GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
SECRETARÍA DE ESTADO PARA LA FUNCIÓN PÚBLICA
DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA
@dministración electrónica

Esquema Nacional de Interoperabilidad

GUÍA DE APLICACIÓN DE LA NORMA TÉCNICA DE INTEROPERABILIDAD

Política de Firma Electrónica y de certificados de la Administración

Madrid, octubre 2011

Esta publicación ha sido elaborada por la Dirección General para el Impulso de la Administración Electrónica

1ª edición electrónica - Versión 01/09/2011

Catálogo general de publicaciones oficiales:
http://publicacionesoficiales.boe.es

Catálogo de publicaciones de la Secretaría General Técnica del Ministerio de Política Territorial y Administración Pública:
http://www.mpt.gob.es/publicaciones.html

Así mismo, se puede encontrar esta publicación en:
http://administracionelectronica.gob.es/

Edita: Ministerio de Política Territorial y Administración Pública
Secretaría General Técnica

NIPO: 850-11-052-4

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.

0. CONSIDERACIONES PREVIAS

Este documento constituye una guía de aplicación de la *Norma Técnica de Interoperabilidad de Política de Firma Electrónica 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.

1. INTRODUCCIÓN

1. El **Esquema Nacional de Interoperabilidad** (en adelante, ENI) se define en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos como "… *el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deben ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad".*

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 la Comisión Permanente del Consejo Superior de Administración Electrónica y el Comité Sectorial de Administración Electrónica.

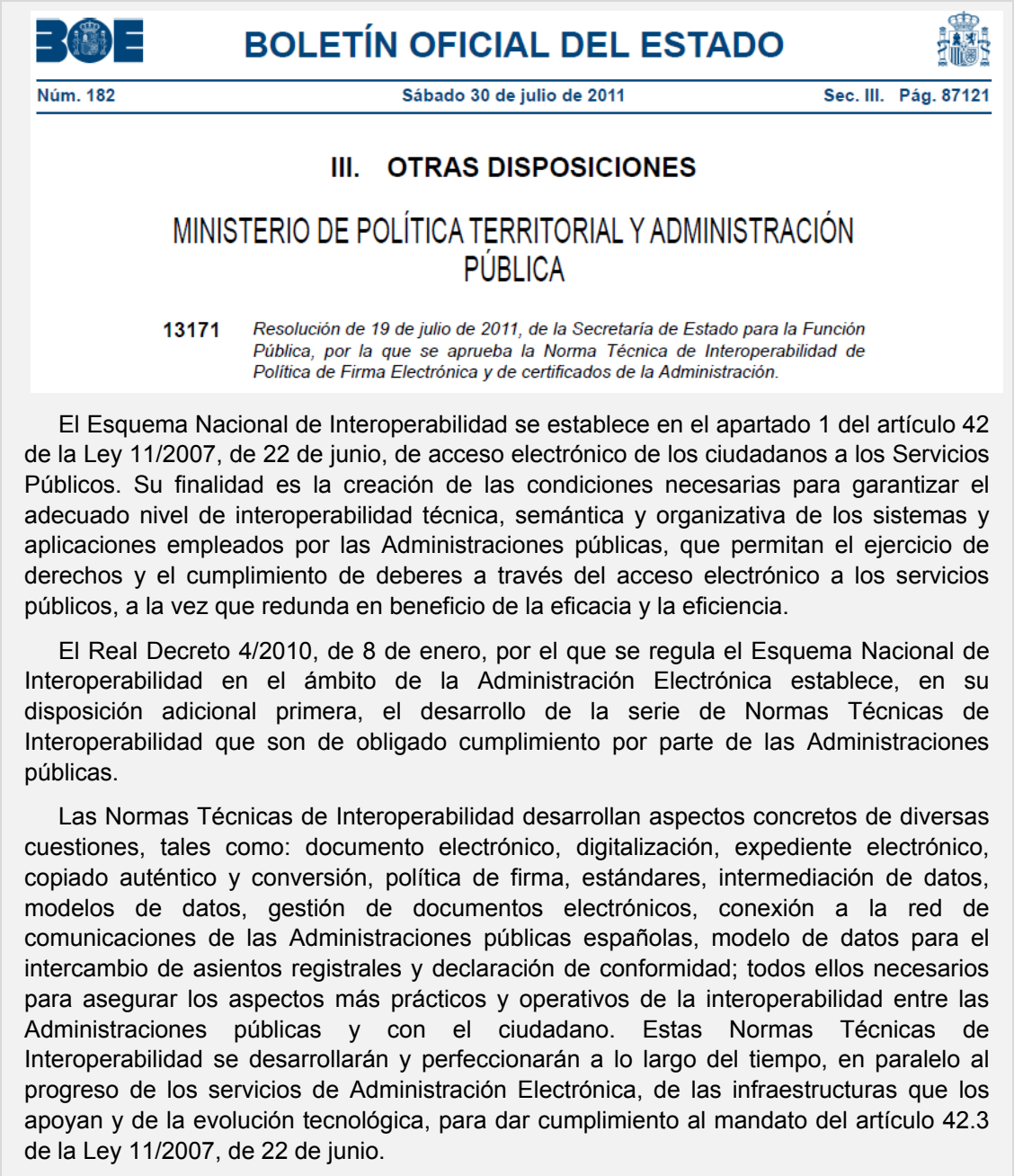
4. Las diferentes NTIs se han desarrollado con el objetivo de cubrir las necesidades derivadas de la normativa aplicable en un planteamiento de partida basado en mínimos, de forma que se garantice la interoperabilidad entre las distintas administraciones favoreciendo su implantación y aplicación en un 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 Electrónica y de certificados de la Administración* establece el conjunto de criterios para el desarrollo o adopción de políticas de firma electrónica basadas en certificados por parte de las Administraciones públicas. Además define el contenido de una política de firma electrónica basada 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. En la NTI también se establecen aspectos de interoperabilidad relativos a los prestadores de servicios de certificación y se definen las funciones de las plataformas de validación de certificados electrónicos y de firma electrónica, cuestiones todas ellas que han de considerarse para el desarrollo de políticas de firma electrónica.

6. La *NTI de Política de Firma Electrónica y de certificados de la Administración* fue publicada en el Boletín Oficial del Estado Número 182 del sábado 30 de julio de 2011 (http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-13171), 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. 182 Sábado 30 de julio de 2011 Sec. III. Pág. 87121

III. OTRAS DISPOSICIONES

MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

13171 *Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.*

El Esquema Nacional de Interoperabilidad se establece en el 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.

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, 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 declaración de conformidad; 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, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, la norma relativa a las políticas de firma responde a lo previsto en el artículo 18 del citado Real Decreto 4/2010, de 8 de enero, sobre la interoperabilidad en la política de firma electrónica y de certificados.

En particular, la Norma Técnica de Interoperabilidad 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 electrónica basada en certificados por parte de las Administraciones públicas. Para ello, define el contenido de una política de firma electrónica basada 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 pretenden establecer un marco para la definición de políticas de firma electrónica basada en certificados alineada con las últimas tendencias a nivel europeo como es la Decisión de la Comisión 2011/130/EU de 25 de febrero de 2011 por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior, compatible a su vez con sistemas de firma electrónica ya implantados.

