POLÍTICA DE FIRMA ELECTRÓNICA

Empresa Metropolitana de Abastecimiento y Saneamiento de Aguas de Sevilla

ÍNDICE

1. POLÍTICA DE FIRMA ELECTRÓNICA

1.1. Alcance de la política

Esta política de firma es una aplicación de la política de firma de la AGE en su última versión en vigor, en el marco de EMASESA y los sistemas de información que soportan procesos de identificación y firma electrónica.

Dentro de esta política se desarrolla para EMASESA los procesos de identificación admitidos, los procesos de firma criptográfica y no-criptográfica definidos, así como los procesos de retención y mantenimiento de la información válida para el calendario de conservación de EMASESA de gestión documental.

1.2. Datos identificativos de la política

Se usará como identificador de la política el ya definido por la AGE a tal efecto, con el OID 2.16.724.1.3.1.1.2.x.y, o el urn:oid: 2.16.724.1.3.1.1.2.x.y Donde (x.y) sirve para distinguir las versiones sucesivas de la misma.

Las firmas por tanto realizadas en EMASESA, deben contener esta política definida con los identificadores aplicados a tal efecto sobre las firmas realizadas.

1.3. Actores y definiciones previas

A lo largo de los siguientes puntos se describirán procesos y actores que participan en los mismos. Es necesario por tanto conocer la siguiente relación de conceptos:

Firmante: Persona que dispone de un dispositivo software o hardware de generación de firmas que actúa en nombre o propio, trabajador de la entidad o como representante legal de la misma.

Verificador: Persona o entidad que comprueba la validez de la firma realizada por el actor anterior en base a la política de firma. El verificador puede ser un tercero de confianza entre dos partes.

Prestador de certificados de firma electrónica: Persona o entidad que emite certificados electrónicos.

Emisor de política de firma: Entidad que se encarga de gestionar y mantener la política de firma, así como velar por el cumplimiento de la misma en la organización.

Autenticación: Proceso mediante el cual una persona o una entidad se identifica como tal ante un tercero. Los mecanismos más comunes de identificación por secreto compartido (usuario/clave), certificado electrónico o mediante un proveedor de identidad de confianza externo, por ejemplo, el sistema Cl@ve del Ministerio.

Clave de un solo uso o OTP: Elemento de seguridad normalmente usado como segundo factor en procesos de autenticación, para confirmar la identidad de una persona o entidad, mediante el envío de una clave de un solo uso a un dispositivo, generalmente un móvil vía SMS, un token de claves aleatorias rotativas o a una cuenta de correo confirmada previamente de dicho usuario.

Código Seguro de Verificación o CSV: Es un código único que identifica a un documento electrónico en diferentes ámbitos que predica su autenticidad, y que por lo general, se puede comprobar su integridad en la sede electrónica de la entidad.

Firma electrónica: Proceso criptográfico realizado con un certificado electrónico para asegurar la autenticidad, integridad y el no repudio de la firma de un documento.

Firma CSV o no-criptográfica: Sistema de firma electrónica vinculada a la Administración Pública, órgano o entidad, y en su caso, a la persona firmante del documento, que permite comprobar la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Sellado de tiempo: Proceso técnico mediante el cual se extiende la vigencia de la firma más allá de la menor fecha de caducidad de los certificados electrónicos que han participado de un proceso de firma. Al aplicar un sello de tiempo a una firma, la caducidad de la misma viene marcada por la fecha de caducidad del certificado usado en el sello de tiempo. Es también conocida como Firma Longeva.

Resellado: Proceso técnico similar al anterior donde se aplica un nuevo sello de tiempo a una firma ya existente para que se amplíe nuevamente en tiempo a la validez del nuevo certificado usado para el sellado de tiempo.

Calendario de conservación: Será el tiempo que se ha de conservar vigentes las firmas electrónicas de un documento y por tanto se han de realizar los procesos de resellados necesarios para garantizar la validez de la firma. Generalmente este periodo vendrá definido de forma general por la tipología documental y los cuadros de clasificación, aunque puede tener excepciones a la misma por la naturaleza del escrito en sí.

