas realizadas en cascada sobre el documento. vii. Por defecto, se aplicará resellado sobre documentos PAdES-LTV sobre los ficheros PDF y XAdES-LT sobre los ficheros XML.
Tipo de firma	Clase de firma: Avanzada o Reconocida, en función del tipo de certificado utilizado. Tipo de certificado: Certificado de persona física/Representante de persona jurídica/Pertenencia a entidad/Sello electrónico de los contemplados en la Lista de Confianza de Prestadores de Servicios de Certificación. Formatos: PAdES-T, PAdES-LT Sello de tiempo: Sí Tipo de firma: Enveloped	Clase de firma: Reconocida. Tipo de certificado: Certificado de persona física/Representante de persona jurídica/Pertenencia a entidad de los contemplados en la Lista de Confianza de Prestadores de Servicios de Certificación. Formatos: XAdES-LT Sello de tiempo: No Tipo de firma: Enveloped En caso de facturas electrónicas se atenderá a lo dispuesto en el estándar Facturae.	Clase de firma: Reconocida. Tipo de certificado: Sello Electrónico de órgano. (descritos en el punto 5.3 c) Formatos: PAdES-LTV, XAdES-LT Sello de tiempo: Sí Tipo de firma: Enveloped

	Identificación ciudadana mediante comparecencia en sede para acceso a notificación electrónica o realización de trámites	Firma electrónica con identificación y evidencia electrónica de un documento electrónico (personal funcionario habilitado)	Firma electrónica con identificación y evidencia electrónica de un documento electrónico
Descripción	En caso de que una persona interesada comparezca en la sede electrónica municipal.	En aquellos supuestos en los que alguna de las personas interesadas en los procedimientos administrativos no disponga de los medios electrónicos necesarios, consiguiendo con ello la identificación y firma electrónica de ésta en el procedimiento administrativo	En aquellos supuestos en los que la identificación de la persona y la plasmación de su voluntad de firma, a través de evidencias electrónicas que cuentan con un registro previo fruto de las potestades, prerrogativas y competencias municipales previstas en normas con rango legal o su correspondiente desarrollo reglamentario
Características	i. La persona interesada se identifica para acceder a distintos trámites disponibles. ii. Se va a validar las firma electrónica que se utiliza para identificarse, en cuanto a no estar revocada y su vigencia. iii. Una vez procesado el acceso, se identifica a la persona interesada, y si es preciso, los datos de identificación se muestran en el formulario de registro, o al menos se muestran en el detalle de la Carpeta Ciudadana en el acceso a notificación electrónica.	i. La persona interesada se identifica preferentemente por medios electrónicos mostrando sus títulos identificativos (NIF, NIE, Pasaporte, Carnet de conducir) y, en supuestos excepcionales, con cita previa, en presencial en las oficinas de asistencia en materia de registro. ii. El personal funcionario habilitado nombrado al efecto, una vez realizada la identificación descrita en el apartado anterior cumplimentará la solicitud formulada y la firmará electrónicamente. iii. La solicitud y documentación relacionada se firma electrónicamente por empleado público municipal.	i. La persona interesada accede al documento/formulario electrónico. ii. La persona interesada cumplimenta el documento/formulario electrónico con información que permite contrastar y verificar evidencias electrónicas que cuentan con un registro previo. iii. Una vez cubierto el documento/formulario y presentado en el registro electrónico, momento en que se aplica automáticamente un sello de órgano se realiza una comprobación sobre la confirmación y validación de las evidencias electrónicas. Esta confirmación y validación se podrá realizar a través de la figura de actuación administrativa automatizada. iv. La documentación adjunta recibe un sellado electrónico mediante actuación administrativa automatizada en el momento de su registro junto con el formulario o documento de solicitud.
Tipo de firma	Clase de firma: Avanzada o Cualificada, en función del tipo de certificado utilizado. Tipo de certificado: Certificado de persona física/Representante de persona jurídica/Pertenencia a entidad/Sello electrónico de los contemplados en la Lista de Confianza de Prestadores de Servicios de Certificación. Se admite el uso de Cl@ve Este proceso de acceso e identificación no deja constancia en un documento en sí mismo, solo queda en el registro del sistema. En el caso de la notificación, es la acción posterior la que generará un Justificante del acceso en formato XAdES-LT.	Clase de firma: Reconocida. Tipo de certificado: Certificado de empleado público de los contemplados en la Lista de Confianza de Prestadores de Servicios de Certificación. Formatos: XAdES-LT Sello de tiempo: No Tipo de firma: Enveloped	Clase de firma: No se incrusta firma sobre los documentos. El sellado posterior se corresponde al caso de uso “Copia electrónica de documentos en papel”

13. Glosario de términos

Por la particularidad de los conceptos del presente documento, se considera necesario incluir un glosario de términos, para facilitar la comprensión de la Política de Firma, sellos electrónicos, certificados y otros sistemas de identificación del Ayuntamiento de Gijón.

a) **Casos de uso de la firma electrónica:** en este documento nos referimos a los casos de uso de la firma electrónica, a los escenarios posibles de generación de documentos electrónicos firmados. Para cada caso de uso se identificarán los sistemas de firma posibles, los formatos de firma electrónica, los posibles niveles de firma, la normativa de firma electrónica a aplicar, etc. En el caso del Ayuntamiento, se definen los casos de uso diferentes: firma electrónica de un documento electrónico, copia electrónica de documentos en papel, copia auténtica de un documento electrónico firmado electrónicamente, procesos de firma mediante actuación administrativa automatizada e incorporación de documentos firmados digitalmente por un tercero.

b) **Clases de firma electrónica:** en este documento nos referiremos a las clases, a la validez jurídica de la firma electrónica, según se define en la Ley 59/2003, de Firma Electrónica: firma simple u ordinaria, avanzada y reconocida o cualificada.

c) **Evidencias electrónicas:** conjunto de información en formato electrónico que permite aportar información a un acto, y que puede ser utilizado como prueba judicial en el caso de que haya una disputa sobre este acto. En el caso del Ayuntamiento, se guardarán en los sistemas de información corporativos o en la plataforma que gestione el servicio.

d) **Formato de firma electrónica:** forma en la que se codifican las firmas electrónicas. Los formatos utilizados son XAdES, CAdES y PAdES.

e) **Nivel de firma:** con este nombre nos referiremos a si el documento tiene una única firma o múltiples firmas y, en este caso, si se generan en paralelo o en cascada.

f) **Estándares técnicos de firma electrónica:** documentos que detallan las normas relativas a la firma electrónica, organizadas en torno a los conceptos de generación y validación de firma, en un contexto particular (contractual, jurídico, legal...), definiendo las reglas y obligaciones de todos los actores involucrados en este proceso. El objetivo de este proceso es determinar la validez de la firma electrónica para los distintos tipos de transacción.

g) **Sistema de firma:** con este nombre nos referimos a si la firma electrónica de un documento se ha realizado con un certificado digital del firmante o con un sistema de identificación más evidencia electrónica del acto de la firma.

h) **Tipo de firma:** forma en la que se relaciona la firma electrónica con el documento firmado, bien sea dentro del mismo documento, como un documento aparte o dentro de estructuras XML.