La presente 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 la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta 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 electrónica y de certificados de la Administración, cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Política de firma electrónica 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», sin perjuicio de lo dispuesto en la Disposición Transitoria primera 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.

Madrid, 19 de julio de 2011.–La Secretaria de Estado para la Función Pública, María Consuelo Rumí Ibáñez.

8. El texto completo de la *NTI de Política de Firma Electrónica y de certificados de la Administración* está formado por los siguientes cuatro apartados y un anexo:

NORMA TÉCNICA DE INTEROPERABILIDAD DE POLÍTICA DE FIRMA ELECTRÓNICA Y DE CERTIFICADOS DE LA ADMINISTRACIÓN.

ÍNDICE

I.2 Ámbito de aplicación.

II. La política de firma electrónica.

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.

II.7 Archivado y custodia.

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.

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.

Anexo. Etiquetas de creación y validación de firmas electrónicas para los formatos admitidos.

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).

2. OBJETIVO Y ALCANCE DE LA NTI DE POLÍTICA DE FIRMA ELECTRÓNICA Y DE CERTIFICADOS DE LA ADMINISTRACIÓN

10. El objeto de la *NTI de Política de Firma Electrónica 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 electrónica 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 basadas en certificados y que, como tales, serán desarrollados y consolidados a través de las políticas de firma electrónica basada en certificados.
>
> 2. El objetivo final de esta NTI es facilitar el uso de firmas electrónicas seguras 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 electrónica basadas en certificados por parte de las Administraciones públicas, es decir, establece una serie de directrices para que éstas desarrollen sus propias políticas de firma 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 electrónica y certificados de la Administración*.

Nótese que la NTI detalla únicamente condiciones para políticas de firmas electrónicas 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 la NTI no incluye ninguna limitación que impidan incluir en la Política de firma, 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 11/2007, de 22 de junio, 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 electrónica 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.

2.1. Qué NO incluye la NTI

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

i. Una política de firma electrónica 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 electrónica 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 11/2007, de 22 de junio, 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)*.

3. ÁMBITO DE APLICACIÓN Y DESTINATARIOS

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

> I.2 Ámbito de aplicación.
>
> El contenido de esta NTI será de aplicación para el desarrollo o adopción de políticas de firma electrónica 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.

17. Por tanto, las indicaciones contenidas en la NTI son de aplicación para el desarrollo de políticas de firma electrónica 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 electrónica y 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 electrónica de las organizaciones.

ii. Responsables de la implantación de políticas de firma electrónica en organizaciones.

4. FIRMA ELECTRÓNICA Y CERTIFICADOS: DEFINICIONES Y CONTEXTO

19. Aunque la NTI no aborda la definición de conceptos de firma electrónica, este punto recoge algunas referencias y conceptos básicos relacionados con la firma electrónica y los certificados que, estando completamente desarrollados en la normativa específica de firma electrónica, es conveniente conocer para una correcta interpretación de la NTI y de esta guía.

20. La Ley 59/2003, de 19 de diciembre, de firma electrónica, es la normativa de referencia para la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

21. Esta Ley distingue los siguientes conceptos:

i. **Firma electrónica:** "*… es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante"*

ii. **Firma electrónica avanzada***: "… es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.*"

iii. **Firma electrónica reconocida:** "*firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma*."

22. Para que una firma electrónica pueda ser considerada **firma electrónica avanzada**, de la Ley 59/2003, de 19 de diciembre, se infieren los siguientes requisitos:

i. **Identificación o autenticación de usuarios**: posibilita garantizar la identidad del firmante de manera única. Existen dos tipos de finalidades de la autenticación:

   a. Identificación del origen de los datos: el identificado está relacionado con ciertos datos que le son propios y que lo vinculan con el mensaje enviado.

   b. Identificación de entidades: comparación de los datos enviados con datos almacenados, enviados anteriormente.

ii. **Integridad:** garantiza que el contenido de un mensaje de datos ha permanecido completo e inalterado, con independencia de los cambios que hubiera podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación.

iii. **No repudio**: es la garantía de que no puedan ser negados los mensajes en una comunicación telemática. Existen dos tipos:

   a. No repudio en origen: garantiza al receptor que el mensaje ha sido enviado por el emisor aunque éste quiera negar tal comunicación.

   b. No repudio en destino: garantiza al emisor que su comunicación ha sido recibida, no pudiendo negar el receptor tal comunicación.

23. Por otra parte, la citada Ley 59/2003, de 19 de diciembre, define el **certificado electrónico** distinguiendo los siguientes conceptos:

i. **Certificado electrónico**: "… *es un 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*".

ii. **Certificado reconocido**: "*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*."

24. En este contexto, la Ley 11/2007, de 22 de junio, recoge otras definiciones de algunos conceptos necesarios para la correcta interpretación de la NTI, por ejemplo, conceptos tales como **Sistema de firma electrónica** o **Sellado de tiempo**, y hace referencia a la citada Ley 59/2003, de 19 de diciembre, para definir otros términos como **Certificado electrónico** o **Firma electrónica**. El R.D. 4/2010 ENI también recoge en su anexo una serie de definiciones de términos relacionados. Todos estos conceptos están recogidos en el punto 8.1 de esta guía.

5. LA POLÍTICA DE FIRMA ELECTRÓNICA

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

> II. *La política de firma electrónica*
>
> 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.
>
> II.7 Archivado y custodia.

5.1. Definición y contenido

26. 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».
>
> 2. ...

27. 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.

28. La finalidad de una política de firma es por tanto 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.

29. 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 electrónica y de certificados definirá:
>
> a) Los procesos de creación, validación y conservación de firmas electrónicas.
> b) Características y requisitos de los sistemas de firma electrónica, certificados y sellos de tiempo.
>
> 3. …

30. 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 electrónica 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.
> b) Datos para la identificación del documento y del responsable de su gestión.
> c) Reglas comunes para el firmante y verificador de la firma electrónica que incluirán:
> i. Formatos admitidos de firma electrónica y reglas de uso de algoritmos.
> ii. Reglas de creación de firma.
> iii. Reglas de validación de firma.
> 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.

31. Atendiendo a este subapartado, una política de firma electrónica 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 actores que participan en una determinada relación o trámite así como 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 electrónica, 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

32. 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 Electrónica 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 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. …

33. Cabe destacar que toda política de firma 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

34. Una política de firma electrónica y 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.

35. 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.

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

37. 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 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

38. 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 electrónica basada en certificados incluirá:
>
> a) Nombre del gestor de la política.

b) Dirección de contacto.
c) OID del gestor de la política de firma.

39. Las consideraciones para la gestión de una política de firma electrónica son objeto del subapartado II.6 de la NTI, que se desarrolla en el punto 5.6 de esta guía.

5.3. Actores involucrados en la firma electrónica

40. Como ya se ha mencionado, toda política de firma electrónica 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 la propia firma, bien en su creación o en su validación.

41. El subapartado II.3 de la *NTI de Política de Firma Electrónica 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: persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.
>
> b) 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 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.
>
> c) Prestador de servicios de certificación (PSC): persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
>
> d) Emisor y gestor de la política de firma: entidad que se encarga de generar y gestionar el documento de política de firma, 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.