1.3.1. Usos de la firma electrónica

Los objetivos en el uso de certificados de firma electrónica son los siguientes:

- En la firma electrónica de transmisión de datos, como herramienta para proporcionar seguridad al intercambio, garantizando la autenticación de los actores involucrados en el proceso, la integridad del contenido del mensaje de datos enviado y el no repudio de los mensajes en una comunicación telemática.
- En la firma de documentos y contenidos electrónicos, como herramienta para garantizar la autenticidad, integridad y no repudio de los mismos, con independencia de que forme parte de una transmisión de datos.

Los certificados electrónicos de firma podrán ser utilizados, por parte de los ciudadanos y empleados públicos:

a) Como medio de autenticación de la identidad, ya que el Certificado de Autenticación (Digital Signature) asegura que la comunicación electrónica se realiza con la persona que dice que es. El titular podrá, a través de su certificado, acreditar su identidad frente a cualquiera, ya que se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo.

b) Como medio de firma electrónica de documentos, ya que mediante la utilización del Certificado de Firma (nonRepudition), el receptor de un documento firmado electrónicamente puede verificar la autenticidad de esa firma, pudiendo de esta forma demostrar la identidad del firmante sin que éste pueda repudiarlo.

c) Como medio de certificación de Integridad de un documento, ya que permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación.

1.4. Autenticación

1. Los sistemas admitidos para la identificación de usuarios son:
   - Certificado electrónico cualificado, ya sea personal, de pertenencia a entidad o representación.
   - Identificación en proveedores de identidad de confianza a nivel de la AGE, como por ejemplo Cl@ve.
   - Usuario/Clave o sistemas de secreto compartido implementados en EMASESA y con previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública.
2. En el caso de identificación con usuario/clave o secreto compartido es necesario implementar alguno de los siguientes mecanismos de seguridad adicional en los primeros accesos correctos desde un nuevo equipo:

- Disponer de un captcha o un control máximo de intentos fallidos de identificación, bloqueando o imposibilitando el acceso por un tiempo incremental al número de intentos.
- Segundo factor en la identificación, con el envío de un OTP a una cuenta de correo del usuario o bien a un número de móvil confirmados previamente en el proceso de alta a los sistemas de los usuarios.

3. En ningún caso las claves de los usuarios estarán almacenadas como texto plano en los sistemas de información, sino que se guardará el hash calculado mediante algoritmo de resumen SHA2, SHA3 o HMAC. Los algoritmos SHA1 o MD5 están ya descatalogados por el ENS.
4. La identificación mediante certificado, debe comprobar que el certificado es válido en ese instante de tiempo contra su prestador de certificados electrónicos y esté dentro de la tipología de certificados cualificados homologados por el Ministerio de Industria. Se recomienda un segundo factor adicional, como en el caso anterior, en el primer acceso desde un determinado equipo. Es obligatorio para entornos que según el ENS requieran nivel medio o alto de seguridad.
5. En la identificación contra un proveedor de identidad de confianza para EMASESA, es recomendable disponer alguno de los mecanismos de segundo factor indicados en usuario/clave como medida adicional de seguridad si el propio sistema no dispone de dicho mecanismo. Aplica solo en el primer acceso desde un equipo, para no sobrecarga al usuario final.

