POLÍTICA DE FIRMA Y SELLO ELECTRÓNICOS Y DE CERTIFICADOS DE LA ADMINISTRACIÓN

Guía de aplicación de la Norma Técnica de Interoperabilidad

2ª edición electrónica

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE FUNCIÓN PÚBLICA
SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

FICHA CATALOGRÁFICA

TÍTULO: Guía de aplicación de la Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y de certificados de la administración .

Elaboración y coordinación de contenidos: Secretaría General de Administración Digital (SGAD)

Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones

2ª edición electrónica: mayo de 2017

Disponible esta publicación en el Portal de Administración Electrónica (PAe):
http://administracionelectronica.gob.es/

Edita:

© Ministerio de Hacienda y Función Pública
Secretaría General Técnica
Subdirección General de Información,
Documentación y Publicaciones
Centro de Publicaciones

Colección: administración electrónica

NIPO: 169-17-109-8

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
CENTRO DE PUBLICACIONES

ÍNDICE

ÍNDICE DE TABLAS

Histórico de versiones del documento		
Nombre del documento	**Fecha**	**Descripción**
20110901_ENI_GuiaAplicacion_NTI _Politica-Firma-Certificados	01/09/2011	Primera versión.
20170517_ENI_GuiaAplicacion_NTI _Politica-Firma-Certificados	17/05/2017	Segunda versión.

1. CONSIDERACIONES PREVIAS

Este documento constituye una guía de aplicación de la *Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración* (en adelante NTI), y como tal, su objetivo es servir como herramienta de apoyo para la aplicación e implementación de lo dispuesto en la NTI. Para ello, su contenido incluye tanto citas explícitas al texto de la NTI como explicaciones y contenidos complementarios a aquélla.

Para facilitar su manejo y comprensión, esta guía incluye diferentes recursos gráficos cuya leyenda se muestra a continuación:

Título. Contenido.	Cita textual de la NTI.
	Indicador de contenido considerado de especial importancia o relevancia.
	Advertencia o aclaración para la correcta interpretación del contenido.

A lo largo del desarrollo de esta guía, y en la propia NTI, se referencia a otras normas que incluyen información relacionada con la política de firma y que es necesario conocer para abordar de manera global estos aspectos. En concreto, las normas con contenido relacionado son:

i. Catálogo de estándares.

ii. Documento electrónico.

iii. Política de gestión de documentos electrónicos.

2. INTRODUCCIÓN

1. El **Esquema Nacional de Interoperabilidad** (en adelante, ENI) se establece en el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que sustituye al apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones Públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia, en el marco, entre otras normas, de la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas.

2. 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 (en adelante, R.D. 4/2010 ENI) fija, en su Disposición adicional primera, el desarrollo de las siguientes Normas Técnicas de Interoperabilidad:

   a) Catálogo de estándares.
   b) Documento electrónico.
   c) Digitalización de documentos.
   d) Expediente electrónico.
   e) Política de firma electrónica y de certificados de la Administración.
   f) Protocolos de intermediación de datos.
   g) Relación de modelos de datos.
   h) Política de gestión de documentos electrónicos.
   i) Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas.
   j) Procedimientos de copiado auténtico y conversión entre documentos electrónicos.
   k) Modelo de Datos para el intercambio de asientos entre las Entidades Registrales.

   Más la siguiente, relativa al artículo 28 del mismo R.D. 4/2010 ENI:

   l) Declaración de conformidad con el ENI.

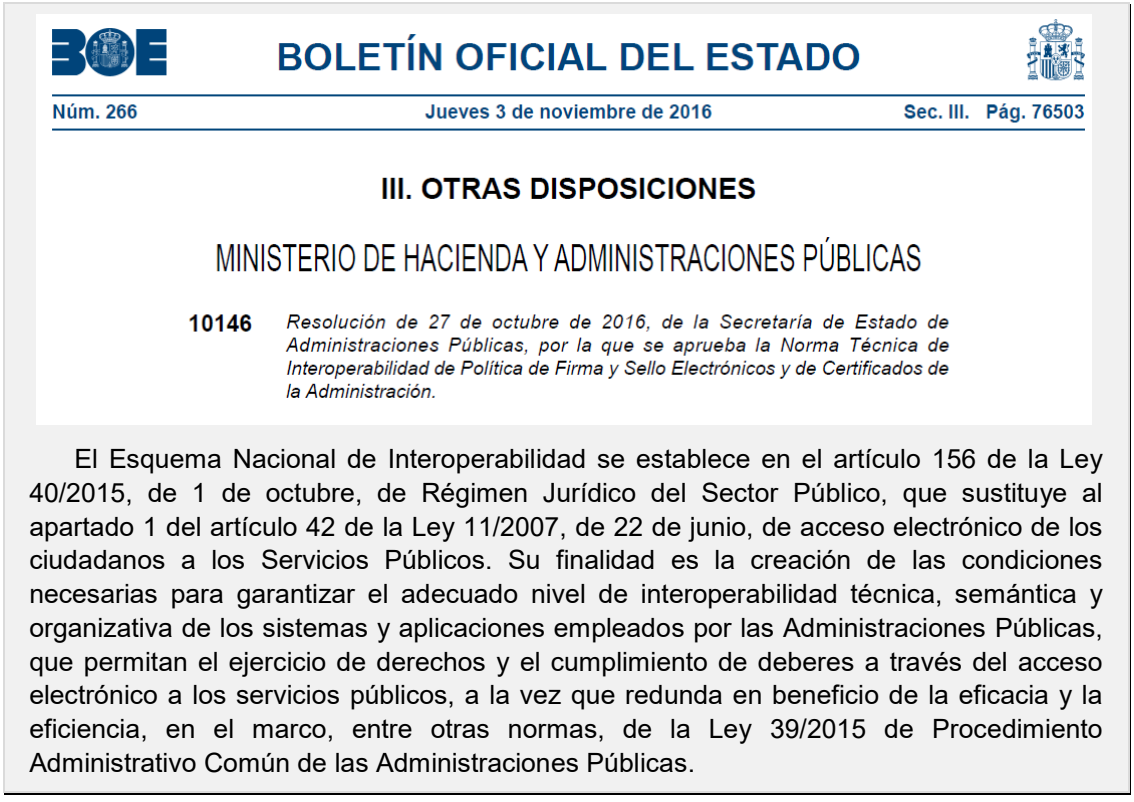
3. Estas Normas Técnicas de Interoperabilidad se aprobaron en aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del R.D. 4/2010 ENI, fruto de un proceso de elaboración en el que participaron todas las Administraciones Públicas a las que les son de aplicación, y fueron informadas favorablemente por el Comité de Dirección de Tecnologías de la Información y Comunicaciones y por el Comité Sectorial de Administración Electrónica.

4. Las diferentes NTIs se han desarrollado con el objetivo de cubrir las necesidades derivadas de la normativa aplicable en un planteamiento de partida basado en mínimos, de forma que se garantice la interoperabilidad entre las distintas administraciones, favoreciendo su implantación y aplicación en un corto plazo con un impacto mínimo, pero sin perder una orientación de desarrollo y perfeccionamiento a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica.

5. En particular, la *NTI de Política de Firma y Sello Electrónicos y de Certificados de la Administración que sustituye a la anterior denominada de Política de Firma Electrónica y de Certificados de la Administración,* establece el conjunto de criterios para el desarrollo o adopción de políticas de firma y sello electrónicos basadas en certificados por parte de las Administraciones Públicas. Para ello, define el contenido de una política de firma electrónica y sello electrónico basados en certificados, especificando las características de las reglas comunes como: formatos, uso de algoritmos, creación y validación de firma para documentos electrónicos; así como de las reglas de confianza en certificados electrónicos, sellos de tiempo y firmas longevas.

6. La *NTI de Política de Firma y Sello Electrónicos y de Certificados de la Administración* fue publicada en el Boletín Oficial del Estado Número 266 del jueves 3 de noviembre de 2016 (http://www.boe.es/diario_boe/txt.php?id=BOE-A-2016-10146), y está disponible para su consulta en el Portal de Administración electrónica (http://administracionelectronica.gob.es/), junto al resto de normas técnicas del ENI.

7. El contexto de la NTI se refleja en el texto expositivo y artículos de su Resolución que se incluyen a continuación:



BOLETÍN OFICIAL DEL ESTADO

Núm. 266 Jueves 3 de noviembre de 2016 Sec. III. Pág. 76503

III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

10146 *Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración.*

El Esquema Nacional de Interoperabilidad se establece en el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que sustituye al apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones Públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia, en el marco, entre otras normas, de la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas.

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 establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones Públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma y sello, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y reutilización de la información del sector público; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, según se establece en el artículo 29 del Esquema Nacional de Interoperabilidad.

En particular, la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración se aprobó mediante Resolución de 19 de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública, para responder a lo previsto en el artículo 18 del citado Real Decreto 4/2010, de 8 de enero, sobre la interoperabilidad en materia de firma y sello electrónicos y de certificados.

Posteriormente, la evolución de las tecnologías de aplicación, la experiencia derivada de la aplicación de la citada Norma Técnica de Interoperabilidad, la entrada en vigor de la citada Ley 40/2015, de 1 de octubre, y la evolución del contexto regulatorio europeo, particularmente por razón del Reglamento 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 y por el que se deroga la Directiva 1999/93/CE, y su normativa de desarrollo, hacen necesario una actualización de esta Norma Técnica de Interoperabilidad.

La Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y de certificados de la Administración, que sustituye a la anterior denominada de Política de Firma Electrónica y de certificados de la Administración, establece el conjunto de criterios para el desarrollo o adopción de políticas de firma y sello electrónicos basada en certificados por parte de las Administraciones públicas. Para ello, define el contenido de una política de firma electrónica y sello electrónico basados en certificados, especificando las características de las reglas comunes, como formatos, uso de algoritmos, creación y validación de firma para documentos electrónicos, así como de las reglas de confianza en certificados electrónicos, sellos de tiempo y firmas longevas.

Las condiciones establecidas en esta norma persiguen establecer un marco para la definición de políticas de firma y sello electrónicos basada en certificados alineada con actos europeos recientes como 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 (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, compatible a su vez con sistemas de firma electrónica ya implantados.

La presente actualización de la norma técnica se ha elaborado con la participación de todas las Administraciones Públicas a las que les es de aplicación, ha sido informada

favorablemente por el Comité de Dirección de Tecnologías de la Información y Comunicaciones y por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y de certificados de la Administración, que sustituye completamente a la anterior Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración, y cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y de certificados de la Administración que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 27 de octubre de 2016.–El Secretario de Estado de Administraciones Públicas, Antonio Germán Beteta Barreda.

8. El texto completo de la *NTI de Política de Firma y Sello Electrónicos y de Certificados de la Administración* está formado por los siguientes cuatro apartados:

NORMA TÉCNICA DE INTEROPERABILIDAD DE POLÍTICA DE FIRMA Y SELLO ELECTRÓNICOS Y DE CERTIFICADOS DE LA ADMINISTRACIÓN.

ÍNDICE

IV.1 Reglas de confianza para los certificados electrónicos.

IV.2 Reglas de confianza para sellos electrónicos.

IV.3 Reglas de confianza para firmas longevas.

9. Esta estructura de Resolución de aprobación refleja prácticas habituales en otros sectores para el tratamiento de cuestiones técnicas como es, en el ámbito de las telecomunicaciones, el Real Decreto 1287/1999, de 23 de julio, por el que se aprueba el Plan técnico nacional de la radiodifusión sonora digital terrenal; en el sector de la edificación el Real Decreto 314/2006, de 17 de marzo, por el que se aprueba el Código Técnico de la Edificación; y en el sector de la obra civil, por ejemplo, el Real Decreto 637/2007, de 18 de mayo, por el que se aprueba la norma de construcción sismorresistente: puentes (NCSP-07).

3. OBJETIVO Y ALCANCE DE LA NTI DE POLÍTICA DE FIRMA Y SELLO ELECTRÓNICOS Y DE CERTIFICADOS DE LA ADMINISTRACIÓN

10. El objeto de la *NTI de Política de firma y sello electrónicos y de certificados de la Administración,* recogido en su apartado I.1, parte de lo establecido en la disposición adicional primera del R.D. 4/2010 ENI, y atiende a la necesidad de definir las pautas para el desarrollo de políticas de firma electrónica.

> I. *Consideraciones generales*
>
> I.1 Objeto.
>
> 1. La Norma Técnica de Interoperabilidad (en adelante, NTI) de Política de firma y sello electrónicos y de certificados de la Administración tiene por objeto establecer el conjunto de criterios comunes asumidos por la Administración pública en relación con la autenticación y el reconocimiento mutuo de firmas electrónicas y sellos electrónicos basados en certificados electrónicos cualificados o reconocidos y que, como tales, serán desarrollados y consolidados a través de las políticas de firma y sello electrónicos basados en certificados.
>
> 2. El objetivo final de esta NTI es facilitar el uso de firmas electrónicas y sellos electrónicos seguros e interoperables entre las distintas organizaciones de la Administración pública.

11. Por lo tanto, la NTI establece el conjunto de criterios para el desarrollo o adopción de políticas de firma y sello electrónicos basadas en certificados cualificados o reconocidos por parte de las Administraciones Públicas, es decir, establece una serie de directrices para que éstas desarrollen sus propias políticas de firma y sello basada en certificados, ya sean marco o particulares, a reconocer dentro de sus ámbitos competenciales. Según esto, cada organización cumpliría las directrices especificadas en la NTI, pudiendo establecer restricciones específicas para su ámbito.

12. Como tal, la Política de firma electrónica basada en certificados de la Administración General del Estado (AGE) define, tal y como establece el punto 1 del artículo 18 del R.D. 4/2010 ENI, un marco general de interoperabilidad para la autenticación y el reconocimiento mutuo de firmas electrónicas en consonancia con lo establecido en la *NTI de Política de firma y sello electrónicos y de certificados de la Administración*.

13. 