42. 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.

5.4. Usos de la firma electrónica

43. 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.

44. 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 electrónica 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.

45. 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.

46. Nótese que la NTI se limita a citar posibles usos de la firma electrónica que podrían ser contemplados en una política de firma electrónica 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 de general de un sector específico que incluya tratamiento de documentos electrónicos, correos y transmisiones, como en una política específica que sólo definiese condiciones para el intercambio seguro de información en un determinado trámite. El desarrollo de una política de firma electrónica definiría los usos de la firma 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.

47. 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.

48. 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.

49. 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.

50. 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.

51. 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.

52. 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.

53. 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

54. Las organizaciones pueden optar por desarrollar sus propias políticas particulares adaptadas a sus necesidades específicas, o bien, utilizar una política marco, demostrada herramienta de interoperabilidad.

55. 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 electrónica y certificados de la Administración.*

56. Por ejemplo, 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 electrónica y certificados de la Administración*.

57. 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"*.

58. 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.

59. 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. Cada organización valorará la necesidad y conveniencia de desarrollar una política propia frente a la posibilidad de utilizar una política marco existente.
>
> 2. La definición del alcance y ámbito de aplicación de una política de firma electrónica se realizará considerando su interacción con otras políticas de firma electrónica, y asegurando que:
>
> a) Su desarrollo es interoperable con la política marco, en caso de políticas de firma 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 electrónica 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).

60. 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 electrónica debe realizarse considerando su interacción con otras políticas de firma electrónica.

61. Por tanto, de forma general, toda organización debe, en primer lugar, valorar la necesidad de desarrollar una política propia en lugar de acogerse a políticas existentes. Además, en su desarrollo, para asegurar la interacción con otras políticas, debe atenderse a lo establecido en el epígrafe II.5.3 de la NTI.

5.6. Gestión de la política de firma

62. La *NTI de Política de Firma Electrónica 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.

1. La política de firma electrónica 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 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.

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.

63. Por lo tanto, el gestor de la política de firma, 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.

64. 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

65. La *NTI de Política de Firma Electrónica 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 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 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 definirá un servicio para mantener las evidencias de validez de las firmas longevas y gestionar la actualización de las firmas. Dicho servicio especificará los mecanismos y condiciones bajo los que se archiva y custodia tanto la propia firma 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 AdES -X o -A.
> 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 electrónica 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, para añadir, cuando el anterior sellado este próximo a su caducidad, un sello de fecha y hora de archivo con un algoritmo más robusto.
> Las políticas de firma podrán definir la aplicación de mecanismos de resellado para facilitar la conservación de la firma electrónica.

b) Almacenamiento de la firma electrónica en un depósito seguro, garantizando la protección de la firma contra falsificaciones y asegurando la fecha exacta en que se guardó la firma electrónica.

Las operaciones de fechado se realizarán con marcas de fecha y hora, no siendo necesario su sellado de tiempo.

6. La definición de medidas y procedimientos para archivado y custodia de firmas electrónicas 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, se atenderá a lo establecido en la NTI de Política de gestión de documentos electrónicos.

66. 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.

67. 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.

68. 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 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

69. 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.

70. Este tipo de reglas técnicas, tal y como refleja el epígrafe III.1.1 de la NTI, 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 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 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, 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 electrónica 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.

6.1. Formatos admitidos de firma electrónica

71. 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 electrónicas basadas en certificados electrónicos, se ajustarán a las especificaciones de los estándares europeos relativos a los formatos de firma electrónica así como a lo establecido en la NTI de Catálogo de estándares.
>
> 2. Los formatos de firma electrónica serán:

a) Estándares abiertos basados en estándares de firma europeos y ampliamente utilizados.

b) Seleccionados de entre los definidos por la Comisión Europea para la política de interoperabilidad de firmas electrónicas que será regulada a través de Decisión Comunitaria.

c) Compatibles con la definición de políticas de generación y validación de firmas para facilitar la interoperabilidad deseada y el automatismo en el tratamiento de firmas electrónicas generadas por distintas organizaciones.

d) Tales que permitan desarrollar funcionalidades avanzadas como la generación de firmas longevas de cara a garantizar su preservación.

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

3. …

72. En este sentido, tal y como apunta el epígrafe III.2.3 de la NTI, cada organización es responsable de determinar los formatos y estructuras concretas de firma a incluir en su política, debiendo aplicar los criterios expuestos en la *NTI de Política de Firma Electrónica y de certificados de la Administración* de forma proporcional al uso y necesidades de la firma electrónica en cada caso. Por ejemplo, para firma de transmisiones de datos, una organización podría descartar la necesidad de utilizar formatos de firmas longevas. En cualquier caso, los formatos utilizados por cada organización deben ser interoperables con la política marco en la que se basan.

III.2 Formatos admitidos de firma electrónica.

2. …

3. Cada organización determinará los formatos y estructuras concretas de firma a incluir en su política, aplicando los criterios expuestos en esta NTI de forma proporcional al uso y necesidades de la firma electrónica en cada caso.

4. …

73. Por otra parte, el epígrafe III.2.4 de la NTI, se centra en la publicación y actualización de las especificaciones de los formatos admitidos en la política de cada organización. Por ejemplo, en la Política de firma de la AGE, el Consejo Superior de la Administración Electrónica (CSAE) es la entidad responsable de dicha tarea.

III.2 Formatos admitidos de firma electrónica.

3. …

4. Cada organización identificará a la entidad gestora encargada de publicar y actualizar la relación de las especificaciones relativas a los formatos admitidos en su política.

5. ...

74. Por último, el epígrafe III.2.5 establece que la política de firma ha de incluir los requisitos a considerar para incluir nuevas versiones de los formatos soportados. Estos requisitos o, en su caso, los procedimientos de actualización, se determinarían en el mismo documento de la política.

III.2 Formatos admitidos de firma electrónica.

4. ...

> 5. La política de firma incluirá los requisitos o, en su caso, procedimientos de actualización, para considerar la inclusión de nuevas versiones de los formatos soportados.

75. 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

76. 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.

77. 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.

78. 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

79. De la misma manera, el subapartado III.4 de la NTI establece los formatos a utilizar para firma electrónica de contenido.

> III.4 Formatos de firma electrónica de contenido.
>
> 1. En la política de firma se especificarán los formatos admitidos para la firma electrónica de contenido.
>
> 2. Los formatos para la firma electrónica de contenido, atendiendo a la NTI de Catálogo de estándares, serán:
>
> 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. ...

80. Los formatos que especifica el epígrafe III.4.2 están completamente alineados con la Decisión 2011/130/EU de 25 de febrero de 2011 por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior.

81. Nótese que la NTI se limita a establecer un conjunto de estándares a considerar en cada política, sobre los que cada organización podrá seleccionar los que considere que mejor se adaptan a sus necesidades específicas. Por ejemplo, la Política de firma de la AGE no contempla PAdES como formato admitido, aunque sí incluye una mención sobre que "*PAdES se tendrá en consideración especial para su estudio y posible incorporación en futuras versiones de la política de firma*".

82. El epígrafe III.4.3 alude al uso de los mecanismos definidos por los diferentes estándares y anteriormente mencionados para la 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 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. …

83. 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 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.

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

84. 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.
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.