1.5. Firma electrónica

1. Las firmas electrónicas, ya sean avanzadas o cualificadas, siempre se harán con certificados cualificados homologados por el Ministerio de Industria, tanto del personal de EMASESA, como personas o entidades ajenas a la organización, pero participantes en procesos de firma en la misma.
2. Para el personal interno, el uso preferente de certificados serán los emitidos a tal efecto con pertenencia a EMASESA o aquellos de representación legal de la misma. El uso de certificados personales debe ser excepcional y solo motivados por problemas técnicos puntuales o por causa justificada.
3. Los formatos de firma, por orden de preferencia deben ser:
   - PADES, para firma de documentos PDF de menos de 10MB.
   - XADES-Enveloping o Internally Detached, para firma de documentos no PDF de menos de 10MB.
   - CADES, firma para ficheros de cualquier tipo de más de 10MB.
   - XADES-Manifest, firma de ficheros de más de 10MB, sujeto a la próxima política de firma de la AGE, si bien ya se puede usar o implementar en los sistemas de información que se estime oportuno. Es el formato sucesor al CADES.
4. Los algoritmos de resumen deben ser al menos SHA-256 o superior.
5. Toda firma electrónica debe pasar por un proceso de verificación y sellado de tiempo, para garantizar la vigencia de la firma al menos más allá de la validez de los certificados involucrados.

1.6. Firma CSV o No-Criptográfica

1. Para poder iniciar una Firma CSV o No-criptográfica un usuario, ya sea interno o externo, deberá identificarse por alguno de los mecanismos de autenticación mencionados justo antes de iniciar el proceso de firma, incluso aunque el usuario ya esté identificado previamente en el sistema. Es un requisito necesario para acreditar la identidad de la persona en el proceso de firma.

2. El usuario debe poder verificar la documentación que va a firmar antes de tomar la decisión. Para el ello el interesado debe poder consultar la documentación en un formato legible, y a ser posible, en el mismo formato que el justificante que al final se le entregará al usuario.
3. Se ha de manifestar de forma explícita el consentimiento y expresión de la voluntad de firma la documentación. Para ello los sistemas que lo implementen deberán mostrar una casilla con el texto “Declaro que son ciertos los datos a firmar/muestro mi conformidad con el contenido del documento y confirmo mi voluntad de firmar” que el interesado deberá marcar, y el botón de firmar no se le ofrezca hasta que haya marcado dicha casilla.
4. Para garantizar el no repudio de la firma csv o no-criptográfica, el sistema deberá vincular el acto de voluntad y los datos firmados con el usuario. Para ello el sistema debe generar un justificante de firma no-criptográfica con la siguiente información:
    a. Fecha y hora de la autenticación.
    b. Nombre y apellidos del usuario.
    c. NIF/NIE del usuario.
    d. Mecanismo de autenticación usado (usuario/clave, certificado o proveedor idp).
    e. En el caso que el mecanismo de autenticación devuelve identificadores o comprobantes de la operación, incluir al justificante. En caso contrario, incluir un identificador de transacción propio a la aplicación.
    f. Fecha y hora de la firma.
    g. Algoritmo resumen usado y valor para el documento a firmar por el usuario.
    h. CSV o elemento de trazabilidad en el gestor documental.
    i. Dirección IP e información del navegador usado por el usuario en el instante de la firma (user-agent).

       Esta información deberá ser recogida en un documento, y este firmado y sellado mediante un certificado de entidad de EMASESA.
5. Los documentos a firmar por el usuario, serán a su vez firmados con el certificado cualificado de entidad de EMASESA y se le aplicará sellado de tiempo. Deberán aplicarse las políticas de retención que se definan para el tipo documental del cuadro de clasificación correspondiente.
6. El justificante de firma se le debe ofrecer al usuario junto al documento firmado para que pueda disponer de una evidencia del proceso en el que ha participado.

1.7. Medios para realización de firma

1. La firma electrónica de documentación se deberá realizar preferentemente desde los medios o sistemas de información que provea EMASESA para la realización de las mismas. De esta forma, se tiene controlado los certificados que se deben usar y los medios, ya sea equipos de escritorio o dispositivos móviles, homologados por la organización para dicha función.
2. En el caso de que la firma de un documento no proceda de un sistema de información existente, sino que se ha generado directamente desde una herramienta ofimática, se deberá usar preferente Portafirmas como herramienta genérica de firma de documentos, usando para ello la funcionalidad de redacción que incluye la herramienta y adjuntando la documentación en la medida de lo posible en formato PDF.
3. Se puede usar servicios de firma en la nube como Clave-Firma y Fire del Ministerio, o soluciones de proveedores de emisión de certificados como CloudId (FNMT), IvSign (Camerfirma), Giltza (Izenpe), etc; que estén homologados y generen formatos de firma que cumplan los requisitos definidos anteriormente.