Nótese, que la NTI detalla únicamente condiciones para políticas de firma y sello electrónicos basadas en certificados puesto que son mecanismos cuya implantación, a través de estándares completamente desarrollados, permiten un uso interoperable apoyado en la figura de la Política. Esto es, los propios estándares tienen ya desarrolladas especificaciones para su utilización en un marco de política de firma, cuestiones que, para el resto de sistemas de firma, al no estar basados en un conjunto de estándares tan completo o desarrollado, no existen mecanismos generalmente reconocidos para su uso bajo el marco de una política. No obstante, la NTI no incluye ninguna limitación que impidan incluir en la Política de firma y sello,

además de lo establecido para firmas con certificados, otros sistemas de firma reconocidos en la legislación (CSV, claves concertadas u otros sistemas no criptográficos) para los que se aplicaría lo establecido en la Ley 39/2015, de 1 de octubre, la Ley 40/2015, de 1 de octubre, y resto de normativa vigente aplicable. De esta forma, por ejemplo, podría tener especial interés incluir en la política los Códigos Seguros de Verificación (CSV) si éstos se generan, como es habitual, sobre firmas con certificados.

14. Atendiendo a lo anterior, y con el objetivo de dar apoyo a la aplicación e implementación de lo dispuesto en la NTI, esta guía desarrolla las directrices y requisitos generales para el desarrollo e implementación de políticas de firma y sello electrónicos basadas en certificados a través de los siguientes puntos:

i. Concepto y generalidades de una política de firma electrónica, así como sus datos identificativos, actores y usos de la firma electrónica, interacción con otras políticas e indicaciones para su gestión así cómo consideraciones para el archivado y custodia de la firma electrónica.

ii. Reglas comunes relativas a los formatos de firma admitidos y algoritmos utilizados así como a las reglas de creación y validación de firmas.

iii. Reglas de confianza para los certificados electrónicos, sellos de tiempo y firmas longevas.

3.1. Qué NO incluye la NTI

15. La NTI de Política de firma y sello electrónicos y de certificados de la Administración a la que da soporte esta guía, no debe considerarse como:

i. Una política de firma y sello electrónicos basada en certificados en sí misma, ya que sólo define directrices generales para el desarrollo de políticas marco o específicas por parte de los diferentes órganos de la Administración.

ii. Una guía de implementación técnica de firma y sello electrónicos basada en certificados. Esto es, la NTI no desarrolla los procedimientos específicos que rigen la operativa particular de cada organización en la creación y validación de firmas electrónicas. En este sentido, la NTI no establece ningún tipo de previsión respecto a arquitecturas de los sistemas de creación de firma electrónica (servidor, cliente, etc.). La NTI sólo especifica directrices que, una vez consolidadas en la política de firma de una organización, marcarán las especificaciones técnicas sobre las que ésta podrá implementar sus mecanismos de creación y verificación de firma particulares.

iii. Recopilación completa de consideraciones sobre los sistemas de firma electrónica reconocidos en la legislación. La NTI sólo incluye cuestiones relativas a firmas electrónicas basadas en certificados electrónicos. Para firmas electrónicas basadas en CSV, claves concertadas u otros sistemas no criptográficos se aplicaría lo establecido en la Ley 39/2015, de 1 de octubre, la

Ley 40/2015, de 1 de octubre, y resto de normativa vigente aplicable, sin detrimento de que en un futuro pudiesen ser objeto de otra regulación específica.

iv. Referencia de consideraciones relativas a la aplicación de la firma electrónica como medida de seguridad, más allá de su aplicación a contenido y transmisiones. La utilización de la firma electrónica como medida de seguridad debe contemplar lo establecido a tal efecto en el *Esquema Nacional de Seguridad (ENS)*.

4. ÁMBITO DE APLICACIÓN Y DESTINATARIOS

16. El ámbito de aplicación de la NTI de Política de firma y sello electrónicos y de certificados de la Administración se define en el apartado I.2 de la NTI:

> I.2 Ámbito de aplicación.
>
> 1. El contenido de esta NTI será de aplicación para el desarrollo o adopción de políticas de firma y sello electrónicos basada en certificados por parte de cualquier órgano de la Administración pública o Entidad de Derecho Público vinculada o dependiente de aquélla (en adelante, organizaciones) según el ámbito establecido en el artículo 3 del 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.
>
> 2. Las políticas de firma y sello harán referencia a un contexto concreto de carácter horizontal donde sea necesario normalizar aspectos de las firmas electrónicas de los Documentos Electrónicos Administrativos para garantizar la interoperabilidad, no a una Administración u organismo particular. Para establecer los aspectos técnicos de las firmas dentro de una Administración u organismos concreto, se optará por la generación de instrucciones técnicas internas, procedimientos o directrices de aplicaciones, que en todo caso deberán ajustarse a lo establecido por el Esquema Nacional de Seguridad.

17. Por tanto, las indicaciones contenidas en la NTI son de aplicación para el desarrollo de políticas de firma y sello electrónicos basadas en certificados por parte de todos los órganos de la Administración y Entidades de Derecho Público vinculadas o dependientes de aquélla (en adelante, organizaciones).

18. Dentro del ámbito de aplicación definido anteriormente, los destinatarios del contenido de la *NTI de Política de firma y sello electrónicos y de certificados de la Administración*, y por lo tanto de esta guía de aplicación, son los siguientes:

i. Responsables de la definición de políticas particulares de firma y sello electrónicos de las organizaciones.

ii. Responsables de la implantación de políticas de firma y sello electrónicos en las organizaciones.

19. 

Nótese que la NTI no establece la obligatoriedad de generar políticas de firma por parte de las Administraciones Públicas. Al contrario, exige que la generación de una política de firma se asocie a un contexto horizontal. Precisa que, en caso de querer organizar los aspectos técnicos de las firmas en las organizaciones, deberán usarse otros instrumentos distintos de las políticas, como son las instrucciones técnicas, procedimientos o directrices.

5. LA POLÍTICA DE FIRMA ELECTRÓNICA

20. El apartado II de la *NTI de Política de firma y sello electrónicos y de certificados de la Administración* establece la definición y el contenido que ha de incluir toda política de firma y sello electrónicos basada en certificados de una organización, a través de siete subapartados.

> II. *La política de firma y sello electrónicos*
>
> II.1 Definición y contenido.
>
> II.2 Datos identificativos de la política.
>
> II.3 Actores involucrados en la firma electrónica.
>
> II.4 Usos de la firma electrónica.
>
> II.5 Interacción con otras políticas.
>
> II.6 Gestión de la política de firma y sello.
>
> II.7 Archivado y custodia.

5.1. Definición y contenido

21. El epígrafe II.1.1 de la NTI recoge la definición de política de firma electrónica establecida en el R.D. 4/2010 ENI, así como los aspectos que ésta ha de definir.

> II.1 Definición y contenido.
>
> 1. Según la definición del Real Decreto 4/2010, de 8 de enero, una política de firma electrónica es el «conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma». Es de aplicación tanto a las firmas como a los sellos electrónicos.
>
> 2. ...

22. En el marco de una política, cuando se firman datos, el 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. En este caso se trataría de una firma que no especifica de forma expresa ninguna semántica o significación concreta y, por lo tanto, será necesario derivar el significado de la firma a partir del contexto y especialmente, de la semántica del documento firmado.

23. La finalidad de una política de firma es, por tanto, la de reforzar la confianza en las transacciones electrónicas a través de una serie de condiciones para un contexto dado. Este contexto puede ser: una transacción determinada, un régimen legal, un rol que asuma la parte firmante o cualquier otro ámbito.

24. El epígrafe II.1.2 establece los aspectos generales a definir en toda política de firma.

> II.1 Definición y contenido.
>
> 1. …
>
> 2. Una política de firma y sello electrónicos y de certificados definirá:
>
> a) Los procesos de creación, validación y conservación de firmas electrónicas y sellos electrónicos.
> b) Características y requisitos de los sistemas de firma electrónica, sellos electrónicos, certificados y sellos de tiempo.
>
> 3. …

25. Según éstos, el epígrafe II.1.3 desarrolla los apartados en que se concretará la definición de los aspectos generales anteriores:

> II.1 Definición y contenido.
>
> 2. …
>
> 3. Toda política de firma y sello electrónicos basada en certificados incluirá:
>
> a) Definición del alcance y ámbito de aplicación, que concretará su relación con otras políticas existentes, marco o particulares, así como la identificación de los actores involucrados y los usos de la firma electrónica y sello electrónico.
>
> b) Datos para la identificación del documento y del responsable de su gestión.
>
> c) Reglas comunes para el firmante, el creador del sello, y el verificador de la firma o sello electrónicos que incluirán:
>
> i. Formatos admitidos de firma electrónica y sello electrónico, y reglas de uso de algoritmos.
> ii. Reglas de creación de firma o sello electrónicos.
> iii. Reglas de validación de firma o sello electrónicos.
>
> d) Reglas de confianza, que incluirán los requisitos establecidos para certificados, sellos de tiempo y firmas longevas.
>
> e) Otras reglas opcionales a fijar por cada organización, como podrán ser:
>
> i. Reglas específicas de compromisos que cada organización podrá establecer para cada uno de los servicios que presta, estableciendo requisitos específicos necesarios para que la firma sea válida en cada caso.
> ii. Reglas de certificados de atributos mediante las que cada organización podrá establecer información adicional a añadir a los certificados digitales en función de sus necesidades y del contexto.
>
> f) Definición de condiciones para el archivado y custodia de firmas electrónicas.
>
> g) Descripción de consideraciones de gestión de la política que se aplicarán a dicho documento.

26. Atendiendo a este subapartado, una política de firma y sello electrónicos contendría:

i. **Definición del alcance y ámbito de aplicación,** dentro del cual debe concretarse el tipo de relaciones afectadas por el documento, por ejemplo, relaciones de los ciudadanos con la organización, relaciones entre organizaciones o relaciones asociadas a una transacción específica.

   Para la definición de este alcance y ámbito de aplicación, es necesario identificar a los actores que participan en una determinada relación o trámite, así como los

posibles usos de la firma electrónica. La definición genérica de los actores y usos de la firma electrónica que pueden considerarse para la definición del alcance de una política de firma, se definen en los subapartados II.3 y II.4 de la NTI, y se tratan en los puntos 5.3 y 5.4 de esta guía.

Dentro de la definición del alcance y ámbito de aplicación de una política de firma o sello electrónicos, debe definirse también su relación con otras políticas existentes, marco o particulares, según corresponda, tal y como establece el subapartado II.5 de la NTI y describe el punto 5.5 de esta guía.

ii. **Datos identificativos**, establecidos en el subapartado II.2 de la NTI, y que se describen en el punto 5.2 de esta guía, para la identificación del documento y del responsable de su gestión, así como su periodo de validez.

iii. **Reglas comunes** para los actores involucrados en la firma electrónica: firmante y verificador. Estas reglas aparecen por tanto en cualquier política de firma y permiten establecer responsabilidades respecto a la firma electrónica sobre la persona o entidad que crea la firma, y la persona o entidad que la verifica, definiendo los requisitos mínimos que deben presentarse.

   Las consideraciones a tener en cuenta para la definición de estas reglas o requisitos comunes se establecen en el apartado III de la NTI, se tratan en el punto 6 de esta guía, e incluyen:

   a. Formatos admitidos de firma electrónica y reglas de uso de algoritmos.
   b. Reglas de creación de firma.
   c. Reglas de validación de firma.

iv. **Reglas de confianza**, que, tal y como establece el apartado IV de la NTI, deben incluir los requisitos establecidos para certificados, sellos de tiempo y firmas longevas. El punto 7 de esta guía desarrolla consideraciones sobre este tipo de reglas.

v. Opcionalmente, otras **reglas** a definir por cada organización, como pueden ser:

   a. Reglas específicas de compromisos entendidas como características específicas de la firma que cada organización podría establecer para cada uno de los servicios que presta, estableciendo requisitos específicos necesarios para que la firma sea válida en cada caso.
   b. Reglas de certificados de atributos mediante las que cada organización establece información adicional a añadir a los certificados digitales (atributos) en función de sus necesidades y del contexto.

vi. Descripción de **consideraciones de gestión de la política** que se aplicarán al documento, tal y como expone el subapartado II.6 de la NTI y define el punto 5.6 de esta guía.

vii. Definición de **condiciones para el archivado y custodia** de firmas electrónicas, cuyos requisitos se establecen en el subapartado II.7 de la NTI, y se desarrollan en el punto 5.7 de esta guía.

5.2. Datos identificativos de la política

27. Para facilitar el correcto uso y localización de una política de firma electrónica basada en certificados, ésta debe incluir datos de identificación del documento, periodos de validez y transición, así como los datos del responsable de la gestión del documento. Estos datos son los establecidos en el apartado II.2 de la *NTI de Política de firma y sello electrónicos y de certificados de la Administración.*

5.2.1. Identificación de la política

> II.2 Datos identificativos de la política.
>
> 1. El documento de política de firma y sello incluirá la siguiente información para su identificación:
>
> a) Nombre del documento.
> b) Versión.
> c) Identificador (OID - Object IDentifier) de la política.
> d) URI (Uniform Resource Identifier) de referencia de la política.
> e) Fecha de expedición.
> f) Ámbito de aplicación.
>
> 2. …

28. Cabe destacar que toda política de firma y sello ha de tener un identificador único (un OID en ASN.1 y una URI en XML), a incluir de manera obligatoria en la firma electrónica. Para ello se debe utilizar el campo correspondiente para identificar tanto la política como su versión, junto con las condiciones generales y específicas de aplicación para su validación.

5.2.2. Periodos de validez y transición

29. Una política de firma y sello electrónicos y de certificados tiene un periodo de validez, es decir, es válida desde la fecha de expedición, que se indica dentro de los datos de identificación del documento, hasta la publicación de una nueva versión actualizada.

30. Una vez publicada una nueva versión de una política, se puede facilitar un periodo de tiempo transitorio, en el que convivan las dos versiones y que permita adecuar las diferentes plataformas de las organizaciones a las especificaciones de la nueva versión.

31. Este periodo de tiempo transitorio debe indicarse en la nueva versión y pasado dicho periodo sólo será válida la versión actualizada.

32. Con el fin de recoger la necesidad de especificar estos periodos, el epígrafe II.2.2 de la NTI establece que:

> II.2 Datos identificativos de la política.
>
> 1. …
>
> 2. La política de firma y sello incluirá la definición de su periodo de validez y las consideraciones respecto a los periodos de transición que procedan.
>
> 3. …

5.2.3. Identificación del gestor del documento de la política

33. Dada la importancia del gestor del documento de política de firma, en tanto que es el responsable de su correcta aplicación, actualización y gestión, en general, el epígrafe II.2.3 de la NTI establece los datos necesarios para asegurar su correcta identificación dentro de dicho documento:

> II.2 Datos identificativos de la política.
>
> 2. …
>
> 3. Para la identificación de su gestor, la política de firma y sello electrónicos basada en certificados incluirá:
>
> a) Nombre del gestor de la política.
> b) Dirección de contacto.
> c) OID del gestor de la política de firma.

34. Las consideraciones para la gestión de una política de firma y sello electrónicos son objeto del subapartado II.6 de la NTI y se desarrollan en el punto 5.6 de esta guía.

5.3. Actores involucrados en la firma electrónica

35. Como ya se ha mencionado, toda política de firma y sello electrónicos debe desarrollarse teniendo en cuenta los diferentes roles o actores que pueden tener presencia en torno a la firma. Sobre estos roles, además de definir el alcance y ámbito de aplicación de la propia política, se deducirán diferentes responsabilidades respecto a la propia firma, bien en su creación o en su validación.

36. El subapartado II.3 de la *NTI de Política de firma y sello electrónicos y de certificados de la Administración*, establece una definición de los actores generalmente identificados en ámbitos de políticas de firma electrónica basada en certificados:

> II.3 Actores involucrados en la firma electrónica.
>
> Los actores involucrados en el proceso de creación y validación de una firma electrónica serán:
>
> a) Firmante: Una persona física que crea una firma electrónica utilizando datos de creación de firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.
>
> b) Creador de un sello: Una persona jurídica que crea un sello electrónico.

c) Verificador: Entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por la política de firma y sello concreta por la que se rige la plataforma de relación electrónica o el servicio concreto al que se esté 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 confianza (PSC): Una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza.

e) Emisor y gestor de la política de firma: Entidad que se encarga de generar y gestionar el documento de política de firma y sello, por el cual se deben regir el firmante, el verificador y los prestadores de servicios en los procesos de generación y validación de firma electrónica.

En este documento que utilizará el término 'firmante', tanto para referirse al firmante como al creador de un sello. Puede tratarse de un proceso de actuación administrativa automatizada.

37. Dada la relevancia de cada uno de los actores involucrados, es crítico para el desarrollo de la política establecer unos roles y responsabilidad comunes, en torno a la realización técnica de la firma, de forma que sea fácilmente identificable quien asume cada rol dentro de cada organización. En este sentido, estos roles en políticas marco también deben poder identificarse fuera de la propia organización, pues por ejemplo, la firma podría tener que ser validada fuera de la propia organización.

38. En esta Guía, al igual que en el documento de la NTI se utilizará el término 'firmante' para referirse tanto al firmante como al creador de un sello. Puede tratarse de un proceso de actuación administrativa automatizada.

39. Se empleará el término 'firma' para referirse tanto a firma electrónica como a sello electrónico.

5.4. Usos de la firma electrónica

40. La firma electrónica, como mecanismo para la seguridad de la información, puede aplicarse con diferentes propósitos y a diferentes niveles, conllevando diferentes tratamientos e implicaciones. Por tanto, el desarrollo de cualquier política de firma debe recoger los usos que es necesario contemplar según el ámbito de aplicación y alcance de ésta, especificando condiciones para cada uno de los usos que corresponda.

41. Concretamente, en el caso de firma electrónica basada en certificados, el subapartado II.4 de la NTI distingue dos usos de la firma electrónica que pueden ser objeto de desarrollo en políticas de firma según las necesidades de cada organización.

II.4 Usos de la firma electrónica.

a) Las políticas de firma y sello electrónicos podrán definir condiciones para la aplicación de una firma electrónica basada en certificados con los siguientes propósitos:

b) Firma de transmisiones 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.

c) Firma de contenido como herramienta para garantizar la autenticidad, integridad y no repudio de aquel, con independencia de que forme parte de una transmisión de datos.

42. De esta forma, en función del uso de la firma electrónica, cada política de firma electrónica contemplaría los formatos admitidos para cada uno, así como las condiciones de archivado y custodia necesarias, aplicando en cualquier caso condiciones proporcionales a cada uso.

43. 
Nótese que la NTI se limita a citar posibles usos de la firma electrónica que podrían ser contemplados en una política de firma y sello electrónicos según las necesidades particulares que puedan surgir, sin establecer usos a incluir de forma obligatoria. De esta forma, se da cabida a la aplicación de las pautas de la NTI en todo tipo de políticas de firma ya se trate, por ejemplo, de políticas de firma en general de un sector específico que incluya tratamiento de documentos electrónicos, correos y transmisiones, o de una política específica en la que solo se definan las condiciones para el intercambio seguro de información en un determinado trámite. El desarrollo de una política de firma electrónica definirá los usos de la firma electrónica en su alcance o ámbito de aplicación, atendiendo a las necesidades de la organización que la desarrolla. En este contexto, por ejemplo, la Política de firma electrónica de la AGE sólo contempla firmas electrónicas de contenido y no por ello incumple lo establecido en este subapartado de la NTI.

5.4.1. Firma electrónica de transmisiones de datos

44. 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. Por ejemplo, se podría utilizar a nivel de cabecera del mensaje SOAP y, en este caso, serviría para securizar el intercambio de mensajes entre dos servidores. Por lo tanto, puesto que se está firmando el sobre SOAP y no el contenido del mensaje, este mecanismo no es suficiente para hacer llegar un documento firmado al destinatario final si hay más de dos servidores implicados.

45. Por otra parte, la firma de transmisiones de datos generalmente se realiza en el servidor, entendido éste como el sistema responsable de lanzar o generar el paquete de información a transmitir.

5.4.2. Firma electrónica de contenido

46. La firma electrónica de contenido equivale, en el entorno electrónico, a la firma manuscrita tradicional, en tanto que está asociada directamente al contenido y garantiza la autenticidad de aquél.

47. En este sentido, la firma electrónica de contenido puede ser tanto la firma de una factura electrónica, como de un documento, un expediente electrónico o cualquier otro tipo de información o trámite.

48. A diferencia de la firma de las transmisiones, la **firma de contenido**, proporciona integridad, autenticación y no repudio entre dos extremos, independientemente de que éste sea intercambiado a través de uno u otro mecanismo.

49. En caso de intercambio, tanto la firma como el propio contenido irían anexos a la transmisión o intercambio, propiamente dicho. Por lo tanto, ambos usos de la firma no son complementarios sino compatibles, ya que pueden utilizarse simultáneamente.

50. Generalmente, se utiliza la firma de contenido cuando se necesita tener efectos jurídicos frente a terceros, como sería, por ejemplo, el caso de un documento electrónico.

5.5. Interacción con otras políticas de firma electrónica

51. Las Administraciones Públicas se acogerán preferentemente a la Política Marco de Firma Electrónica basada en Certificados.

52. Las organizaciones pueden desarrollar otras políticas propias particulares adaptadas a sus necesidades específicas, siempre que estén orientadas a un contexto concreto y que cuenten con el informe favorable del Comité Sectorial de Administración Electrónica y del Comité Ejecutivo de la Comisión de Estrategia TIC.

53. En cualquier caso, todas las políticas han de poder convivir de manera conjunta, facilitando la interacción entre las mismas, siempre en cumplimiento de lo dispuesto en la *NTI de Política de firma y sello electrónicos y de certificados de la Administración.*

54. La Política de firma electrónica basada en certificados de la AGE define, tal y como establece el punto 1 del artículo 18 del R.D. 4/2010 ENI, un marco general de interoperabilidad para la autenticación y el reconocimiento mutuo de firmas electrónicas en consonancia con lo establecido en la *NTI de Política de firma y sello electrónicos y de certificados de la Administración*.

55. Nótese que la expresión *política marco* responde a la voz utilizada en el artículo 18 del R. D. 4/2010 ENI, que define la política de firma electrónica y de certificados de la AGE como una política que *"servirá de marco general de interoperabilidad para la autenticación y el reconocimiento mutuo de firmas electrónicas dentro de su ámbito de actuación"*.

56. Dicha Política puede convivir y ser utilizada a su vez como referencia para el desarrollo de políticas de firmas particulares que, de existir, deben estar disponibles en formato legible, de modo que puedan ser aplicadas en un contexto concreto para cumplir con los requerimientos de creación y validación de firma electrónica cumpliendo con la NTI.

57. Para ello, el subapartado II.5 de la NTI establece condiciones generales que garantizan esta interacción entre políticas:

> II.5 Interacción con otras políticas.
>
> 1. Las Administraciones Públicas se acogerán preferentemente a la Política Marco de Firma Electrónica basada en Certificados.
>
> a) Cada organización valorará la necesidad y conveniencia de desarrollar una política propia frente a la posibilidad de utilizar una política marco existente.
>
> b) Las Administraciones Públicas podrán aprobar otras políticas de firma y sello electrónicos dentro de sus ámbitos competenciales si las características particulares de los procedimientos administrativos bajo su competencia lo hacen necesario. Las políticas de firma y sello particulares estarán orientadas a un contexto concreto, de carácter horizontal, no a una organización concreta. En el caso de que en una organización se deseen normalizar únicamente aspectos técnicos de las firmas electrónicas, se optará por otro instrumento distinto de una Política de firma y sello, como instrucciones técnicas internas o directrices de aplicaciones.
>
> c) Serán aprobadas con informe favorable del Comité Sectorial de Administración Electrónica y del Comité Ejecutivo de la Comisión de Estrategia TIC, una vez verificada su interoperabilidad con la Política Marco de Firma Electrónica basada en Certificados.
>
> d) Con objeto de permitir la interoperabilidad de las firmas electrónicas acordes a políticas, las políticas que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Dirección de Tecnologías de la Información y las Comunicaciones del Ministerio de Hacienda y Administraciones Públicas.
>
> 2. La definición del alcance y ámbito de aplicación de una política de firma y sello electrónicos se realizará considerando su interacción con otras políticas de firma y sello electrónicos, y asegurando que:
>
> a) Su desarrollo es interoperable con la política marco, en caso de políticas de firma y sello particulares.
> b) Define las condiciones de utilización y convivencia con otras políticas particulares, si se trata de una política marco.
>
> 3. En toda política de firma y sello electrónicos se asegurará que:
>
> a) Las extensiones o restricciones establecidas para las reglas de creación o validación de firma atienden a la validación de los formatos de firma establecidos en esta NTI y política marco si procede, de forma que se garantice la interoperabilidad entre las diferentes organizaciones.
> b) Incluye, si procede, la referencia a la URL de la política marco de firma electrónica en la que se inscribe, con indicación expresa de la versión.
> c) Las firmas que se generen siguiendo políticas marco o particulares, incluyen un campo donde se indique de forma explícita la política a la que pertenecen.
> d) Para que otras aplicaciones puedan interpretar las reglas de una política particular correctamente, dicha política está disponible en formato XML (eXtensible Markup Language) y ASN.1 (Abstract Syntax Notation One).

58. Tal y como se establece en el epígrafe II.5.2 de la NTI, la definición del alcance y ámbito de aplicación de una política de firma y sello electrónicos debe realizarse considerando su interacción con otras políticas de firma electrónica.

59. Además, en el caso de que una organización desarrolle una política propia en lugar de acogerse a políticas existentes, para asegurar la interacción con otras políticas, debe acogerse a lo establecido en el epígrafe II.5.3 de la NTI.

5.6. Gestión de la política de firma y sello

60. La *NTI de Política de firma y sello electrónicos y de certificados de la Administración* dedica su subapartado II.6 a la gestión de la política de firma, reflejando, tanto cuestiones generalmente reconocidas en otros ámbitos como es la necesidad de actualización, y cuestiones particulares de la firma electrónica:

> II.6 Gestión de la política de firma y sello.
>
> 1. La política de firma y sello electrónicos incluirá la descripción básica de su proceso de gestión, estableciendo las directrices para su mantenimiento, actualización y publicación, e identificando al responsable de llevar a cabo estas tareas.
>
> 2. El gestor de la política de firma mantendrá actualizada la versión de la política de firma y sello atendiendo a:
>
> a) Modificaciones motivadas por necesidades propias de la organización.
> b) Cambios en políticas relacionadas.
> c) Cambios en los certificados electrónicos emitidos por los prestadores de servicios de certificación referenciados en la política de firma y sello.
>
> 3. Para facilitar la validación de firmas electrónicas creadas atendiendo a versiones anteriores de una política, se podrá mantener un repositorio con el historial de versiones anteriores que provea la ubicación de cada versión.

61. Por lo tanto, el gestor de la política de firma y sello, cuyos datos de contacto deben incluirse en el documento de política junto con el resto de datos identificativos indicados en el punto 5.2, deberá mantener actualizada la versión de la política de firma atendiendo a lo establecido en el epígrafe II.6.2 de la NTI.

62. Por otra parte, destacar que en el marco de la interoperabilidad, son críticas las actualizaciones y demás actuaciones relacionadas con la gestión de documentos, sobre todo en ámbitos de interacción de diferentes políticas.

5.7. Archivado y custodia

63. La *NTI de Política de firma y sello electrónicos y de certificados de la Administración* dedica su subapartado II.7 al archivado y custodia de firmas electrónicas.

> II.7 Archivado y custodia.
>
> 1. Atendiendo a las necesidades y normativa específicas de su ámbito, las políticas de firma y sello podrán contemplar la definición de condiciones y responsabilidades para el archivado y custodia de las firmas electrónicas en sus diferentes aplicaciones.
>
> 2. Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, se podrán utilizar:
>
> a) Firmas longevas mediante las que se añadirá información del estado del certificado asociado, incorporando un sello de tiempo, así como los certificados que conforman la

cadena de confianza, aplicando las reglas de confianza para firmas longevas descritas en el subapartado IV.3.

b) Otros métodos técnicos que impedirán la modificación de la firma para la que se ha verificado su validez, de acuerdo a los requisitos establecidos en la política de firma y sello correspondiente, y que habrá sido almacenada en un sistema en un momento del tiempo determinado. Todos los cambios que se realicen sobre el sistema en el que se encuentra almacenada la firma podrán auditarse para asegurar que dicha firma no ha sido modificada. Los requisitos de seguridad de dichos sistemas cumplirán con las condiciones de los niveles de seguridad establecidos por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

3. Cada política de firma y sello definirá un servicio para mantener las evidencias de validez de las firmas longevas y gestionar la actualización de las firmas y sellos. Dicho servicio especificará los mecanismos y condiciones bajo los que se archiva y custodia tanto la propia firma o sello como los certificados e informaciones de estado utilizadas en su validación.

4. El almacenamiento de los certificados y las informaciones de estado podrá realizarse dentro del fichero resultante de la firma electrónica o en un depósito específico:

a) En caso de almacenar los certificados y las informaciones de estado dentro de la firma, se sellarán también dichas informaciones, siguiendo las modalidades de firmas recogidas en 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», o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior».

b) Si los certificados y las informaciones de estado se almacenan en un depósito específico, se sellarán de forma independiente.

5. La protección de la firma/sello electrónico frente a la posible obsolescencia de los algoritmos y el aseguramiento de sus características a lo largo del tiempo de validez, se realizará a través de uno de los siguientes procesos:

a) Utilización de mecanismos de resellado de tiempo, para añadir, cuando el anterior sellado este próximo a su caducidad, un sello de fecha y hora de archivo con un algoritmo más robusto.

b) Se recomienda utilizar mecanismos de resellado/refirma, en el caso de obsolescencia de los algoritmos o formatos, con un algoritmo más robusto.

c) Almacenamiento de la firma electrónica en un depósito seguro, que garantice la protección de la firma contra modificaciones y asegurando la fecha exacta en que se guardó la firma electrónica, y en la que se comprobó la autenticidad y vigencia de los elementos que la conforman.

d) Otros sistemas que garanticen la preservación de las firmas y sellos a largo plazo con certeza de la comprobación de su validez en el momento más próximo que sea posible respecto a su generación o admisión. Estos sistemas adicionales deberán estar descritos minuciosamente en el documento de gestión de política de custodia documental de la entidad, con indicación de los plazos en los que los sistemas estuvieron vigentes y los archivos a los que estos sistemas se aplicaron, especialmente para el caso de valoración documental a largo plazo por especialistas en archivos.

6. La definición de medidas y procedimientos para archivado y custodia de firmas/sellos electrónicos se realizará atendiendo con proporcionalidad a los diferentes

usos de la firma electrónica contemplados en el alcance y ámbito de aplicación de la política.

7. Para archivado y gestión de documentos electrónicos firmados o sellados, se atenderá a lo establecido en la NTI de Política de gestión de documentos electrónicos.

64. Tal y como se establece en el epígrafe II.7.2 de la NTI, para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, ésta puede ser complementada con la información del estado del certificado asociado, incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza, aplicando por lo tanto las reglas de confianza para firmas longevas descritas en el punto 7.3 de esta guía.

65. Además de la utilización de firmas longevas, tal y como establece la NTI, la conservación de las firmas a lo largo del tiempo puede garantizarse mediante otras medidas técnicas, como es el almacenamiento de la firma en un depósito seguro.

66. Como se ha expuesto anteriormente, las firmas longevas permiten ser validadas a lo largo del tiempo por la inclusión de evidencias de validez, evitando así que puedan ser repudiadas. Por tanto, para este tipo de firmas, tal y como se establece en el epígrafe II.7.3 de la NTI, la política de firma y sello debe definir el servicio para mantener dichas evidencias y gestionar la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

6. REGLAS COMUNES

67. El apartado III de la NTI, relativo a las reglas comunes, está formado por siete subapartados en los que se establecen las consideraciones necesarias para la definición de las reglas comunes de una política de firma.

> III. *Reglas comunes*
>
> III.1 Reglas comunes.
>
> III.2 Formatos admitidos de firma electrónica.
>
> III.3 Firma electrónica de transmisiones de datos.
>
> III.4 Firma electrónica de contenido.
>
> III.5 Reglas de uso de algoritmos.
>
> III.6 Reglas de creación de firma electrónica.
>
> III.7 Reglas de validación de firma electrónica.

68. Este tipo de reglas técnicas, tal y como refleja el epígrafe III.1.1 de la NTI, permiten establecer responsabilidades respecto a la firma/sello electrónicos sobre la persona o entidad que crea la firma y la persona o entidad que la verifica, definiendo los requisitos técnicos mínimos que deben presentarse en cada caso, que variarán dependiendo también del formato utilizado. Para ello, a lo largo del apartado se establecen consideraciones sobre los formatos a utilizar, uso de algoritmos y condiciones para los procesos de creación y validación de la firma electrónica basada en certificados.

> III.1 Reglas comunes.
>
> 1. Las reglas comunes permitirán establecer responsabilidades respecto a la firma/sello electrónicos sobre la persona o entidad que crea la firma y la persona o entidad que la verifica, definiendo los requisitos mínimos que deben presentarse, debiendo estar firmados si son requisitos para el firmante, o no firmados si son requisitos para el verificador.
>
> 2. Estas reglas se definirán en base a los formatos de firma/sello electrónico admitidos, teniendo en cuenta los diferentes usos de la firma electrónica basada en certificados, al uso de algoritmos y a los procesos de creación y validación de firma y sello.

6.1. Formatos admitidos de firma electrónica

69. El subapartado III.2 de la NTI recoge las consideraciones generales a tener en cuenta sobre formatos admitidos de firma electrónica.

> III.2 Formatos admitidos de firma electrónica.
>
> 1. Los formatos admitidos por las organizaciones para las firmas/sellos electrónicos basados en certificados electrónicos, se ajustarán a:
>
> a) la «Decisión de Ejecución UE 2015/1506» o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) no 910/2014 del

Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior».

b) lo establecido en la NTI de Catálogo de estándares.

c) los formatos CAdES, XAdES y PAdES en las versiones establecidas en la Norma Técnica de Interoperabilidad de Política de firma del 2011.

2. Los formatos de firma/sello electrónico serán:

a) Si procede, interoperables con la política marco en la que se basan.

70. Las especificaciones concretas de los formatos a aplicar para cada uno de los usos de la firma electrónica definidos en el apartado II.4, son objeto de los subapartados III.3 y III.4 de la NTI que se tratan en los siguientes apartados.

6.1.1. Firma electrónica de transmisiones de datos

71. El subapartado III.3 anteriormente mencionado, establece las consideraciones para formatos de firma electrónica a utilizar en las transmisiones de datos.

III.3 Formatos de firma electrónica de transmisiones de datos.

1. La firma electrónica de transmisiones de datos estará basada en estándares recogidos en la NTI de Catálogo de estándares, siendo responsabilidad del emisor y gestor de la política la definición de las consideraciones concretas a aplicar por cada organización.

2. Cada política definirá las versiones soportadas así como los cambios en aquellas que pueden provocar una actualización de dicha política.

72. Este subapartado establece que la firma electrónica de transmisiones de datos estará basada en estándares recogidos en la *NTI de Catálogo de estándares.* Por ejemplo, para transmisiones de datos basadas en Servicios Web, se recomienda la aplicación de firmas electrónicas según el estándar WS-Security: SOAP Message Security de OASIS; en particular, con la especificación estándar X.509 Certificate Token Profile.

73. Además, la NTI apunta que cada política debe definir las versiones soportadas así como los cambios en aquellas que pueden provocar una actualización de dicha política. Por ejemplo, para WS-Security: SOAP Message Security podría soportarse la versión 1.0, la 1.1 y superiores, siempre que no implicasen cambios significativos respecto a las particularidades escogidas en la política, en cuyo caso, sería necesario realizar una actualización del documento.

6.1.2. Firma electrónica de contenido

74. De la misma manera, el subapartado III.4 de la NTI establece los formatos a utilizar para firma/sello electrónico de contenido.

III.4 Formatos de firma/sello electrónico de contenido.

1. Los formatos para la firma/sello electrónica de contenido se ajustarán a la «Decisión de Ejecución UE 2015/1506» o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) 910/2014».

2. Por compatibilidad con las políticas de firma anteriores, se permitirán aunque no se recomiendan los siguientes formatos:

a) XAdES (XML Advanced Electronic Signatures), según la especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2.
b) CAdES (CMS Advanced Electronic Signatures), según la especificación técnica ETSI TS 101 733, versión 1.6.3 y versión 1.7.4.
c) PAdES (PDF Advanced Electronic Signatures), según la especificación técnica ETSI TS 102 778-3.

3. ...

75. Los formatos empleados para la firma/sello electrónico de contenido estarán completamente alineados con 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 (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, o en la que la sustituya.

76. Nótese que la NTI permite, únicamente por compatibilidad con las políticas anteriores, el conjunto de formatos detallado en el epígrafe II.4.2, si bien no se recomienda su utilización.

77. El epígrafe III.4.3 alude al uso de los mecanismos definidos por los diferentes estándares anteriormente mencionados para reflejar la referencia a la política en la que se enmarca la propia firma, como es el uso de firmas de clase EPES (Explicit Policy-based Electronic Signature).

III.4 Formatos de firma electrónica de contenido.

2. …

3. El perfil mínimo de formato que se utilizará para la generación de firmas de contenido en el marco de una política será «-EPES», esto es, clase básica (BES) añadiendo información sobre la política de firma. En cualquier caso, cada organización podrá definir en su política de firma y sello las consideraciones adicionales que considere respecto a la interpretación y utilización de diferentes perfiles y clases de los formatos siempre en consonancia con lo establecido en esta NTI.

4. …

78. Por último, el epígrafe III.4.4 de la NTI recoge la definición de los tipos de firma para documentos electrónicos que complementan la información de la *NTI de Documento Electrónico*, y menciona la aplicación de otros formatos definidos en normativa específica, como es el caso del formato de factura electrónica «Facturae»:

III.4 Formatos de firma electrónica de contenido.

3. ...

4. Las organizaciones aplicarán consideraciones de casos particulares para firma de contenido, al menos, en los siguientes casos:

a) Los documentos electrónicos a los que se aplique firma/sello basada en certificados de cara a su intercambio se ajustarán a las especificaciones de formato y estructura establecidas en la NTI de Documento electrónico.

El formato de firma basada en certificados que acompaña a un documento electrónico se reflejará en el metadato mínimo obligatorio definido en la NTI de Documento electrónico 'Tipo de firma', que, en este caso, podrá tomar uno de los siguientes valores:

i. XAdES internally detached signature.
ii. XAdES enveloped signature.
iii. CAdES detached/explicit signature.
iv. CAdES attached/implicit signature.
v. PAdES.
vi. XAdES (Decision 1506) detached
vii. XAdES (Decision 1506) enveloped
viii. CAdES (Decision 1506) detached
ix. CAdES (Decision 1506) attached
x. PAdES (Decision 1506)

b) La firma/sello de facturas electrónicas según el formato «Facturae» se realizará conforme a lo regulado por la Orden PRE/2971/2007, de 5 de octubre, o normativa que la sustituya.

79. Aunque no son objeto de la propia NTI, la siguiente tabla recoge de forma muy resumida las características de cada uno de los tipos de firma:

TIPO DE FIRMA	DESCRIPCIÓN
XAdES internally detached signature	Contenido firmado y firma comparten una misma estructura XML como nodos independientes y del mismo nivel. Dentro de este tipo, para las firmas de documentos de gran tamaño, se puede considerar el uso de etiquetas 'manifest', para la inclusión de las referencias al documento firmado.
XAdES enveloped signature	Contenido firmado y firma comparten una misma estructura XML necesaria para la validación de la firma. La firma se ubica justo después del contenido firmado.
CAdES detached / explicit signature	Contenido firmado y firma constituyen ficheros independientes
CAdES attached/implicit signature.	El fichero de firma envuelve el propio contenido firmado de forma que, para acceder al contenido, es necesario interpretar la firma.
PAdES	Contenido firmado y firma se incluyen bajo un único fichero PDF que permite el acceso a ambos componentes de forma independiente.

Tabla 1. Resumen descripción de tipos de firma de contenido.

Nótese que el tipo de firma aplicado sobre un documento electrónico conllevará un determinado tratamiento de cara a su integración en la estructura XML para el intercambio de documentos electrónicos

	definida en la NTI de Documento Electrónico. *La descripción completa, consideraciones de aplicación y las pautas para el tratamiento de los tipos de firma establecidos para documentos electrónicos en la generación de XMLs de documentos y expedientes electrónicos atendiendo a los esquemas XSD definidos en el ENI se tratan en el Manual de usuario de esquemas XML para el intercambio de documentos y expedientes electrónicos del ENI.*

80. Con carácter didáctico, los siguientes puntos incluyen las principales características de cada uno de los formatos mencionados en la NTI y las consideraciones generales a tener en cuenta para su aplicación, que, deberán concretarse, en cada política de firma.

6.1.2.1. Formato XAdES

81. El formato XAdES amplía las especificaciones del estándar XML-DSig, que recoge las reglas básicas de creación y procesamiento de firmas electrónicas de documentos XML, definiendo estructuras que permiten incorporar información adicional a la firma para facilitar su validación.

82. En el caso de firmas XAdES, las estructuras a considerar para el desarrollo de una política de firma son, al menos, las siguientes:

i. *Internally detached signature:* en la que se genera un único documento electrónico que contiene el fichero original, codificado en base64[1], y las firmas. Tanto el fichero original como las firmas se encuentran en el mismo nivel XML, vinculados ambos mediante una relación interna.

   Para las firmas de documentos de gran tamaño, puede resultar más eficiente incluir, en lugar del fichero original en base64, una referencia al contenido firmado mediante las etiquetas 'manifest' definidas en el estándar XAdES. Estas etiquetas incorporan una referencia al documento firmado y un hash de dicho documento. De esta manera, se puede separar el tratamiento del contenido del documento, de su firma, manteniendo la misma estructura de firma.

ii. *Enveloped signature:* en este caso la firma está contenida en el fichero firmado. Esta estructura es la establecida, por ejemplo, para firma de facturas electrónicas conforme a lo regulado en la Orden PRE/2971/2007.

83. La estructura *externally detached* no incluye el documento original sino que se hace referencia a aquél a través de una URL que sirve para su localización. Esta estructura no incluye el hash del documento firmado, sino solo su URL. Este tipo de estructuras no facilitan la interoperabilidad, ya que la posibilidad de validar la firma dependerá de la disponibilidad de dicha URL y de su accesibilidad por parte de la entidad verificadora de la firma, ya que es necesario acceder a la URL para calcular

[1] *Si el formato del documento original fuese un fichero que contenga sólo texto (fichero XML), no sería precisa su codificación en base64.*

el hash del documento necesario para validar la firma. Por tanto, son estructuras cuya inclusión en las políticas de firma de las organizaciones no es recomendable.

6.1.2.2. Formato CAdES

84. El formato CAdES amplía las especificaciones del estándar CMS (Cryptographic Message Syntax), definiendo estructuras más complejas con información adicional para la posterior verificación y validación de la firma.

85. El estándar CMS es un formato empleado para firmar electrónicamente, cifrar los datos y autenticar a las partes. Los valores se generan usando el estándar Abstract Syntax Notation One (ASN.1), según la recomendación ITU-T X.680.

86. Las firmas CAdES, con el fin de facilitar la conservación tanto del documento como de la propia firma, como norma general, se deberían generar con estructura *internally detached* donde, tal y como se explicó en el punto anterior, la firma y el documento se mantienen en bloques separados pero en el mismo fichero.

87. En el caso de que, debido al tamaño de los datos a firmar, no resulte técnicamente posible o aconsejable realizar las firmas con el formato anteriormente descrito, la política de firma podría contemplar la posibilidad de generar la estructura de firma *detached*, que incluye el hash del documento original en la firma.

6.1.2.3. Formato PAdES

88. El formato PAdES amplía las especificaciones del estándar de firma en PDF, añadiendo la información adicional de firma similar a la usada en las firmas CAdES o XADES.

89. La parte 3 del estándar PAdES "*PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles*" recoge la estructura de las firmas PAdES cuando la firma incluida dentro del documento PDF es de tipo CAdES.

90. Los perfiles para creación y verificación de firma en documentos PDF, formatos PAdES-BES y PAdES-EPES, tienen características muy similares a los descritos para CAdES, ya que ambos están basados en el estándar CMS.

91. En el caso de documentos PDF, la firma se encuentra embebida en la propia estructura del documento, tal y como especifica el estándar ISO 32000-1:2008.

92. La estructura de firma recomendada para el formato PAdES es la basada en la norma ETSI TS 102 778-3, que incrusta una firma CAdES *detached* dentro del documento PDF.

93. Nótese, que el formato PAdES es un formato de firma que aúna la usabilidad y accesibilidad de un archivo PDF, junto con la robustez y longevidad de los formatos avanzados (AdES). Es, además, uno de los formatos interoperables propuestos por la Comisión Europea. Por todo ello, la *NTI de Política de firma y sello electrónicos y de certificados de la Administración* considera PAdES como: formato admitido.

6.2. Reglas de uso de algoritmos

94. Las reglas de uso de algoritmos es un tipo de reglas comunes que, como tales, cada organización ha de contemplar en el desarrollo de su política de firma electrónica, siguiendo en cualquier caso lo establecido en el subapartado III.5 de la NTI:

> III.5 Reglas de uso de algoritmos.
>
> 1. La política de firma y sello especificará las reglas de uso de algoritmos en los diferentes formatos así como la longitud de las claves asociadas a aquéllos de forma proporcional a las necesidades detectadas en los diferentes usos de la firma/sello electrónicos, cumpliendo en cualquier caso lo establecido en la NTI de Catálogo de estándares y lo previsto en las normas que se definan en aplicación del Reglamento (UE) 910/2014.
>
> 2. Para los entornos de seguridad regulados por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/ 2015, de 1 de octubre, de Régimen Jurídico del Sector Público, de aplicación en los procedimientos de administración electrónica, se ajustarán a la «Decisión de Ejecución UE 2015/1506» o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) 910/2014» o las especificaciones técnicas publicadas por los organismos de Estandarización Europeos. La definición de usos de algoritmos podrá contemplar diferentes posibilidades según lo establecido en las guías aplicables, como la norma CCN-STIC 807 del Esquema Nacional de Seguridad relativa al uso de criptografía, las normas ETSI TS 119 312 'Criptographic Suites for secure electronic signatures', o aquellas que las sustituyan.
>
> 3. Para los entornos de alta seguridad, de acuerdo con el criterio del Centro Criptológico Nacional (CCN) serán de aplicación las recomendaciones revisadas de la CCN-STIC 405 así como en la norma CCN-STIC 807 del Esquema Nacional de Seguridad relativa al uso de criptografía.

6.3. Reglas de creación y validación de firma para documentos electrónicos

95. Al igual que las reglas de uso de algoritmos, las reglas de creación y validación de firma para documentos electrónicos son reglas comunes que cada organización ha de incluir como parte de su política de firma electrónica; en este caso, siguiendo lo establecido en los subapartados III.6 y III.7, respectivamente, de la NTI.

96. 

Nótese, que la NTI utiliza de forma intencionada la denominación genérica *"fichero, formulario u otro objeto binario"*, con el fin de establecer unas pautas básicas de aplicación general, en la creación y validación de la firma electrónica de cualquier contenido. De esta forma, por ejemplo, si el objeto a firmar ha de constituir un documento electrónico, se tendrá en cuenta lo establecido en esta NTI, así como, de forma adicional, en la *NTI de Documento Electrónico*.

> III.6 Reglas de creación de firma electrónica.
>
> 1. Las políticas de firma y sello definirán las condiciones particulares bajo las que, en su ámbito, se generará la firma electrónica.

2. Las plataformas que presten el servicio de creación de firma electrónica proporcionarán las funcionalidades necesarias para soportar un proceso de creación de firmas y sellos basado en los siguientes puntos:

a) Selección por parte del usuario firmante del fichero, formulario u otro objeto binario para ser firmado. Los formatos de ficheros atenderán a lo recogido en la NTI de Catálogo de estándares.

El firmante se asegurará de que el fichero que se quiere firmar no contiene contenido dinámico que afecte a su validez y que pudiese modificar el resultado de la firma/sello a lo largo del tiempo.

b) El servicio de firma electrónica ejecutará las siguientes verificaciones previas a la creación de la firma:

i. La firma/sello electrónicos pueden ser validados para el formato del fichero específico que va a ser firmado.

ii. Validez del certificado, comprobando si el certificado ha sido revocado, o suspendido, si entra dentro de su periodo de validez, y la validación de la cadena de certificación, incluyendo la validación de todos los certificados en la cadena, y de su vigencia y estado de no revocación, y si el certificado ha sido expedido por un Prestador de Servicios de Confianza Cualificado, incluido en la TSL del país emisor.

Si alguna de estas verificaciones es errónea, el proceso de firma se interrumpirá.

Si no fuese posible realizar estas comprobaciones en el momento de la firma, será necesario, en todo caso, que los sistemas receptores de la firma asuman dicha validación, antes de aceptar el fichero, formulario u otro objeto binario firmado.

c) El servicio creará un fichero con la firma/sello según corresponda en función del formato utilizado.

En el momento de la firma, se incluirá la referencia del identificador único de la versión del documento de política de firma y sello electrónicos en el que se ha basado su creación.

3. La vinculación del firmante se establecerá a través de etiquetas que, incluidas bajo la firma, y definidas según los estándares correspondientes (XAdES, CAdES y/o PAdES), proporcionarán la siguiente información complementaria a ésta:

a) Fecha y hora de firma, que podrá ser meramente indicativa en función de cómo se haya generado la firma.

b) Certificado del firmante.

c) Cadena de validación.

d) Política de firma y sello sobre la que se basa el proceso de generación de firma electrónica.

e) Formato del objeto original.

4. Como datos opcionales, la firma/sello electrónicos podrá incluir:

a) Lugar geográfico donde se ha realizado la firma del documento.

b) Rol de la persona firmante en la firma electrónica.

c) Acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, etc.).

d) Sello de tiempo sobre algunos o todos los objetos de la firma.

5. En caso de creación de firmas/sellos electrónicos por distintos firmantes sobre un mismo objeto, donde el segundo firmante ratifica la firma del primero se utilizará la etiqueta correspondiente, CounterSignature, para contabilizarlas.

6. En el caso de que las múltiples firmas/sellos se realicen al mismo nivel, cada una de ellas se representará como una firma independiente.

97. Destacar que la NTI establece que el fichero a firmar no debe incluir contenido dinámico que pudiese modificar el resultado de la firma a lo del tiempo. En este sentido cabe observar que, si el fichero que se quiere firmar no ha sido creado por el firmante, será él el responsable de asegurarse de que esto se cumpla.

98.  Además, los epígrafes III.6.5 y III.6.6 establecen consideraciones básicas para la creación de firmas múltiples sobre un mismo contenido, pero sin especificar más allá cuestiones de uso, que podrán ser definidas por cada organización en función de sus necesidades específicas.

99. Por último, mencionar que si el documento electrónico resultante de la aplicación de la firma va a ser objeto de intercambio, se representará bajo la estructura definida para tal fin en la *NTI de Documento Electrónico*, bajo la cual, es posible localizar el fichero que se firma, la firma y los metadatos asociados a ambos.

*La descripción completa, las consideraciones de aplicación y las pautas para el tratamiento de los **tipos de firma** establecidos para documentos electrónicos **en la generación de XMLs de documentos y expedientes electrónicos** atendiendo a los esquemas XSD definidos en el ENI se describen en el **Manual de usuario de esquemas XML para el intercambio de documentos y expedientes electrónicos del ENI**.*

100. El subapartado III.7 de la NTI relativo a las reglas de validación de firma electrónica se incluye a continuación:

> III.7 Reglas de validación de firma/sello electrónicos.
>
> 1. Las políticas de firma y sello definirán las condiciones particulares bajo las que, en su ámbito, será posible validar la firma electrónica de un documento siguiendo los requisitos establecidos en el artículo 32.1 del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
>
> 2. En el caso de documentos electrónicos, para acceder a la visualización de la firma/sello, el usuario podrá presentar dicho documento electrónico, que contenga los datos, metadatos y firmas/sellos, en una sede electrónica o en otros sistemas generales que proporcionen herramientas de reproducción de documentos electrónicos.
>
> 3. Las condiciones mínimas que se producirán para la validación de la firma/sello serán las siguientes:
>
> a) Garantía de que la firma es válida para el fichero específico que está firmado.
>
> b) Validez de los certificados:
>
> i. El instante de tiempo que se tomará como referencia para la validación será:
> 1) El momento en que se produjo la firma/sello si se da alguno de los siguientes supuestos:
> a) los servicios de los prestadores facilitan los históricos de estado de los certificados y la firma/sello lleva un sello de tiempo válido en el momento de la verificación.
> b) se trata de firmas/sellos longevos que incluyen las evidencias de la validez de la firma electrónica en el momento de la generación o primera validación, y dichas evidencias se encuentran selladas con un sello de tiempo válido.
> 2) En otros casos, el momento de la validación.

ii. Se comprobará que los certificados no fueron revocados ni suspendidos y que no han expirado.

iii. Se comprobará la validez de toda la cadena de certificación, incluyendo todos los certificados que la componen, con independencia de que éstos se encuentren incluidos en la propia firma o no.

iv. Se verificará que el certificado ha sido expedido por un prestador de servicios de certificación de confianza bajo una Declaración de Prácticas de Certificación que cumplirá la normativa y estará incluido en la política de firma y sello aplicable, y ha sido expedido por un Prestador de Servicios de Confianza Cualificado, incluido en la TSL del país emisor.

v. Verificación, si existen y si así lo requiere la política de la plataforma de relación electrónica o un servicio concreto de dicha plataforma, de los sellos de tiempo de los formatos implementados, incluyendo la verificación de los periodos de validez de los sellos de tiempo.

4. Para validar la firma electrónica se considerará la siguiente información:

a) Fecha y hora de la firma/sello: Si se ha realizado el sellado de tiempo, el sello de tiempo más antiguo dentro de la estructura de la firma se utilizará para determinar la fecha de la firma/sello. En caso de que no existan sellos de tiempo, la fecha y hora de la firma tendrán carácter indicativo, pero no se utilizarán para determinar el momento en que se realizó la firma. En caso de que no existan sellos de tiempo en la firma, la validación del certificado se realizará en el momento de la validación de la firma/sello.

b) Certificado del firmante. Este campo se utilizará para verificar el estado del certificado, y en su caso la cadena de certificación, en la fecha de la generación de la firma/sello.

c) Política de firma y sello sobre la que se basa el proceso de generación de firma electrónica. Se utilizará para identificar, mediante su hash y su identificador (OID), que la política de firma y sello que se ha utilizado para la generación de la firma se corresponde con la que se utilizará para el servicio en cuestión.

Esta validación de la política de firma y sello, implicará que el verificador dispondrá de los medios para verificar las condiciones impuestas en la política de firma y sello concreta. La disponibilidad de la política de firma y sello en un formato interpretable por medios automatizados (XML o ASN.1) y siguiendo los estándares europeos de representación de políticas de firma, indicada en el epígrafe 3.d del subapartado II.5 de esta NTI, facilitará la labor de las aplicaciones receptoras de firmas electrónicas en aplicar distintas políticas de firma y sello.

5. Si se han realizado varias firmas/sellos sobre un mismo documento, se seguirá el mismo proceso de verificación que con la primera firma/sello, comprobando cada firma o la etiqueta *CounterSignature* en el campo de propiedades no firmadas, donde se informa de los refrendos de firma generados.

6. El encargado de la verificación de la firma/sello podrá definir sus procesos de validación y de archivado, siempre en consonancia con los requisitos de la política de firma y sello a la que se ajuste el servicio y con lo establecido en la NTI de Política de gestión de documentos electrónicos.

7. Para la verificación del estado de los certificados en el caso de formatos de firma longeva, la validez de la firma/sello vendrá determinada por la validez del sello de tiempo de las evidencias de la validación incluidas en la firma. En estos casos la validez de la firma/sello a lo largo del tiempo se mantendrá resellando la firma/sello antes de la caducidad del certificado de la TSA (Autoridad de sellado de tiempo) que realizó el sello anterior, de forma que siempre sea posible verificar que en el momento en que se realizó la firma/sello, el certificado era válido.

8. En el caso de validación por un tercero, el validador ofrecerá a la parte usuaria el resultado correcto del proceso de validación.

101. Destacar que la información de firma en que se basa la validación definida en la NTI corresponde con la que se establece en el subapartado III.6 y que se habría incorporado a la firma en el momento de su creación haciendo uso de las etiquetas definidas en cada formato para tal fin.

7. REGLAS DE CONFIANZA

102. El apartado IV de la NTI, relativo a las reglas confianza, está formado por tres subapartados, en los que se establecen las consideraciones necesarias para la definición de las reglas de confianza de una política de firma relativas a certificados, sellos electrónicos y firmas longevas.

> IV. *Reglas de confianza*
>
> IV.1 Reglas de confianza para los certificados electrónicos.
>
> IV.2 Reglas de confianza para sellos electrónicos.
>
> IV.3 Reglas de confianza para firmas longevas.

7.1. Reglas de confianza para los certificados electrónicos

103. Las reglas de confianza para certificados electrónicos se establecen en el subapartado IV.1 de la NTI. El establecimiento de este tipo de reglas atiende a la definición de características de los propios certificados, de su validación y de los prestadores de servicios de certificación.

7.1.1. Certificados admitidos

104. El propósito de un certificado de firma es permitir al ciudadano, entidad u órgano de la administración firmar trámites o documentos, garantizando la identidad del firmante poseedor de la clave privada de firma, así como la integridad del documento firmado. La NTI establece en sus epígrafes IV.1.1, IV.1.2, IV.1.3 y iV.1.4 los certificados admitidos de firma electrónica, englobados dentro de las reglas de confianza.

> IV.1 Reglas de confianza para los certificados electrónicos.
>
> 1. Las políticas de firma y sello, marco o particulares, podrán fijar limitaciones y restricciones específicas para los certificados electrónicos que admiten en cada uno de los servicios que corresponda, si el uso destinado del certificado establecido en su Política de Certificación no está acorde al ámbito de la Política de firma y sello, siempre en consideración de la normativa aplicable en cada caso.
>
> 2. Se presumirán válidos los certificados cualificados que usen los ciudadanos en las firmas y sellos electrónicos. Si una administración apreciara algún aspecto que cuestionara esta validez lo hará saber al ciudadano que dispondrá del plazo previsto en la normativa de procedimiento administrativo para subsanar lo que corresponda o ratificar por otra vía los documentos firmados electrónicamente. El firmante no podrá alegar que ha utilizado una firma inválida con arreglo a una determinada Declaración de Prácticas de Certificación como condición en la que se base un recurso de nulidad o anulabilidad de un acto.
>
> 3. Los certificados válidos para ejecutar la firma/sello electrónicos de contenido serán los certificados electrónicos cualificados de firma y sello según el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

> 4. La relación de prestadores de servicios de certificación que emiten certificados electrónicos cualificados se consultará en la TSL (Lista de servicios de confianza) publicada en la sede electrónica del Ministerio de Industria, Turismo y Comercio y en las TSL del resto de países de la UE, de conformidad con la Decisión de Ejecución UE 2015/1505 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
>
> 5. ...

105. Según los epígrafes IV.1.3 y IV.1.4, será válido cualquier certificado electrónico cualificado incluido en las Listas de Servicios de Confianza emitidas acorde al artículo 22, apartado 5, del Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

106. El Reglamento (UE) 910/2014, EIDAS, establece la obligación de los Estados Miembro de emitir unas Listas de Confianza con información relativa a los Prestadores Cualificados, que permitan establecer la confianza en los certificados cualificados que emiten y, por tanto, la interoperabilidad de las firmas realizadas con esos certificados en el ámbito Europeo.

107. A la citada relación de prestadores de servicios de certificación se puede acceder a través de las siguientes URLs:

https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf

https://sede.minetur.gob.es/prestadores/tsl/tsl.xml

108. Por otra parte, el R.D. 1671/2009, de 6 de noviembre, modificado parcialmente por la Ley 39/2015 y la Ley 40/2015, concreta los certificados en el ámbito de la AGE. Con carácter meramente informativo, la siguiente tabla recoge las características de cada uno de estos tipos de certificados:

Tipo de Certificado	Articulado R.D 1671/2009	Contenido
De sello electrónico	Artículo 19	a) Descripción del tipo de certificado: «sello electrónico». b) Nombre del suscriptor. c) Número de identificación fiscal del suscriptor.
De empleado público	Artículo 22	a) Descripción del tipo de certificado en el que deberá incluirse la denominación «certificado electrónico de empleado público». b) Nombre y apellidos del titular del certificado. c) Número del documento nacional de identidad o número de identificación de extranjero del titular del certificado. d) Órgano u organismo público en el que presta servicios el titular del certificado. e) Número de identificación fiscal del órgano u organismo público en el que presta sus servicios el titular del certificado.

De empleado público con seudónimo	Artículo 22	a) Descripción del tipo de certificado en el que deberá incluirse la denominación «certificado electrónico de empleado público con seudónimo». b) Seudónimo del titular del certificado, consistente en su número de identificación profesional u otro indicador proporcionado por la Administración correspondiente. c) Órgano u organismo público en el que presta servicios el titular del certificado. d) Número de identificación fiscal del órgano u organismo público en el que presta sus servicios el titular del certificado.
De sede electrónica	Artículo 18	a) Descripción del tipo de certificado: «sede electrónica». b) Nombre descriptivo de la sede electrónica. c) Denominación del nombre del dominio. d) Número de identificación fiscal de la entidad suscriptora. e) Unidad administrativa suscriptora del certificado.

Tabla 2. Tipologías de los certificados definidos en el R.D. 1671/2009 y sus características.

109. Nótese que, tal y como se establece en el punto segundo del artículo 18 del R.D. 1671/2009, de 6 de noviembre, los certificados de sede electrónica son sólo válidos para la identificación de la sede electrónica, quedando excluida su aplicación para la firma electrónica de contenido.

110. Un Prestador de Servicios de Certificación, cuando proporciona un certificado de firma a un usuario, puede establecer restricciones sobre el uso de ese certificado a través de la Declaración de Prácticas de Certificación de ese certificado concreto, tales como su uso para unos procedimientos determinados o bajo unas condiciones, fuera de las cuales, no se considera responsable. Dichas condiciones pueden ser muy variadas, dependiendo del acuerdo que el Prestador establezca con el usuario. No están normalizadas y no son procesables automáticamente.

111. El epígrafe IV.1.1 establece que la Política de Firma puede contener restricciones y limitaciones a la regla general, establecida en los epígrafes IV.1.3 y IV.1.4, en donde se señala que son validos todos los certificados incluidos en las Listas de Servicios de Confianza (TSL), si el uso destinado del certificado establecido en su Política de Certificación no está acorde al ámbito de la Política de firma. Por ejemplo, si la Política de firma es una Política de firma longeva para archivo, y la Política de Certificación del certificado establece que dichos certificados no se emiten para hacer firmas longevas.

112. El epígrafe IV.1.2 establece que el firmante, el cual conoce las limitaciones al uso del certificado establecidas en las Políticas de Certificación, es el responsable del uso adecuado del certificado, conforme a las restricciones que estén establecidas en dicha política y en la Declaración de Practicas de certificación, si existen.

7.1.2. Reglas de validación de los certificados electrónicos

113. Por último, los epígrafes IV.1.5 y IV.1.6 de la NTI se centran en la validación de los certificados electrónicos.

IV.1 Reglas de confianza para los certificados electrónicos.

4. …

5. La política de firma y sello electrónicos podrá establecer el período de precaución o de gracia que corresponda aplicar para la validación de los certificados. Este periodo podrá ser, desde el momento en que se realiza la firma o el sellado de tiempo, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs (Certificate Revocation Lists) o el tiempo máximo de actualización del estado del certificado en el servicio OCSP (Online Certificate Status Protocol). Esta definición tendrá en cuenta también la posibilidad de que estos tiempos varíen según el Prestador de Servicios de Certificación.

6. El verificador validará los certificados electrónicos en base a los procesos de validación y archivado definidos en la política de firma y sello a la que se ajuste el servicio en cada caso.

114. El periodo de precaución o de gracia que se menciona en el epígrafe quinto es un periodo de tiempo de espera utilizado para comprobar el estado de revocación de un certificado. El verificador puede esperar ese tiempo para validar la firma o realizar la validación en el mismo momento y revalidarla después. Esta espera protege de posibles demoras entre el instante en que el firmante inicia la revocación de un certificado y el momento en que concluye la distribución de la información del estado de revocación de dicho certificado a los puntos de información correspondientes.

115. Además, la política de firma y sello electrónicos puede establecer el período de precaución o de gracia que corresponda aplicar para la validación de los certificados. Cabe observar que este periodo, desde el momento en que se realiza la firma o el sellado de tiempo sea, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs (Certificate Revocation Lists) o el tiempo máximo de actualización del estado del certificado en el servicio OCSP (Online Certificate Status Protocol). Esta definición debe tener en cuenta también la posibilidad de que estos tiempos varíen según el Prestador de Servicios de Certificación.

116. Según esto, el verificador deberá validar los certificados electrónicos en base a los procesos de validación y de archivado definidos en la política de firma a la que se ajuste el servicio en cada caso, tal y como establece el epígrafe IV.1.6 de la NTI.

7.2. Reglas de confianza para sellos de tiempo

117. El **sello de tiempo** asegura que, tanto los datos originales del contenido que va a ser sellado, como la información del estado de los certificados, se generaron antes de una determinada fecha. Para ello, el sellado de tiempo consiste en 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 actúe como tercero de confianza y que asegure la exactitud e integridad de la indicación de tiempo del documento. El subapartado IV.2 de la NTI establece las reglas de confianza para los sellos de tiempo.

IV.2 Reglas de confianza para sellos de tiempo.

1. Los sellos cualificados de tiempo cumplirán los indicados en el artículo 42.1 del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

2. Los elementos básicos de un sello cualificado de tiempo serán los indicados en las Normas Europeas de estandarización:

a) ETSI EN 319 422 V1.1.1 Time-stamping protocol and time-stamp token profiles.
b) ETSI EN 319 421 V1.1.1 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

O en las que las sustituyan.

3. El sellado de tiempo y la información de validación podrán ser añadidos por el emisor, el receptor o un tercero y se incluirán como propiedades no firmadas en los campos correspondientes según el formato de firma utilizado.

4. En la política de firma y sello se establecerán las condiciones según las que determinar los sellos de tiempo admitidos atendiendo a sus necesidades particulares, y en base a la normativa y legislación vigente. Esto incluye el establecimiento del tiempo máximo aceptable para realizar el sellado de tiempo, anterior, en cualquier caso, a la caducidad del certificado.

7.3. Reglas de confianza para firmas longevas

118. Una **firma longeva** es aquella que permite garantizar su validez a largo plazo, una vez vencido el periodo de validez del certificado.

119. Para ello, este tipo de firma incorpora información adicional a las firmas electrónicas que permite demostrar la autenticidad, validez y no-repudio del contenido firmado en un determinado instante.

120. Además, en el caso de firmas longevas es conveniente incluir un sello de tiempo que permita garantizar que el certificado era válido en el momento en que se realizó la firma.

121. Esta información puede ser incluida tanto por el firmante como por el verificador, aunque en el caso de que sea incluida por el firmante se recomienda hacerlo después de trascurrido el mencionado periodo de precaución o periodo de gracia (período para comprobar el estado de revocación de un certificado).

122. Tal y como establece el epígrafe IV.3.3 de la NTI, relativo a reglas de confianza para firmas longevas, en el caso de que se desee incorporar a la firma la información completa de validación, se debe usar validación mediante OCSP, ya que mediante este método las propiedades o atributos a incluir son de menor tamaño.

123. Por otra parte, a partir de firmas de clase EPES es posible incluir suficiente información para validar la firma a largo plazo en cualquiera de los formatos admitidos.

124. Las consideraciones generales para las reglas de confianza de firmas longevas se recogen en el subapartado IV.3 de la NTI:

> IV.3 Reglas de confianza para firmas longevas.
>
> 1. En el caso de firmas longevas, el firmante o el verificador de la firma incluirá un sello de tiempo que permita garantizar que el certificado era válido en el momento en que se realizó la firma. En el caso de que sea incluida por el firmante, se podrá realizar una vez haya trascurrido el periodo de precaución o periodo de gracia.
>
> 2. Para la conversión de una firma electrónica a firma electrónica longeva:
>
> a) Se verificará la firma electrónica, validando la integridad de la firma acorde a las reglas de validación de firma electrónica del epígrafe III.7.
> b) Se realizará un proceso de completado de la firma electrónica que consistirá en la obtención y almacenamiento de las referencias a:
> i. Certificados: incluyendo los certificados del firmante y de la cadena de certificación.
> ii. Informaciones de estado de los certificados, CRLs o las respuestas OCSP.
> c) Aplicación del sellado de tiempo a las referencias a los certificados y a las informaciones de estado.
>
> 3. Para la incorporación a la firma de la información completa de validación, se usará validación mediante CRLs u OCSP.
>
> 4. Las políticas de firma y sello contemplarán la definición de formatos y consideraciones de uso de firmas longevas conforme a las necesidades específicas de su ámbito de aplicación y a la normativa específica aplicable.

125. En función de las necesidades de conservación de la información firmada a largo plazo en cada procedimiento administrativo, y de la conveniencia de seguir permitiendo una verificación automatizada de la firma una vez que ha caducado o ha sido revocado el certificado firmarte, una política de firma podrá establecer reglas especificas para las firmas longevas:

- Un primer paso para la conservación a largo plazo de las firmas consiste en añadir un sello de tiempo a la firma, a través del atributo o campo correspondiente de la especificación técnica. De esta forma, se obtiene una firma XAdES-T Level, CAdES-T Level o PAdES-T Level, que permite la verificación de las firmas aunque se haya producido la revocación del certificado firmante. Este tipo de firma longeva asegura la fecha de la firma. Por tanto, no permite la verificación automatizada de la firma una vez que se ha producido la caducidad del certificado firmante pero permite asegurar la validez de la firma aunque dicho certificado haya sido revocado.
- Si se desea extender la verificación automatizada una vez excedida la fecha de caducidad del certificado, será necesario añadir información de revocación a la firma, y sellar dicha información de revocación mediante un sello de tiempo. Los atributos/campos a través de los cuales se va a añadir la información de revocación varían en función de la especificación técnica de la firma. Típicamente, se usan atributos para:
    - Los certificados de la cadena de confianza que sean necesarios para validar la firma. Esto incluye los certificados de la cadena de confianza del certificado firmante, los de las evidencias de revocación, si son distintos de

los del certificado firmante, y los de los sellos de tiempo, hasta el certificado del que se origina la cadena de confianza.

- Las evidencias de revocación de los certificados (CRL u OCSP) necesarias para verificar la firma, incluyendo las evidencias de revocación del certificado firmante, sello de tiempo y certificados de las Autoridades de Certificación (CA) emisoras que forman la cadena de confianza. En el caso de que se desee incorporar a la firma esta información de validación, la validación mediante OCSP suele proporcionar evidencias de menor tamaño.

Si, además de dicha información, se añade un sello de tiempo de archivo, se obtienen firmas XAdES-LTA Level, CAdES-LTA Level o PAdES-LTA Level, con las que se asegura la verificación de las firmas. Puede añadirse más de un sello de tiempo de archivo, asegurándose de que, antes de incluirlo en la firma, se han incluido también todas las evidencias necesarias para su validación, como la información de revocación de sellos de tiempo de archivo previos.

La transformación de una firma en firma longeva puede realizarse, tanto por el firmante, como por el verificador, ya que se trata de la inclusión de elementos de verificación en la estructura de las firmas. Cuando las firmas se transfieren entre partes, es recomendable que el firmante genere las firmas con el nivel de longevidad necesario, para permitir a la parte receptora de la firma (verificador), verificarla en el momento de su recepción.

El archivo de las firmas a largo plazo, si se desea permitir su verificación posterior, requiere, por lo general, un nivel LTA. Pero podría realizarse con un nivel inferior, combinado con otras técnicas de preservación de evidencias, como a través de sistemas acorde a la especificación técnica TS 101 533- Data Preservation Systems Security. Dichos sistemas de preservación de evidencias no son objeto de las políticas de firma.

8. DEFINICIONES Y ACRÓNIMOS

8.1. Definiciones

@firma: Plataforma de firma electrónica del Ministerio de Hacienda y Función Pública.

Aplicación: Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de la informática.

Autenticación (1): Acreditación por medios electrónicos de la identidad de una persona–o ente, del contenido de la voluntad expresada en sus operaciones, transacciones y documentos, y de la integridad y autoría de estos últimos.

Autenticación (2): Proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico. [Reglamento (UE) 910/2014].

Autenticidad: Referido a un documento, propiedad que puede atribuírsele como consecuencia de que puede probarse que es lo que afirma ser, que ha sido creado o enviado por la persona de la cual se afirma que lo ha creado o enviado, y que ha sido creado o enviado en el momento en que se afirma, sin que haya sufrido ningún tipo de modificación.

Certificado de atributos: Conjunto de atributos de un usuario junto con alguna otra información, hechos infalsificables por el cifrado con la clave privada de la autoridad de certificación que la emitió. Registro que liga una persona física con datos relacionados con su actividad, sus estudios, pertenencia a asociaciones,... Este certificado sirve para respaldar que el ciudadano puede realizar determinadas acciones como miembro de un colectivo.

Certificado de autenticación de sitio web: Declaración electrónica que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se le ha expedido el certificado. Se trata de certificados de autenticación y garantía de integridad, no de firma. [Reglamento (UE) 910/2014].

Certificado cualificado de autenticación de sitio web: Certificado de autenticación de sitio web expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo IV. [Reglamento (UE) 910/2014].

Certificado cualificado de firma electrónica: Certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I. [Reglamento (UE) 910/2014].

Certificado cualificado de sello electrónico: Certificado de sello electrónico que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III. [Reglamento (UE) 910/2014].

Certificado electrónico: Según el artículo 6 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, documento firmado electrónicamente por un prestador de

servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Certificado electrónico reconocido: Según el artículo 11 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley, en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes, y a la fiabilidad y las garantías de los servicios de certificación que presten.

Certificado de firma electrónica: Declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona. [Reglamento (UE) 910/2014].

Certificado de sello electrónico: Declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona. [Reglamento (UE) 910/2014].

Ciudadano: Cualesquiera personas físicas, personas jurídicas y entes sin personalidad que se relacionen, o sean susceptibles de relacionarse, con las Administraciones Públicas.

Código seguro de verificación (CSV): Código único que vincula un documento electrónico al órgano u organismo responsable y, en su caso, a la persona firmante del documento. Sirve para la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Conversión: Proceso de transformación de un documento u otro objeto digital de un formato, o versión de formato, a otro.

Copia: Duplicado de un objeto, resultante de un proceso de reproducción.

Creador de un sello: Persona jurídica que crea un sello electrónico. [Reglamento (UE) 910/2014].

Dato: Una representación de hechos, conceptos o instrucciones de un modo formalizado, y adecuado para su comunicación, interpretación o procesamiento por medios automáticos o humanos.

Declaración de prácticas de certificación: Especificación, emitida por el prestador de servicios de certificación, de las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos que expide.

Dirección electrónica: Identificador de un equipo o sistema electrónico desde el que se provee de información o servicios en una red de comunicaciones.

Disponibilidad: Referido a un documento, indica la propiedad o característica del mismo, que permite que éste pueda ser localizado, recuperado, presentado o interpretado. El documento debe señalar la actividad o actuación donde se generó, proporcionar la información necesaria para la comprensión de las actuaciones que motivaron su creación y utilización, identificar el contexto marco de las actividades y

las funciones de la organización y mantener los vínculos existentes con otros documentos como reflejo de una secuencia de actuaciones.

Dispositivo cualificado de creación de firma/sello: Dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II. [Reglamento (UE) 910/2014].

Documento: Información de cualquier naturaleza archivada en un soporte y susceptible de identificación y tratamiento diferenciado.

Documento electrónico (1): Información de cualquier naturaleza, en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Documento electrónico (2): Todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual. [Reglamento (UE) 910/2014].

Dominio: Ámbito real o imaginario de una actividad.

Emisor y gestor de la política de firma: Entidad que se encarga de generar y gestionar el documento de política de firma y sello, por el cual se deben regir el firmante, el verificador y los prestadores de servicios, en los procesos de generación y validación de firma electrónica.

Especificación técnica: Especificación que figura en un documento en el que se definen las características requeridas de un producto, tales como los niveles de calidad, el uso específico, la seguridad o las dimensiones, incluidas las prescripciones aplicables al producto en lo referente a la denominación de venta, la terminología, los símbolos, los ensayos y métodos de ensayo, el envasado, el marcado y el etiquetado, así como los procedimientos de evaluación de la conformidad.

Estándar: Especificación técnica aprobada por un organismo de normalización reconocido para una aplicación repetida o continuada, cuyo cumplimiento no sea obligatorio y que esté incluida en una de las siguientes categorías:

i. Norma internacional: norma adoptada por una organización internacional de normalización y puesta a disposición del público.
ii. Norma europea: norma adoptada por un organismo europeo de normalización y puesta a disposición del público.
iii. Norma nacional: norma adoptada por un organismo nacional de normalización y puesta a disposición del público.

Estándar abierto: Aquél que reúne las siguientes condiciones:

i. Que sea público y su utilización esté disponible de manera gratuita o a un coste que no suponga una dificultad de acceso.
ii. Que su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.

Expediente electrónico: Conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.

Fiabilidad: Referido a un documento, propiedad o característica que indica que su contenido puede ser considerado una representación completa y precisa de las actuaciones, las actividades o los hechos de los que da testimonio y al que se puede recurrir en el curso de posteriores actuaciones o actividades.

Firma electrónica (1): 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 (2): Datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar. [Reglamento (UE) 910/2014].

Firma electrónica avanzada: Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, 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 utilizar, con un alto nivel de confianza, bajo su exclusivo control.

Firma electrónica cualificada: Firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica. [Reglamento (UE) 910/2014].

Firma electrónica longeva: Firma electrónica que permite garantizar su validez a lo largo del tiempo, incluso una vez vencido el periodo de validez del certificado.

Firma electrónica reconocida: Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Firmante (1): Persona física que crea una firma electrónica utilizando datos de creación de firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

Firmante (2): Persona física que crea una firma electrónica. [Reglamento (UE) 910/2014].

Formato: Conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria.

Función hash: Aplicado a un documento electrónico, función que permite obtener una secuencia de valores de longitud fija, resumen de su contenido (huella digital / binaria o hash), y que identifica unívocamente el documento sobre el que se generó.

Huella digital / binaria o hash: Secuencia de valores resultado de la aplicación de una función hash a un documento electrónico.

Identidad: Conjunto de características de un documento que lo identifican de manera única y lo distinguen de cualquier otro documento. Junto con la integridad, un componente de la autenticidad.

Integridad: Referido a un documento, propiedad o característica que indica su carácter de completo, sin alteración de ningún aspecto esencial. La integridad es un componente de la autenticidad junto a la identidad.

Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

Interoperabilidad en el tiempo: Dimensión de la interoperabilidad relativa a la interacción entre elementos que corresponden a diversas oleadas tecnológicas; se manifiesta especialmente en la conservación de la información en soporte electrónico.

Interoperabilidad organizativa: Dimensión de la interoperabilidad relativa a la capacidad de las entidades y de los procesos a través de los cuales llevan a cabo sus actividades, para colaborar con el objeto de alcanzar logros mutuamente acordados relativos a los servicios que prestan.

Interoperabilidad semántica: Dimensión de la interoperabilidad relativa a que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación.

Interoperabilidad técnica: Dimensión de la interoperabilidad relativa a la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como las interfaces, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad, u otros de naturaleza análoga.

Lista de revocación de certificados (CRL): Lista de certificados que han sido revocados o, por alguna otra razón, ya no son válidos.

Lista de servicios de confianza (TSL): Lista, de acceso público, que recoge información precisa y actualizada de aquellos servicios de certificación y firma electrónica que se consideran aptos para su empleo en un marco de interoperabilidad de las Administraciones Públicas españolas y europeas.

Marca de tiempo: Asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

Online Certificate Status Protocol (OCSP): Protocolo para determinar el estado de revocación de certificados electrónicos vía mensajes http.

Organización: Cualquier órgano de la Administración Pública o Entidad de Derecho Público vinculada o dependiente de aquélla.

Periodo de precaución o de gracia: Tiempo de espera recomendado para la comprobación del estado de revocación de un certificado. Se utiliza para prevenir posibles demoras en la actualización de los sistemas de información de revocación de certificados.

Política de firma electrónica: Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

Política marco: Política de firma electrónica que puede servir como marco general de interoperabilidad para el desarrollo de políticas particulares, con el objeto de cubrir necesidades específicas de las organizaciones para una transacción determinada, en un contexto concreto, o bien para su adopción como política de firma electrónica de una organización. Las políticas marco pueden convivir junto con otras políticas particulares. Un ejemplo de política marco, es la Política de firma de la Administración General del Estado.

Prestador cualificado de servicios de confianza: Prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación. [Reglamento (UE) 910/2014].

Prestadores de servicios de confianza (PSC): Persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado, bien como prestador no cualificado de servicios de confianza.

Procedimiento administrativo: Proceso formal, jurídicamente regulado para la toma de decisiones por parte de las Administraciones Públicas, para garantizar la legalidad, eficacia, eficiencia, calidad, derechos e intereses presentes y que termina con una resolución en la que se recoge un acto administrativo. Este proceso, se implementa en la práctica mediante un proceso operativo que coincide en mayor o menor medida con el formal.

Proceso operativo: Conjunto organizado de actividades que se llevan a cabo para producir un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Sede electrónica: A efectos de interoperabilidad, aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones de la que es titular una Administración Pública, órgano o entidad administrativa.

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

Sello cualificado de tiempo electrónico: Sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42. [Reglamento (UE) 910/2014].

Sello electrónico: Datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos. [Reglamento (UE) 910/2014].

Sello electrónico cualificado: Sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico. [Reglamento (UE) 910/2014].

Sello de tiempo: 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.

Sello de tiempo electrónico: Datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante. [Reglamento (UE) 910/2014].

Sistema de firma electrónica: Conjunto de elementos intervinientes en la creación de una firma electrónica. En el caso de la firma electrónica basada en certificado electrónico, componen el sistema, al menos, el certificado electrónico, el soporte, el lector, la aplicación de firma utilizada y el sistema de interpretación y verificación utilizado por el receptor del documento firmado.

Soporte: Objeto sobre el cual o en el cual es posible grabar y recuperar datos.

Validación: Proceso de verificar y confirmar la validez de una firma o sello electrónicos. [Reglamento (UE) 910/2014].

Verificador: Persona física o jurídica que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por una política de firma y sello concreta por la que se rige la plataforma de relación electrónica o el servicio concreto que se esté invocando. Podrá ser una entidad de validación de confianza o una tercera parte que esté interesada en la validez de una firma electrónica.

8.2. Acrónimos

AGE: Administración General del Estado.

ASN.1: Abstract Syntax Notation One.

BES: Basic Electronic Signature.

CAdES: CMS Advanced Electronic Signatures.

CCN: Centro Criptológico Nacional.

CE: Comisión Europea.

CMS: Cryptographic Message Syntax.

CRL: Certificate Revocation List.

CSAE: Consejo Superior de Administración Electrónica.

CSV: Código Seguro de Verificación.

ENI: Esquema Nacional de Interoperabilidad.

ENS: Esquema Nacional de Seguridad.

EPES: Explicit Policy based Electronic Signature.

ISO: International Organization for Standardization

NTI: Norma Técnica de Interoperabilidad.

OCSP: Online Certificate Status Protocol.

OID: Object Identifier.

PAdES: PDF Advanced Electronic Signatures.

PDF: Portable Document Format

PSC: Prestador de servicios de confianza.

TSA: Time Stamping Authority.

TSP: Time-Stamp Protocol.

URI: Uniform Resource Identifier.

URL: Uniform Resource Locator.