85. 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

86. 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[1].

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

[1] *A lo largo de este documento se utilizan los prefijos ds: y xades: para hacer referencia a elementos definidos en los estándares XML-DSig y XAdES, respectivamente.*

i. *Internally detached signature:* en la que se genera un único documento electrónico que contiene el fichero original, codificado en base64[2], y las firmas. Tanto el fichero original como las firmas se encuentran en el mismo nivel XML, vinculados ambos mediante una relación interna.

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.

88. 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. 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. Por tanto, son estructuras cuya inclusión en las políticas de firma de las organizaciones no es recomendable.

6.1.2.2. Formato CAdES

89. 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.

90. 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.

91. Las firmas CAdES con el fin de facilitar la conservación tanto del documento como de la propia firma, cabría contemplar que, de forma general, se generasen con estructura *internally detached* donde, tal y como se explicó en el punto anterior, firma y documento se mantienen en bloques separados pero en el mismo fichero.

92. 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

93. 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.

94. 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.

95. 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.

96. 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.

---

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

97. 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.

98. Nótese que el formato PAdES es un formato de firma que aúna la usabilidad y accesibilidad de un 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 de certificados de la Administración* considera PAdES como formato admitido.

6.2. Reglas de uso de algoritmos

99. 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 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 electrónica, cumpliendo en cualquier caso lo establecido en la NTI de Catálogo de estándares.
>
> 2. Para los entornos de seguridad genérica se tomará la referencia a la URN (Uniform Resource Name) en la que se publican las funciones hash y los algoritmos de firma utilizados por las especificaciones XAdES, CAdES y PAdES, como formatos de firma adoptados, de acuerdo con las especificaciones técnicas ETSI TS 102 176-1, «Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms». Todo ello sin perjuicio de los criterios que al respecto se establezcan atendiendo al Real Decreto 3/2010, de 8 de enero.
>
> 3. Se admitirán como válidos los algoritmos de generación de hash, codificación en base64, firma, normalización y transformación definidos en los estándares XML-DSig (XML Digital Signature) y CMS (Cryptographic Message Syntax).
>
> 4. 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.
>
> 5. La definición de usos de algoritmos podrá contemplar diferentes posibilidades según las necesidades en cada caso.

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

100. 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.

101. Nótese que la NTI se 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 tendría en cuenta lo establecido en la NTI, así como de forma adicional, la *NTI de Documento Electrónico*.

III.6 Reglas de creación de firma electrónica.

1. Las políticas de firma 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 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 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 electrónica puede ser validada para el formato del fichero específico que va a ser firmado.

ii. Los certificados a utilizar han sido expedidos bajo una Declaración de Políticas de Certificación específica y son certificados válidos según la legislación aplicable.

iii. 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.

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 correspondientes asuman dicha validación, antes de aceptar el fichero, formulario u otro objeto binario firmado.

c) El servicio creará un fichero con la firma 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 electrónica 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) Política de firma sobre la que se basa el proceso de generación de firma electrónica.

d) Formato del objeto original.

4. Como datos opcionales, la firma electrónica 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. La información indicada en los epígrafes 3 y 4 del presente subapartado se recogerá en cada formato de firma según las etiquetas del anexo.

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

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

102. Destacar que la NTI establece que el fichero que a firmar no debe contener contenido dinámico que pudiese modificar el resultado de la firma a lo del tiempo. En este sentido cabe contemplar 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 cumple.

103. Además, los epígrafes III.6.6 y III.6.7 establecen consideraciones básicas para la creación de firmas múltiples sobre un mismo contenido pero sin especificar cuestiones de uso más allá que podrán ser definidas por cada organización en función de sus necesidades específicas.

104. 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, 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**.*

105. 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 de electrónica.

1. Las políticas de firma definirán las condiciones particulares bajo las que, en su ámbito, será posible validar la firma electrónica de un documento.

2. En el caso de documentos electrónicos, para acceder a la visualización de la firma, el usuario podrá presentar dicho documento electrónico, que contenga los datos, metadatos y firma o firmas, en una sede electrónica o en otros sistemas generales que proporcionen herramientas de reproducción de documentos electrónicos, como el servicio Valide, en el 060.

3. Las condiciones mínimas que se producirán para la validación de la firma 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 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 lleva un sello de tiempo válido en el momento de la verificación.
b) se trata de firmas longevas 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 aplicable.

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.

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

a) Fecha y hora de la firma: Si se ha realizado el sellado de tiempo, el sello más antiguo dentro de la estructura de la firma se utilizará para determinar la fecha de la firma. 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.

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.

c) Política de firma 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 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, implicará que el verificador dispondrá de los medios para verificar las condiciones impuestas en la política de firma concreta. La disponibilidad de la política de firma 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.

5. Si se han realizado varias firmas sobre un mismo documento, se seguirá el mismo proceso de verificación que con la primera firma, 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 podrá definir sus procesos de validación y de archivado, siempre en consonancia con los requisitos de la política de firma 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 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 a lo largo del tiempo se mantendrá resellando la firma 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, el certificado era válido.

106. 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 y que figuran como anexo a la NTI.

7. REGLAS DE CONFIANZA

107. 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 y 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

108. 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

109. 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 y IV.1.2 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, marco o particulares, podrán fijar limitaciones y restricciones específicas para los certificados electrónicos que admiten en cada uno de los servicios que corresponda, siempre en consideración de la normativa aplicable en cada caso.
>
> 2. Los certificados válidos para ejecutar la firma electrónica de contenido serán los siguientes:
>
> a) Cualquier certificado electrónico reconocido según la Ley 59/2003, de 19 de diciembre, y la Directiva 1999/93/CE, de 13 de diciembre de 1999.
> b) Nuevas tipologías de certificados definidos en la Ley 11/2007, de 22 de junio.
>
> 3. ...

110. Según esto, cualquier certificado electrónico reconocido según la normativa citada en el epígrafe IV.2.a, será considerado como certificado válido. En este sentido cabe contemplar el uso de certificados según el estándar ETSI TS 101 862 (Qualified certificate profile) en el que se define un formato técnico para certificados cualificados que puede ser usado para cumplir los anexos I y II de la Directiva 1999/93/EC del Parlamento Europeo de 13 de diciembre de 1999 sobre el marco comunitario para firmas electrónicas.

111. El epígrafe IV.2.b refleja nuevas tipologías de certificados considerados como admitidos definidos en la Ley 11/2007, más concretamente en su artículo 13 por el que se definen

nuevas formas de identificación y autenticación. Por otra parte, el R.D. 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente dicha Ley, concreta dichos certificados y sus requisitos 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 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 la Ley 11/2007 y sus características.

112. 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.

7.1.2. Requisitos de los prestadores de servicios de certificación

113. Los epígrafes IV.1.3 y IV.1.4 de la NTI establecen los requisitos de los prestadores de servicios de certificación.

> IV.1 Reglas de confianza para los certificados electrónicos.
>
> 2. …
>
> 3. Los requisitos a cumplir por los prestadores de servicios de certificación en relación con la interoperabilidad organizativa, semántica y técnica serán los establecidos en el artículo 21 de la Ley 11/2007, de 22 de junio, en el artículo 19 del Real Decreto 4/2010, de 8 de enero, y en el resto de normativa aplicable en cada caso.
>
> 4. La relación de prestadores de servicios de certificación que emiten certificados reconocidos se podrá consultar en la TSL (Lista de servicios de confianza) publicada en la sede electrónica del Ministerio de Industria, Turismo y Comercio.
>
> 5. …

114. Cabe contemplar que cada política de firma electrónica basada en certificados desarrollase o hiciese referencia a la especificación completa de los requisitos de los prestadores de servicios según la normativa aplicable.

115. Con carácter informativo, la siguiente tabla resume los requisitos a cumplir por los prestadores de servicios de certificación en relación con la interoperabilidad organizativa, semántica y técnica definidos, tal y como menciona el epígrafe tercero, en el artículo 21 de la Ley 11/2007, de 22 de junio, y en el artículo 19 del R.D. 4/2010 ENI.

Interoperabilidad Organizativa	▪ Establecimiento de los usos de los certificados expedidos. ▪ Prácticas al generar los certificados que permitan la aplicación de mecanismos de descubrimiento y extracción de los datos de identidad del certificado. ▪ Definición de la información de los certificados o relacionada con ellos que será publicada por parte del prestador, debidamente catalogada. ▪ Definición de los posibles estados en los pueda encontrarse un certificado. ▪ Niveles de acuerdo de servicio (SLA) definidos y caracterizados para los servicios de validación y de sellado de fecha y hora.
Interoperabilidad Semántica	▪ Definición de los perfiles de certificados que describirán, mediante mínimos, el contenido obligatorio y opcional de los diferentes tipos de certificados que emiten, así como la información acerca de la sintaxis y semántica de dichos contenidos. ▪ Establecimiento de los campos cuya unicidad de información permitirá su uso en labores de identificación.
Interoperabilidad Técnica	▪ Los estándares relativos a políticas y prácticas de certificación y generación de certificados electrónicos. - Estado de los certificados. - Dispositivos seguros de creación de firma. - Programas controladores. - Dispositivos criptográficos. - Interfaces de programación. - Tarjetas criptográficas. - Conservación de documentación relativa a los certificados y servicios. - Límites de los certificados. ▪ La incorporación, dentro de los certificados, de información relativa a las direcciones de Internet donde se ofrecen servicios de validación por parte de los prestadores. ▪ Los mecanismos de publicación y de depósito de certificados y documentación asociada admitidos entre Administraciones públicas.

Tabla 3. Requisitos de interoperabilidad para prestadores de servicios de certificación.

116. Según lo dispuesto en el artículo 23 del R.D. 1671/2009, de 6 de noviembre, “corresponde a los Ministerios de la Presidencia y de Industria, Turismo y Comercio publicar la relación de prestadores de servicios de certificación admitidos y controlar el cumplimiento de las condiciones generales adicionales que se establezcan”. Esto tiene un reflejo directo en el epígrafe IV.1.4 de la NTI.

IV.1 Reglas de confianza para los certificados electrónicos.

> 3. …
>
> 4. La relación de prestadores de servicios de certificación que emiten certificados reconocidos se podrá consultar en la TSL (Lista de servicios de confianza) publicada en la sede electrónica del Ministerio de Industria, Turismo y Comercio.
>
> 5. …

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

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

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

118. Destacar que aunque el MITyC tiene la responsabilidad de supervisar y publicar la relación de prestadores de servicios de certificación, pero será cada organización la que determine los certificados admitidos en su ámbito siempre que éstos cumplan las condiciones establecidas en el artículo 21.1 de la Ley 11/2007, esto es que sean "*tecnológicamente viables y sin que suponga coste alguno para aquellas*".

7.1.3. Reglas de validación de los certificados electrónicos

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

> IV.1 Reglas de confianza para los certificados electrónicos.
>
> 4. …
>
> 5. La política de firma electrónica 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 a la que se ajuste el servicio en cada caso.

120. 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.

121. Además, la política de firma electrónica puede establecer el período de precaución o de gracia que corresponda aplicar para la validación de los certificados. Cabe contemplar 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.

122. 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

123. 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 sello 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 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 elementos básicos de un sello digital de tiempo serán:
>
> a) Datos sobre la identidad de la autoridad emisora del sello: identidad jurídica, clave pública a utilizar en la verificación del sello, número de bits de la clave, algoritmo de firma digital y función hash utilizados.
> b) Tipo de solicitud cursada. Incluyendo, si es un valor resumen o un documento, cuál es su valor y datos de referencia.
> c) Valores resumen «anterior», «actual» y «siguiente».
> d) Fecha y hora UTC (Universal Time Coordinated).
> e) Firma electrónica de todo lo anterior.
>
> 2. 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.
>
> 3. En la política de firma 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.
>
> 4. Los sellos de tiempo seguirán las especificaciones técnicas establecidas en el estándar ETSI TS 102 023, «Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities».

7.3. Reglas de confianza para firmas longevas

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

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

126. 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.

127. 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).

128. Tal y como establece el epígrafe IV.3.3 de la NTI, relativo a reglas de confianza para firmas longevas, en el caso 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.

129. 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.

130. 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 producida o verificada, validando la integridad de la firma, el cumplimiento de los estándares XAdES, CAdES o PAdES y las referencias.
> 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 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 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.

131. Aunque no tiene reflejo directo en la NTI, los siguientes puntos describen las principales características de las estructuras existentes para firmas longevas en cada uno de los formatos contemplados en su subapartado IV.3.

7.3.1. Formato XAdES

132. Dentro del formato de firma XAdES, el formato extendido XAdES-C incorpora dos propiedades no firmadas:

i. *CompleteCertificateRefs*: contiene referencias a todos los certificados de la cadena de confianza necesaria para verificar la firma, excepto el certificado firmante.

ii. *CompleteRevocationRefs*: contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación los certificados.

133. En el caso que se desee incorporar a la firma esta información de validación, se recomienda utilizar el formato XAdES-X, que añade un sello de tiempo a la información anterior.

134. El formato XAdES-XL, además de la información incluida en XAdES-X, incluye dos nuevas propiedades no firmadas: *CertificateValues* y *RevocationValues* que incluyen:

i. Referencias a la información de validación.

ii. Cadena de confianza completa.

iii. CRL o respuesta OCSP obtenida en la validación.

135. En el caso que se desee incorporar a la firma esta información de validación, se recomienda usar el formato XADES-A, que añade un sello de tiempo a la información anterior. En este caso se recomienda usar validación mediante OCSP, ya que mediante este método las propiedades *CertificateValues* y *RevocationValues* son de menor tamaño**.**

7.3.2. Formato CAdES

136. Dentro del formato de firma CAdES, el formato extendido CAdES-C incorpora dos atributos:

i. *Complete-certificate-references***:** contiene referencias a todos los certificados de la cadena de confianza necesaria para verificar la firma.

ii. *Complete-revocation-references***:** contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación de la firma.

137. El formato CAdES-X Long además de la información incluida en CAdES-C, incluye dos nuevos atributos *certificate-values* y *revocation-values* que incluyen:

i. Referencias a la información de validación.

ii. Cadena de confianza completa.

iii. CRL o respuesta OCSP obtenida en la validación.

138. En el caso que se desee incorporar a la firma esta información de validación, la validación mediante OCSP favorece la obtención que las propiedades *certificate-values* y *revocation-values* son de menor tamaño.

139. Por tanto, según el tipo de validación, se recomienda el uso de los siguientes formatos.

i. En el caso que la validación se realice mediante consulta OCSP: los formatos CAdES-X Long type 1 o CAdES-X Long type 2, que añaden un sellado de tiempo a la información incluida en una firma CAdES-X Long. En este caso se incorporan los atributos *certificate-values* y *revocation-values* puesto que la respuesta a una consulta OCSP no ocupa mucho espacio.

ii. En el caso que la validación no pueda realizarse mediante OCSP y se realice mediante consulta a una CRL: los formatos CAdES-X type 1 o CAdES-X type 2, que incluyen un sellado de tiempo a la información incluida en una firma CAdES-C, es decir, a las referencias a las CRL consultada y los certificados de la cadena de confianza. No se recomienda incluir los atributos *certificate-values* y *revocation-values* ya que pueden ser muy voluminosos.

140. En el caso que se esté próximo a la caducidad del sello de tiempo añadido para construir la firma longeva, se puede transformar la firma CAdES-X Long type 1 o CAdES-X Long type 2, en una firma CAdES-A, añadiendo un sellado de tiempo de archivo a la firma anterior.

7.3.3. Formato *PAdES*

141. En caso de forma PAdES, se recomendaría el uso del formato PAdES-Long Term.

142. Al igual que en los casos anteriores, se recomienda usar validación mediante OCSP, ya que el tamaño de la información de validación a añadir es menor.

143. Además se podría añadir un sello de tiempo que incluyese dicha información de validación, ya que la validez de la firma resultante viene determinada por la duración del sello de tiempo que se añade a la firma longeva.

8. DEFINICIONES Y ACRÓNIMOS

8.1. Definiciones

@firma: Plataforma de firma electrónica del Ministerio de Política Territorial y Administración Pública.

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

Autenticación: 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.

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, hechas 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 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 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.

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.

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 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.

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

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

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, 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: Una 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 categorías siguientes:

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 sea 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 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 mantener bajo su exclusivo control.

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.

Firma electrónica: Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Firmante: Persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

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 resumen de su contenido (huella digital / binaria o hash) 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 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.

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.

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.

Prestadores de servicios de certificación (PSC): Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Procedimiento administrativo: Proceso formal regulado jurídicamente para la toma de decisiones por parte de las Administraciones Públicas para garantizar la legalidad, eficacia, eficiencia, calidad, derechos e intereses presentes, que termina con una resolución en la que se recoge un acto administrativo; este proceso formal jurídicamente regulado 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 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 en función de autoridad de sellado de tiempo, que actúa como tercero de confianza, que asegure la exactitud e integridad de la marca de tiempo del documento.

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.

Verificador: Entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por una política de firma concreta. Puede 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

MITyC: Ministerio de Industria, Turismo y Comercio.

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 certificación.

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. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf

ii. Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

http://www.boe.es/boe/dias/2009/11/18/pdfs/BOE-A-2009-18358.pdf

iii. 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.

http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

iv. 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.

http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1331.pdf

v. Ley 59/2003, de 19 de diciembre, de firma electrónica.

http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf

vi. Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica (Diario Oficial n° L 013 de 19/01/2000. pág. 0012-0020).

http://www.boe.es/doue/2000/013/L00012-00020.pdf

vii. ORDEN PRE/2971/2007, de 5 de octubre, sobre la expedición de facturas por medios electrónicos cuando el destinatario de las mismas sea la Administración General del Estado u organismos públicos vinculados o dependientes de aquélla y sobre la presentación ante la Administración General del Estado o sus organismos públicos vinculados o dependientes de facturas expedidas entre particulares.

http://www.boe.es/boe/dias/2007/10/15/pdfs/A41814-41817.pdf

viii. Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad Política de Firma Electrónica y de certificados de la Administración.

http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13171.pdf

ix. Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.

http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-13169

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

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

iii. ETSI TS 102 023, v.1.2.1. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

iv. ETSI TS 102 176-1, v.2.0.0. Electronic Signatures and Infrastructures (ESI); Algorithms and parameters for secure electronic signature. Part 1: Hash functions and asymmetric algorithms

   http://webapp.etsi.org/workProgram/Report_WorkItem.asp?wki_id=25179

v. ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (ESI); XML format for signature policies.

   http://webapp.etsi.org/workProgram/Report_WorkItem.asp?wki_id=13350

vi. ETSI TR 102 041, v.1.1.1. Electronic Signatures and Infrastructures (ESI); Signature policies report.

   http://webapp.etsi.org/workProgram/Report_WorkItem.asp?wki_id=15500

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

   http://webapp.etsi.org/workProgram/Report_WorkItem.asp?wki_id=17211

viii. ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies.

   http://webapp.etsi.org/workProgram/Report_WorkItem.asp?wki_id=19571

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

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

x. IETF RFC 3125, Electronic Signature Policies.

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

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

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

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

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

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

xiv. http://tools.ietf.org/html/rfc5652ITU-T 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

xv. 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

xvi. ETSI TS 101 862. Qualified Certificate profile

http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=23902

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

https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=188&lang=es

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

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/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=239

ii. Lista de servicios de confianza publicada por el Ministerio de Industria, Turismo y Comercio (MITyC):

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

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

http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=190

ANEXO I – INFORMACIÓN Y ETIQUETAS DE FORMATOS DE FIRMA

Este punto refleja el contenido íntegro del anexo de la NTI de Política de Firma Electrónica y de certificados de la Administración.

La siguiente tabla muestra las etiquetas que deben ser utilizadas para reflejar la información del firmante establecida como obligatoria u opcional en el punto 6.3 así como para la validación de la firma electrónica en cada uno de los formatos admitidos según las condiciones establecidas en esta NTI.

La NTI no incluye una definición completa de las etiquetas de creación y validación de firmas electrónicas para los formatos admitidos definidas por cada estándar, sino que se limita a citar aquellas relacionadas con la información de firma mencionada a lo largo del texto.

Información	Obligatoriedad	Campo – etiqueta – elemento[3]		
		XAdES	CAdES	PAdES
Fecha y hora de la firma	Obligatorio	SigningTime (SignedProperties)	Signing-time (SignedData)	Se indica en el campo "M" del diccionario Signature.
Certificado del firmante	Obligatorio	SigningCertificate (SignedProperties)	ESS signing-certificate ESS signing-certificate-v2 (SignedData)	ESS signing-certificate ESS signing-certificate-v2
Política de firma	Obligatorio	SignaturePolicyIdentifier – SigPolicyId (SignedProperties)	SignaturePolicyIdentifier – SigPolicyId (SignedData)	SignaturePolicyIdentifier
		SignaturePolicyIdentifier – SigPolicyHash (SignedProperties)	SignaturePolicyIdentifier – SigPolicyHash (SignedData)	
Formato del objeto original	Obligatorio	DataObjectFormat (SignedProperties)	Content-hints (SignedData)	No permitido
Lugar geográfico (localización)	Opcional	SignatureProductionPlace (SignedProperties)	Signer-location (SignedData)	Se indica en el campo "Location" del diccionario Signature.
Rol de la persona firmante	Opcional	SignerRole - ClaimedRoles (SignedProperties)	Signer-attributes (SignedData)	Signer-attributes

[3] *Nótese que la tabla no constituye un listado completo de las etiquetas definidas por cada estándar sino una referencia a las etiquetas que reflejarán la información para la creación y validación de la firma.*

Información	Obligatoriedad	Campo – etiqueta – elemento[3]		
		XAdES	CAdES	PAdES
Acción del firmante sobre el documento firmado	Opcional	CommitmentTypeIndication (SignedProperties)	Commitment-type-indication (SignedData)	Commitment-type-indication
Sello de tiempo	Opcional	AllDataObjectsTimeStamp (SignedProperties) IndividualDataObjectsTimeStamp (SignedProperties)	Content-time-stamp (SignedData)	Content-time-stamp
Contador de firmas electrónicas	Opcional	CounterSignature (UnsignedProperties)	CounterSignature (UnsignedProperties)	No está permitido

Tabla 4. Etiquetas de creación y validación de firmas electrónicas para los formatos admitidos.

ANEXO II – EQUIPO RESPONSABLE DEL PROYECTO

Coordinador del proyecto

Amutio Gómez, Miguel A.	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Grupo de expertos:

Administración General del Estado

Agurruza Mutuberría, Jokin	INSTITUTO NACIONAL DE ESTADÍSTICA
Alburquerque Pernías, Francisco	MINISTERIO DEL INTERIOR - D. G. DE POLICIA y GUARDIA CIVIL
Álvarez-Cienfuegos Rico, Carmen	MINISTERIO DE INDUSTRIA TURISMO Y COMERCIO
Álvarez Rodríguez, Miguel	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Amores Molero, Felipe	MINISTERIO DE ECONOMÍA Y HACIENDA
Aragonés Arribas, Félix Jesús	MINISTERIO DE ECONOMÍA Y HACIENDA
Arancón Carnicero, Concha	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Arranz Pumar, Candelas	AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA
Arribas Tiestos, Manuel	MINISTERIO DE DEFENSA
Arriero Salcedo, Gabriel	MINISTERIO DE DEFENSA
Barrón Basterrechea, José Luis	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Beriso Gómez-Escalonilla, Pilar	MINISTERIO DE TRABAJO E INMIGRACIÓN
Berral López, Alfonso	MINISTERIO DEL INTERIOR - D. G. DE TRÁFICO
Cabezas Manso, Laura	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Cancio Meliá, Jorge	MINISTERIO DE INDUSTRIA TURISMO Y COMERCIO
Cañero Villegas, Ismael	MINISTERIO DEL INTERIOR
Carrascal Bravo, Guillermo	MINISTERIO DE JUSTICIA
Casado Robledo, Mª Jesús	MINISTERIO DE ECONOMÍA Y HACIENDA
Cornejo Zahonero, Carlos	MEH –TRIBUNAL ECONÓMICO ADMINISTRATIVO CENTRAL
Corral Guinea, Myriam	MINISTERIO DE ECONOMÍA Y HACIENDA
Crespo Sánchez, Juan	MINISTERIO DEL INTERIOR - D. G. POLICÍA Y GUARDÍA CIVIL
Cubo Contreras, Aitor	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Cueva Calabia, José Luis	MINISTERIO DE ECONOMÍA Y HACIENDA
Desantes Fernández, Blanca	MINISTERIO DE CULTURA
Díaz Fraile, Eduardo	MINISTERIO DE MEDIO AMBIENTE Y MEDIO RURAL Y MARINO
Escapa Castro, Lucía	MINISTERIO DE PRESIDENCIA
Escudero Rivas, Carlos	GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL
Esteban de la Torre, Alfredo	MINISTERIO DE EDUCACIÓN
Eusamio Mazagatos, José Antonio	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Fabeiro Sanz, Jorge	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Fernández, Luis	CENTRO CRIPTOLÓGICO NACIONAL
Fradua Garcia-Soto, Idoia	MINISTERIO DE CULTURA
Franco Espino, Beatriz	MINISTERIO DE CULTURA
Galindo Alonso, Olga	GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL
Garcés Pérez, Juan Carlos	CONSEJO GENERAL DEL PODER JUDICIAL
García Celada, Joseba	MINISTERIO DE TRABAJO E INMIGRACIÓN
García García, Emilio	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
García Jiménez, Alfonso	MINISTERIO DE PRESIDENCIA
García Martín, José Aurelio	MINISTERIO DE ECONOMÍA Y HACIENDA
García Martín, Mª Jesús	MINISTERIO DE INDUSTRIA TURISMO Y COMERCIO

Gendive Rivas, Miguel	MINISTERIO DE TRABAJO E INMIGRACIÓN
Gijón Romero, Francisco	MINISTERIO DE FOMENTO
Gómez Raya, José Ignacio	MINISTERIO DE ECONOMÍA Y HACIENDA
González Corral, Isabel	MINISTERIO DE CULTURA
González Rufo, Mª Ángeles	MINISTERIO DE ECONOMÍA Y HACIENDA
González Breña, Julio	AGENCIA ESTATAL DE METEOROLOGÍA
Hernández Carrión, José Luis	MINISTERIO DE JUSTICIA
Hernández Gallardo, Diego	MINISTERIO DE ECONOMÍA Y HACIENDA
Hernández Jiménez, Francisco	INSTITUTO NACIONAL DE ESTADISTICA
Hernández López, Juan Pablo	MINISTERIO DE DEFENSA
Hernández Maroto, Mª Dolores	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Hernández Vicente, Severiano	MINISTERIO DE CULTURA
Iglesias Quintana, Manuel	MINISTERIO DE TRABAJO E INMIGRACIÓN
Igualada Gómez, Rafael	SERVICIO PÚBLICO DE EMPLEO ESTATAL
Jaqueti Fuster, Francisco Javier	INSTITUTO NACIONAL DE ESTADÍSTICA
Lapuente Perea, José Luis	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
López Crespo, Francisco	MINISTERIO DE ASUNTOS EXTERIORES Y COOPERACIÓN
López Montilla, Borja	MINISTERIO DE JUSTICIA
Lucas Vegas, Mª José	MINISTERIO DE TRABAJO E INMIGRACIÓN
Manuel de Villena Cabeza, Luis	MINISTERIO DE MEDIO AMBIENTE Y MEDIO RURAL Y MARINO
Mañes Guerras, Santos	MINISTERIO DE TRABAJO E INMIGRACIÓN
Marcos Martín, Carlos	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Martin Gordo, Félix Alberto	MINISTERIO DE JUSTICIA
Martín Lázaro, Francisco José	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Martín Marcos, Miguel	MINISTERIO DE DEFENSA
Martínez Muñoz, David	MINISTERIO DE ASUNTOS EXTERIORES Y COOPERACIÓN
Martínez Vidal, Miguel Ángel	MINISTERIO DE ECONOMÍA Y HACIENDA
Merchán Arribas, Montaña	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Moliner Aznar, Félix	MINISTERIO DE DEFENSA
Montes Antona, Javier	MINISTERIO DE ECONOMÍA Y HACIENDA
Muñoz Montalvo, Juan Fernando	MINISTERIO DE SANIDAD Y CONSUMO
Muñoz Salinero, Elena	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Nieto Barrantes, Prado	MINISTERIO DE INDUSTRIA TURISMO Y COMERCIO
Ortiz Tovar, Eva María	MINISTERIO DE JUSTICIA
Otheo de Tejada, Josefina	AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA
De Pablo Martín, Fernando	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
De la Paz Rincón, Antonio	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Pérez Galindo, Rafael	MINISTERIO DE INDUSTRIA TURISMO Y COMERCIO
Pérez-Olea Meyer-Doner, Claudio	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Pérez Fernández, Francisco	GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL
Pérez Vázquez, Manuel Carlos	MINISTERIO DE DEFENSA
Quesada Peñas, Juan Luis	MINISTERIO DE INDUSTRIA TURISMO Y COMERCIO
Quintero Villarroya, José Luis	MINISTERIO DE DEFENSA
Ramos, Juan Francisco	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Requejo Zalama, Javier	MINISTERIO DE CULTURA
Robledo Pascual , Óscar	MINISTERIO DE ECONOMÍA Y HACIENDA
Rodríguez Hervás, Francisco Javier	MINISTERIO DEL INTERIOR
Rodríguez Escolar, Nimia	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Rodríguez Ramos, Miguel Ángel	MINISTERIO DE INDUSTRIA TURISMO Y COMERCIO
Romera Iruela, Luis Enrique	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Rubio Martínez, Javier	MINISTERIO DE ECONOMÍA Y HACIENDA
Ruiz del Corral, Manuel	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Ruiz Madueño, Eloy	AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA
Sánchez Abad, Mª Pilar	MINISTERIO DE ECONOMÍA Y HACIENDA
Sánchez Dorronsoro, Gabriel	MINISTERIO DE ECONOMÍA Y HACIENDA
Sánchez Valle, Juan Norberto	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Santiago Freijanes, Marta	MINISTERIO DE CULTURA
Sanz Pulido, Antonio	MINISTERIO DE TRABAJO E INMIGRACIÓN
Serrano Merinero, Ana María	AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA
Simó Ruescas, Leopoldo	MINISTERIO DE DE TRABAJO E INMIGRACIÓN
Triguero Garrido, Mario	GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL
Turón Turón, Ángeles	MINISTERIO DE JUSTICIA
Valcárcel Lucas, Pedro-Castor	GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL
Valdivieso Sánchez, José Luis	AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA
Vallejo Echevarría, Maite	MINISTERIO DE JUSTICIA
Vega Fidalgo, Luis Miguel	GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL
Vélez Fraga, Santiago	MINISTERIO DE ECONOMÍA Y HACIENDA
Vinagre Bachiller, José María	MINISTERIO DE SANIDAD, POLÍTICA SOCIAL E IGUALDAD
Viñado Villuendas, Pilar	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Zapico Alonso, Alberto	AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA

Comunidades Autónomas

Sáez de Vicuña Ortueta, Asier	GOBIERNO VASCO (EJIE SOCIEDAD INFORMÁTICA DEL GOBIERNO VASCO)
Espejo Martínez, Enric	GENERALITAT DE CATALUÑA (CONSORCI ADMINISTRACIÓ OBERTA ELECTRÒNICA DE CATALUNYA)
García Sexto, María José	XUNTA DE GALICIA
Forján Gómez, Carlos	XUNTA DE GALICIA
Fernández Lineros, Francisco José	JUNTA DE ANDALUCÍA
Salmerón Portero, José	JUNTA DE ANDALUCÍA
Leal Zubiete, Juan	JUNTA DE ANDALUCÍA
Domínguez Murillo, Francisco Javier	JUNTA DE ANDALUCÍA
Ojeda, Juan Sebastián	JUNTA DE ANDALUCÍA
García de Bringas Javier	JUNTA DE ANDALUCÍA
Perera Domínguez, Manuel	JUNTA DE ANDALUCÍA
Rodríguez Rodríguez, Juan Carlos	GOBIERNO DEL PRINCIPADO DE ASTURIAS
González Alonso, Borja	GOBIERNO DE CANTABRIA
Gutiérrez Lecue, Miguel Ángel	GOBIERNO DE CANTABRIA
Olivares Sánchez, Pedro	GOBIERNO DE LA REGIÓN DE MURCIA
González, Elena	GOBIERNO DE LA REGIÓN DE MURCIA
Gil Palmero, Fernando	GENERALITAT VALENCIANA
Quereda Ródenas, Rosa	GENERALITAT VALENCIANA
Gil Herrero, Francisco Javier	GENERALITAT VALENCIANA
Borque Almajano, Julio	GOBIERNO DE ARAGÓN
Puyoles Hernandez, Santiago	GOBIERNO DE ARAGÓN
Cantabrana González, Ricardo	GOBIERNO DE ARAGÓN
Lozano Cantín, María Ángeles	GOBIERNO DE ARAGÓN
Pascual Nobajas, Ana	JUNTA DE COMUNIDADES DE CASTILLA-LA MANCHA
Navasa Martínez, Mª de los Ángeles	GOBIERNO DE CANARIAS

Eugenio Baute, Francisco	GOBIERNO DE CANARIAS
García Alberto, Juan Carlos	GOBIERNO DE CANARIAS
del Rosario Verdú, Rafael Carlos	GOBIERNO DE CANARIAS
Ferrer Quintana, José Damián	GOBIERNO DE CANARIAS
Millán Muñoz, María Jesús	GOBIERNO DE CANARIAS
Alfaro Duarte, Fernando	GOBIERNO DE NAVARRA
Arlegui Ochoa, Luis	GOBIERNO DE NAVARRA
Gragera Rodríguez, Jaime	JUNTA DE EXTREMADURA
Arroyo Pérez, Rafael	JUNTA DE EXTREMADURA
Esteban, José Luis	GOBIERNO DE LA COMUNIDAD DE MADRID
Marín, Pepa	GOBIERNO DE LA COMUNIDAD DE MADRID
López-Manzanares Beltrán, Nicolás	GOBIERNO DE LA COMUNIDAD DE MADRID (AGENCIA DE INFORMÁTICA Y COMUNICACIONES DE LA COMUNIDAD DE MADRID)
Sánchez Melero, Arturo	GOBIERNO DE LA COMUNIDAD DE MADRID (AGENCIA DE INFORMÁTICA Y COMUNICACIONES DE LA COMUNIDAD DE MADRID)
Ordás Alonso, Jorge	JUNTA DE CASTILLA Y LEÓN

Corporaciones Locales

Gonzalo Muñoz, Javier	FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS
Serrano Quintana, Juan Manuel	FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

Universidades

Ariño, Luis Alfons	CONFERENCIA DE RECTORES DE LAS UNIVERSIDADES ESPAÑOLAS, UNIVERSITAT ROVIRA I VIRGILI
Guijarro Coloma, Luis	UNIVERSIDAD POLITÉCNICA DE VALENCIA

Otras Instituciones

de Ocaña Lacal, Daniel	TRIBUNAL CONSTITUCIONAL

Con la participación especial de

Álvarez Rodríguez, Miguel	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
Cabezas Manso, Laura	MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Consultor externo

Instituto Nacional de Tecnologías de la Comunicación S.A. (INTECO)