4. No deberá usarse para hacer firmas en local herramientas como Adobe o similares, salvo por problemas técnicos puntuales o por causa justificada. El objetivo buscado es la correcta conservación de las firmas, así como poder garantizar la validez de las mismas por el plazo de tiempo que sea necesario, requisito que no se alcanzará si la documentación queda fuera de la custodia y control de los sistemas de EMASESA.

1.8. Custodia y resellado

1. Las firmas como los documentos serán custodiados en el gestor documental SIGD de EMASESA, junto con los metadatos asociados a su tipo y serie documental de forma preferente a otros sistemas de almacenamiento. Solo en sistemas que ya no tengan mantenimiento o no haya una fácil integración con el SIGD se permitirá la custodia local de la información de firma.

2. En función al calendario de conservación de EMASESA de gestión documental para dicho documento, las firmas han de ser elevadas al formato de archivado, ADES-A o LTA-Level, a efectos de permitir el resellado periódico de las mismas.

2. POLÍTICA DE VALIDACIÓN DE FIRMA ELECTRÓNICA

Se aplicará las mismas normas técnicas definidas para la validación de la firma que la política de la AGE en vigor.

2.1. Vigencia

El periodo de validez de esta política de firma se define a partir de la fecha de publicación en la Sede Electrónica de EMASESA y mientras no sea sustituida por una nueva versión, siendo aplicable a los documentos y procesos realizados durante ese periodo de tiempo.

2.2. Periodo de adaptación

Los sistemas existentes en EMASESA que no se adecuen a esta política tienen dos años para adaptarse a la misma a partir de la fecha de publicación de esta política por los canales definidos para ello.

Solo están exentos de cumplimiento aquellos sistemas sin mantenimiento o bien estén próximos a ser sustituidos por otros que sí implementan esta política.

2.3. Mecanismos de validación de firma electrónica

Para la validación de la documentación firmada por EMASESA se ofrece de los siguientes mecanismos:

- Portal Valide de la AGE, que permite la verificación de documentación firmada de cualquier administración.
- Portal Verifirma de EMASESA, que permite la verificación de documentación firmada y asociada a un CSV mediante un informe de firma. En el propio pie de firma del informe viene recogida la URL donde está publicado este portal.
- Verificación en la sede electrónica de EMASESA, se está trabajando en una nueva versión de la sede que sustituye a la actual y que permitirá la verificación de documentación firmada y asociada a un CSV mediante un informe de firma. Mientras no se dispone de esta nueva versión se ha de emplear los dos métodos anteriores mencionados.

3. CONSIDERACIONES

3.1. Marco legal de aplicación

La Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, nace como complemento del Reglamento eIDAS para eliminar irregularidades y equiparar aspectos de los servicios electrónicos de confianza.

Además, esta ley recoge las sanciones en caso de incumplimiento de algunos de los preceptos de la Ley y del Reglamento eIDAS y los clasifica en leves, graves y muy graves.

Por su parte, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales recoge el deber de confidencialidad:

"los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad".

Asimismo, conviene incidir en el cumplimiento de las garantías básicas que envuelven a los sistemas de firma en virtud de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas – véase sus artículos 10, 11 y 14-. Hay que atender a las nuevas precisiones recogidas en el artículo 10.2 y siguientes, en virtud de la modificación según Real decreto- ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

Éstos regulan la materia aludida en el siguiente sentido:

Artículo 10. - Sistemas de firma admitidos por las Administraciones Públicas:

1. Los interesados 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.

2. En el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

> *a) Sistemas de firma electrónica cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".*
>
> *b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico expedidos por prestador incluido en la "Lista de confianza de prestadores de servicios de certificación".*
>
> *c) Cualquier otro sistema que las Administraciones Públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá*

de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todos los procedimientos en todos sus trámites, aun cuando adicionalmente se permita alguno de los previstos al amparo de lo dispuesto en la letra c).