UTC: Universal Time Coordinated.

XAdES: XML Advanced Electronic Signatures.

XML: eXtensible Markup Language.

XML-DSig: XML Digital Signature.

9. REFERENCIAS

9.1. Legislación

i. Código de Administración Electrónica

Codigo_de_Administracion_Electronica

ii. Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

DOUE-L-2014-81822

iii. Decisión de Ejecución (UE) 2015/1506 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo.

DOUE-L-2015-81819

iv. Decisión de Ejecución (UE) 2015/1505 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo.

DOUE-L-2015-81818

9.2. Estándares y buenas prácticas

i. ETSI TS 101 733, v.1.6.3 y v.1.7.4. Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).

http://webapp.etsi.org/workProgram/Report_WorkItem.asp?wki_id=30997

ii. ETSI TS 103173 v.2.2.1. Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile

http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf

iii. ETSI TS 101 903, v.1.2.2, v.1.3.2 y v.1.4.1. Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES).

http://webapp.etsi.org/workProgram/Report_WorkItem.asp?wki_id=28064

iv. ETSI TS 103171 v.2.1.1. Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile

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

v. ETSI TS 102 778 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signatures (PAdES)

http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf

http://www.etsi.org/deliver/etsi_ts/102700_102799/10277802/01.02.01_60/ts_10277802v010201p.pdf

http://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/01.02.01_60/ts_10277803v010201p.pdf

http://www.etsi.org/deliver/etsi_ts/102700_102799/10277804/01.01.02_60/ts_10277804v010102p.pdf

vi. ETSI TS 103 172 V2.2.2 Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile

http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

vii. ETSI EN 319 421. Trust Service Providers issuing Time-Stamps

http://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf

viii. ETSI EN 319 422. Time-stamping protocol and time-stamp token profiles

http://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf

ix. ETSI TS 102 176-1, v.2.1.1. Electronic Signatures and Infrastructures (ESI); Algorithms and parameters for secure electronic signature. Part 1: Hash functions and asymmetric algorithms

http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.01.01_60/ts_10217601v020101p.pdf

x. ETSI EN 319 412. Certificate profiles

http://www.etsi.org/standards-search#page=1&search=319 412

xi. ESTI TS 119 172-1 v1.1.1. Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents.

http://www.etsi.org/deliver/etsi_ts/119100_119199/11917201/01.01.01_60/ts_11917201v010101p.pdf

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

http://www.etsi.org/deliver/etsi_tr/102000_102099/102045/01.01.01_60/tr_102045v010101p.pdf

xiii. IETF RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

http://www.ietf.org/rfc/rfc2560

xiv. IETF RFC 3125, Electronic Signature Policies.

http://www.ietf.org/rfc/rfc3125

xv. IETF RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

http://www.ietf.org/rfc/rfc3161

xvi. IETF RFC 5280, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.

http://www.ietf.org/rfc/rfc5280.txt

xvii. IETF RFC 5652, Cryptographic Message Syntax (CMS).

http://tools.ietf.org/html/rfc5652

xviii. Recommendation X.680 (1997): Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation.

http://www.itu.int/ITU-T/studygroups/com10/languages/X.680_0699_Amend1.pdf

xix. Web Services Security: SOAP Message Security 1.1 (WS-Security 2004):

http://www.oasis-open.org/committees/download.php/21255/wss-v1.1-spec-errata-os-SOAPMessageSecurity.pdf

xx. Serie 400: CCN-STIC-405 Algoritmos y parámetros de firma electrónica:

https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/400-guias-generales.html

xxi. Serie 800: CCN-STIC-807 Criptología de empleo en el ENS.

https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

9.3. Documentos de trabajo y referencias

i. Política de Firma Electrónica y de Certificados de la Administración General del Estado:

http://administracionelectronica.gob.es/ctt/politicafirma/descargas

ii. Lista de prestadores cualificados de servicios de confianza publicada por el Ministerio de Energía, Turismo y Agenda Digital:

http://www.minetad.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx

iii. Plataforma de validación de firma electrónica (@firma):

http://administracionelectronica.gob.es/ctt/afirma

ANEXO I – EQUIPO RESPONSABLE DEL PROYECTO

Coordinador del proyecto

Amutio Gómez, Miguel A.	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

Responsable de edición

Vigón Arvizu, Beatriz	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

Calidad y Publicación

Juez Alonso, Paloma	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

Grupo de expertos:

Administración General del Estado

Agurruza Mutuberría, Jokin	INSTITUTO NACIONAL DE ESTADÍSTICA
Alburquerque Pernías, Francisco	MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL DE LA POLICÍA
Alberto Martín, Félix	MINISTERIO DE JUSTICIA
Alcaide García, Aleida	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Alcolea Muñoz, Antonio	MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
de Alfonso López, Ricardo	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
de Amil Villarrubia, Pablo	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Amores Molero, Felipe	FÁBRICA NACIONAL DE MONEDA Y TIMBRE
Aragonés Arribas, Félix Jesús	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Arranz, Candelas	AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA
Ballesteros Arjona, Juan Jesús	MINISTERIO DE FOMENTO
Barba Lobatón, Jesús	MINISTERIO DE JUSTICIA
Barrón Basterrechea, José Luis	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Beltrán, Ana	MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE
Berral López Alfonso	MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL DE TRÁFICO
Blanco Arribas, Miguel Ángel	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Bustos Pretel, Gerardo	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Cabezas Manso, Laura	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Candau, Javier	CENTRO CRIPTOLÓGICO NACIONAL
Caruana De las Cagigas, Elisa	MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
Del Caño Gil, Cristina	MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
Casado Robledo, Mª Jesús	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Cívicos Villa, Noemí	MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES
Conejo Fernández, Carmen	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Corral Guinea, Myriam	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Crespo Sánchez, Juan	MINISTERIO DEL INTERIOR – DIRECCIÓN GENERAL DE LA POLICIA
Criado Gómez, Isabel	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Cubo Contreras, Aitor	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Cueva Calabia, José Luis	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Desantes Fernández, Blanca	MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE
De la Calle Vian, Elena	MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
Delgado Casanova, Ricardo	MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN
De Miguel de Santos, María	MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
Díez Pérez, Esther	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Eguíluz Gauna, Jesús	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
Escapa Castro, Lucía	MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES
Eusamio Mazagatos, José Antonio	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

Fernández Crespo, María Esther	MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL DE LA POLICÍA
Fernández Lombardía, Oscar	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Fradua García-Soto, Idoia	MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE
Fuentes Bajo, Ricardo	MINISTERIO DE AGRICULTURA Y PESCA, ALIMENTACIÓN Y MEDIO AMBIENTE
Franco Espino, Beatriz	MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE
Galindo Alonso, Olga	GERENCIA DE INFORMÁTICA Y SEGURIDAD SOCIAL
Gamarra, Juan Carlos	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Garcés, Juan Carlos	CONSEJO GENERAL DEL PODER JUDICIAL
García Celada, Joseba	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
García Gómez, Eugenio	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL - SEPE
García Martín, Mª Jesús	MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
García Martínez, José Luis	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Gijón Romero, Francisco	MINISTERIO DE FOMENTO
Gil Navalón, Roberto	MINISTERIO DE DEFENSA
Gómez Muñoz, Carlos Francisco	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Gómez Plaza, Carlos	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
Gómez Raya, José Ignacio	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Gómez Vaz, Manuel	MINISTERIO DE FOMENTO
González Rufo, Mª Ángeles	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Gonzalo Ramírez, Alberto	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Graña Domínguez, Santiago	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL - SEPE
Hernández Vicente, Severiano	MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE
Hernández Gallardo, Diego	FÁBRICA NACIONAL DE MONEDA Y TIMBRE
Hernández Jiménez, Francisco	INSTITUTO NACIONAL DE ESTADÍSTICA
Hernández Maroto, Mª Dolores	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Hernández Vigliano, Julián	MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES
Herrero García, Carlos	MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE
Horganero Gómez, Sara	MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN
Hortigüela Hortigüela, Concha	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL - GISS
Iniesta Sánchez, Fernando	MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES
Jaqueti, Francisco Javier	INSTITUTO NACIONAL DE ESTADÍSTICA
Jara González, Francisco José	MINISTERIO DEL INTERIOR – DIRECCIÓN GENERAL DE LA POLICIA
Jiménez Muñoz, Luis	CENTRO CRIPTOLÓGICO NACIONAL
Lago Bagues, Ramiro José	MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
Lapuente Perea, José Luis	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
López Crespo, Francisco	MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN
López Herrero, Miguel Ángel	MINISTERIO DE FOMENTO
Lorenzo Fernández, Laura	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
Lucas Vegas, Mª José	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
Llorens González, Juan de Dios	MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
Mañes Guerras, Santos	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
Martín García, Raúl	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL - SEPE
Martín Lázaro, Francisco José	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Martín Marcos, Miguel	MINISTERIO DE DEFENSA
Martín Rey, Rosa Mª	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Martínez Muñoz, David	MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN
Martínez Vidal, Miguel Ángel	INSTITUTO NACIONAL DE ESTADÍSTICA
Maza Frechín, Carlos	MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
Merchán Arribas, Montaña	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
De Miguel Santiago, María Luz	MINISTERIO DE AGRICULTURA Y PESCA, ALIMENTACIÓN Y MEDIO AMBIENTE
Millaruelo Gómez, Alejandro	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

Molina Moscoso, Domingo	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Montes Antona, Javier	FÁBRICA NACIONAL DE MONEDA Y TIMBRE
Muñoz Montalvo, Juan Fernando	MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
Muñoz Salinero, Elena	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Ochando Perales, Javier	MINISTERIO DE DEFENSA
Ortiz Tovar, Eva María	MINISTERIO DE JUSTICIA
Otheo de Tejada, Josefina	AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA
De la Paz Rincón, Antonio	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Pardo, Jesús	FÁBRICA NACIONAL DE MONEDA Y TIMBRE
Pastor Bermúdez, Andrés	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL - GISS
Pérez Alcázar, Ricard	MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE
Pérez Galindo, Rafael	MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
Pérez de Lema Sáenz de Viguera, Andoni	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Rada Muruaga, Begoña	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Ramos Curto, Juan Francisco	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Requejo Zalama, Javier	MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE
Rincón Mirón, Jorge Antonio	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
del Río Molini, Mario	MINISTERIO DE DEFENSA
Robledo Pascual , Óscar	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Rodríguez Hervás, Francisco Javier	MINISTERIO DEL INTERIOR
Rodríguez Escolar, Nimia	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Rodríguez Ramos, Miguel Ángel	MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
Román Cortés, Juan Carlos	AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA
Rubio Martínez, Javier	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Ruiz del Corral, Manuel	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Ruiz de Garibay Cubillo, Andrea	AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA
Salom, Juan	GUARDIA CIVIL
San Atanasio, Pinar	AGENCIA ESTATAL DE METEOROLOGÍA
Sánchez Abad, Mª Pilar	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Sánchez Agulló, Pablo	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Sanz Pulido, Antonio	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
Sobrino Moreno, José María	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Tapias Sancho, Álvaro	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Triguero Garrido, Mario	GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL
Valcárcel Lucas, Pedro-Castor	GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL
Vallejo Echevarría, Maite	MINISTERIO DE JUSTICIA
Vega Fidalgo, Luis Miguel	GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL
Vélez Fraga, Santiago	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Vigón Arvizu, Beatriz	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Villafranca Ramos, Alberto	MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES
Viñado Villuendas, Pilar	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Villalba Tomás	MINISTERIO DEL INTERIOR
Zapardiel, Juan Antonio	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Zapico, Alberto	AGENCIA ESTATAL DE LA ADMINISTRACIÓN TRIBUTARÍA

Comunidades Autónomas

Andrés Sevillano, Albert	ARAGÓN
Báez Rodríguez, Luis Alberto	CANARIAS
Barras, Juan Antonio	CASTILLA Y LEÓN
Del Barrio Morón, Antonio	CASTILLA-LA MANCHA
Berjano Tartiere, Bárbara	ASTURIAS
Cantabrana González, Ricardo	ARAGÓN
Cañal Villanueva, Mª José	CASTILLA Y LEÓN

Castellano, Enrique	CANARIAS
Cortés Domingo, Rubén	CATALUÑA
Chapado Gregorio, Susana	COMUNITAT VALENCIANA
Esparza Ruiz, Catalina	REGIÓN DE MURCIA
Fernández Requejo, Antonio	EXTREMADURA
Font Bibiloni, Andreu	ILLES BALEARS
Galán Huertos, Pilar	CASTILLA Y LEÓN
Gallego Español, Rosa María	CATALUÑA
Garay, Raquel	PAÍS VASCO
García Carrera, Diego	CASTILLA Y LEÓN
García Sexto, María José	JUNTA DE GALICIA
González Rodríguez, Manuel de los Reyes	CANARIAS
Izco García, Fernando	NAVARRA
López González, Mª del Rosario	ASTURIAS
Lozano Cantín, Mª Ángel	ARAGÓN
Marín Cruz, Pepa	COMUNIDAD DE MADRID
Martínez Pelayo, Paula	ASTURIAS
Moreno, Ángel	LA RIOJA
Ojeda Pérez, Juan Sebastián	ANDALUCIA
Olivares Sánchez, Pedro	REGIÓN DE MURCIA
Perera Domínguez, Manuel	ANDALUCIA
Rodríguez Parraga, José María	CASTILLA Y LEÓN
Rodríguez Rodríguez, Juan Carlos	PRINCIPADO DE ASTURIAS
Rosat Jorge, José Luis	CASTILLA Y LEÓN
Ruíz Benítez, Mª del Carmen	CANARIAS
Sánchez Melero, Arturo	COMUNIDAD DE MADRID
Saro, Javier	CANTABRIA
Sáez de Vicuña, Asier	PAÍS VASCO
Zorita Pacheco, Antonio	EXTREMADURA

Corporaciones Locales

Bárcenas Gutiérrez, Pablo	FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

Universidades

Sánchez Martínez, Daniel	CONFERENCIA DE RECTORES DE LAS UNIVERSIDADES ESPAÑOLAS

Otras Instituciones

de Ocaña Lacal, Daniel	TRIBUNAL CONSTITUCIONAL