3. En relación con los sistemas de firma previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

4. Cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

5. Cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma.

Artículo 11. - Uso de medios de identificación y firma en el procedimiento administrativo:

1. Con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo, será suficiente con que los interesados acrediten previamente su identidad a través de cualquiera de los medios de identificación previstos en esta Ley.

2. Las Administraciones Públicas sólo requerirán a los interesados 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.

Artículo 14. Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas.

1. Las personas físicas podrán elegir en todo momento si se comunican con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos o no, salvo que estén obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas. El medio elegido por la persona para comunicarse con las Administraciones Públicas podrá ser modificado por aquella en cualquier momento.

2. En todo caso, estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los siguientes sujetos:

a) Las personas jurídicas.

b) Las entidades sin personalidad jurídica.

c) Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones Públicas en ejercicio de dicha actividad profesional. En todo caso, dentro de este colectivo se entenderán incluidos los notarios y registradores de la propiedad y mercantiles.

d) Quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración.

e) Los empleados de las Administraciones Públicas para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado público, en la forma en que se determine reglamentariamente por cada Administración.

3. Reglamentariamente, las Administraciones podrán establecer la obligación de relacionarse con ellas a través de medios electrónicos para determinados procedimientos y para ciertos colectivos de personas físicas que por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

Tras esta aproximación, meramente referencial sobre la normativa básica a aplicar en nuestra política de firma, en aras a la brevedad, hemos de remitirnos a la normativa más específica, tanto desde el punto de vista técnico como jurídico, a la que se hace referencia en los dos puntos siguientes.

3.2. Referencias técnicas

Para el desarrollo del contenido se han tenido en cuenta las siguientes referencias técnicas:

- ETSI TS 101 733, v.1.6.3, v1.7.4 y v.1.8.1. Electronic Signatures and Infrastructures (SEI); CMS Advanced Electronic Signatures (CAdES).
- ETSI TS 101 903, v.1.2.2, v.1.3.2 y 1.4.1. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).
- ETSI TS 102 778, v 1.2.1. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview, Part 2: PAdES Basic
- Profile based on ISO 32000-1, Part 3: PAdES Enhanced - PAdES-BES and PAdESEPES Profiles; Part 4: Long-term validation.
- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
- ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- ETSI TS 101 861 V1.3.1 Time stamping profile.
- ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.
- ETSI TR 102 041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.
- ETSI TR 102 045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.
- ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.
- IETF RFC 2560, X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP.
- IETF RFC 3125, Electronic Signature Policies.
- IETF RFC 3161 actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 5652, RFC 4853 y RFC 3852, Cryptographic Message Syntax (CMS).
- ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".
- ETSI TS 103171 v.2.1.1., acorde a la Especificación Técnica:

http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf

3.3. Referencias legales

Para el desarrollo del contenido se han tenido en cuenta las siguientes referencias legales sobre las que versa o se apoya el presente documento:

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sellos Electrónicos y de Certificados de la Administración.
- 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.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Resolución de la Secretaría de Estado de Función Pública del 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.
- Real Decreto 203/2021, de 30 marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital, por la que se establecen las condiciones de uso de firma electrónica no criptográfica, en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos.
- Resolución de 3 de octubre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Catálogo de estándares.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de derechos digitales.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de propiedad intelectual.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Decisión de la Comisión Europea 130/2011, de 25 de febrero, que establece unos requisitos mínimos para el tratamiento transfronterizo de documentos firmados electrónicamente por las autoridades competentes bajo la Directiva 2006/123/CE, del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior.