III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

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

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

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

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

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

Posteriormente, la evolución de las tecnologías de aplicación, la experiencia derivada de la aplicación de la citada Norma Técnica de Interoperabilidad, la entrada en vigor de la citada Ley 40/2015, de 1 de octubre, y la evolución del contexto regulatorio europeo, particularmente por razón del Reglamento n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, y su normativa de desarrollo, hacen necesario una actualización de esta Norma Técnica de Interoperabilidad.

La Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y de certificados de la Administración, que sustituye a la anterior denominada de Política de Firma Electrónica y de certificados de la Administración, establece el conjunto de criterios para el desarrollo o adopción de políticas de firma y sello electrónicos basada en certificados por parte de las Administraciones públicas. Para ello, define el contenido de

cve: BOE-A-2016-10146
Verificable en http://www.boe.es

una política de firma electrónica y sello electrónico basados en certificados, especificando las características de las reglas comunes, como formatos, uso de algoritmos, creación y validación de firma para documentos electrónicos, así como de las reglas de confianza en certificados electrónicos, sellos de tiempo y firmas longevas.

Las condiciones establecidas en esta norma persiguen establecer un marco para la definición de políticas de firma y sello electrónicos basada en certificados alineada con actos europeos recientes como la Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, compatible a su vez con sistemas de firma electrónica ya implantados.

La presente actualización de la norma técnica se ha elaborado con la participación de todas las Administraciones Públicas a las que les es de aplicación, ha sido informada favorablemente por el Comité de Dirección de Tecnologías de la Información y Comunicaciones y por el Comité Sectorial de Administración Electrónica.

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

Primero.

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

Segundo.

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

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

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

ÍNDICE

cve: BOE-A-2016-10146
Verificable en http://www.boe.es

I *Consideraciones generales*

I.1 Objeto.

1. La Norma Técnica de Interoperabilidad (en adelante, NTI) de Política de firma y sello electrónicos y de certificados de la Administración tiene por objeto establecer el conjunto de criterios comunes asumidos por la Administración pública en relación con la autenticación y el reconocimiento mutuo de firmas electrónicas y sellos electrónicos basados en certificados electrónicos cualificados o reconocidos y que, como tales, serán desarrollados y consolidados a través de las políticas de firma y sello electrónicos basados en certificados.

2. El objetivo final de esta NTI es facilitar el uso de firmas electrónicas y sellos electrónicos seguros e interoperables entre las distintas organizaciones de la Administración pública.

I.2 Ámbito de aplicación.

1. El contenido de esta NTI será de aplicación para el desarrollo o adopción de políticas de firma y sello electrónicos basada en certificados por parte de cualquier órgano de la Administración pública o Entidad de Derecho Público vinculada o dependiente de aquélla (en adelante, organizaciones) según el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

2. Las políticas de firma y sello harán referencia a un contexto concreto de carácter horizontal donde sea necesario normalizar aspectos de las firmas electrónicas de los Documentos Electrónicos Administrativos para garantizar la interoperabilidad, no a una Administración u organismo particular. Para establecer los aspectos técnicos de las firmas dentro de una Administración u organismos concreto, se optará por la generación de instrucciones técnicas internas, procedimientos o directrices de aplicaciones, que en todo caso deberán ajustarse a lo establecido por el Esquema Nacional de Seguridad.

II *La política de firma y sello electrónicos*

II.1 Definición y contenido.

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

cve: BOE-A-2016-10146
Verificable en http://www.boe.es

2. Una política de firma y sello electrónicos y de certificados definirá:

a) Los procesos de creación, validación y conservación de firmas electrónicas y sellos electrónicos.
b) Características y requisitos de los sistemas de firma electrónica, sellos electrónicos, certificados y sellos de tiempo.

3. Toda política de firma y sello electrónicos basada en certificados incluirá:

a) Definición del alcance y ámbito de aplicación, que concretará su relación con otras políticas existentes, marco o particulares, así como la identificación de los actores involucrados y los usos de la firma electrónica y sello electrónico.
b) Datos para la identificación del documento y del responsable de su gestión.
c) Reglas comunes para el firmante, el creador del sello, y el verificador de la firma o sello electrónicos que incluirán:

i. Formatos admitidos de firma electrónica y sello electrónico, y reglas de uso de algoritmos.
ii. Reglas de creación de firma o sello electrónicos.
iii. Reglas de validación de firma o sello electrónicos.

d) Reglas de confianza, que incluirán los requisitos establecidos para certificados, sellos de tiempo y firmas longevas.
e) Otras reglas opcionales a fijar por cada organización, como podrán ser:

i. Reglas específicas de compromisos que cada organización podrá establecer para cada uno de los servicios que presta, estableciendo requisitos específicos necesarios para que la firma sea válida en cada caso.
ii. Reglas de certificados de atributos mediante las que cada organización podrá establecer información adicional a añadir a los certificados digitales en función de sus necesidades y del contexto.

f) Definición de condiciones para el archivado y custodia de firmas electrónicas.
g) Descripción de consideraciones de gestión de la política que se aplicarán a dicho documento.

II.2 Datos identificativos de la política.

1. El documento de política de firma y sello incluirá la siguiente información para su identificación:

a) Nombre del documento.
b) Versión.
c) Identificador (OID Object IDentifier) de la política.
d) URI (Uniform Resource Identifier) de referencia de la política.
e) Fecha de expedición.
f) Ámbito de aplicación.

2. La política de firma y sello incluirá la definición de su periodo de validez y las consideraciones respecto a los periodos de transición que procedan.
3. Para la identificación de su gestor, la política de firma y sello electrónicos basada en certificados incluirá:

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

cve: BOE-A-2016-10146
Verificable en http://www.boe.es

II.3 Actores involucrados en la firma electrónica.

Los actores involucrados en el proceso de creación y validación de una firma electrónica serán:

a) Firmante: Una persona física que crea una firma electrónica utilizando datos de creación de firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.
b) Creador de un sello: Una persona jurídica que crea un sello electrónico.
c) Verificador: Entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por la política de firma y sello concreta por la que se rige la plataforma de relación electrónica o el servicio concreto al que se esté invocando. Podrá ser una entidad de validación de confianza o una tercera parte que esté interesada en la validez de una firma electrónica.
d) Prestador de servicios de confianza (PSC): Una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza.
e) Emisor y gestor de la política de firma: Entidad que se encarga de generar y gestionar el documento de política de firma y sello, por el cual se deben regir el firmante, el verificador y los prestadores de servicios en los procesos de generación y validación de firma electrónica.

En este documento que utilizará el término 'firmante', tanto para referirse al firmante como al creador de un sello. Puede tratarse de un proceso de actuación administrativa automatizada.
Se usará el término 'firma' tanto para referirse a la firma electrónica como a sello electrónico.

II.4 Usos de la firma electrónica.

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

a) 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.
b) 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.

II.5 Interacción con otras políticas.

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

a. Cada organización valorará la necesidad y conveniencia de desarrollar una política propia frente a la posibilidad de utilizar una política marco existente.
b. Las Administraciones Públicas podrán aprobar otras políticas de firma y sello electrónicos dentro de sus ámbitos competenciales si las características particulares de los procedimientos administrativos bajo su competencia lo hacen necesario. Las políticas de firma y sello particulares estarán orientadas a un contexto concreto, de carácter horizontal, no a una organización concreta. En el caso de que en una organización se deseen normalizar únicamente aspectos técnicos de las firmas electrónicas, se optará por otro instrumento distinto de una Política de firma y sello, como instrucciones técnicas internas o directrices de aplicaciones.

cve: BOE-A-2016-10146
Verificable en http://www.boe.es

c. Serán aprobadas con informe favorable del Comité Sectorial de Administración Electrónica y del Comité Ejecutivo de la Comisión de Estrategia TIC, una vez verificada su interoperabilidad con la Política Marco de Firma Electrónica basada en Certificados.

d. Con objeto de permitir la interoperabilidad de las firmas electrónicas acordes a políticas, las políticas que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Dirección de Tecnologías de la Información y las Comunicaciones del Ministerio de Hacienda y Administraciones Públicas.

2. La definición del alcance y ámbito de aplicación de una política de firma y sello electrónicos se realizará considerando su interacción con otras políticas de firma y sello electrónicos, y asegurando que:

a) Su desarrollo es interoperable con la política marco, en caso de políticas de firma y sello particulares.

b) Define las condiciones de utilización y convivencia con otras políticas particulares, si se trata de una política marco.

3. En toda política de firma y sello electrónicos se asegurará que:

a) Las extensiones o restricciones establecidas para las reglas de creación o validación de firma atienden a la validación de los formatos de firma establecidos en esta NTI y política marco si procede, de forma que se garantice la interoperabilidad entre las diferentes organizaciones.

b) Incluye, si procede, la referencia a la URL de la política marco de firma electrónica en la que se inscribe, con indicación expresa de la versión.

c) Las firmas que se generen siguiendo políticas marco o particulares, incluyen un campo donde se indique de forma explícita la política a la que pertenecen.

d) Para que otras aplicaciones puedan interpretar las reglas de una política particular correctamente, dicha política está disponible en formato XML (eXtensible Markup Language) y ASN.1 (Abstract Syntax Notation One).

II.6 Gestión de la política de firma y sello.

1. La política de firma y sello electrónicos incluirá la descripción básica de su proceso de gestión, estableciendo las directrices para su mantenimiento, actualización y publicación, e identificando al responsable de llevar a cabo estas tareas.

2. El gestor de la política de firma mantendrá actualizada la versión de la política de firma y sello atendiendo a:

a) Modificaciones motivadas por necesidades propias de la organización.

b) Cambios en políticas relacionadas.

c) Cambios en los certificados electrónicos emitidos por los prestadores de servicios de certificación referenciados en la política de firma y sello.

3. Para facilitar la validación de firmas electrónicas creadas atendiendo a versiones anteriores de una política, se podrá mantener un repositorio con el historial de versiones anteriores que provea la ubicación de cada versión.

II.7 Archivado y custodia.

1. Atendiendo a las necesidades y normativa específicas de su ámbito, las políticas de firma y sello podrán contemplar la definición de condiciones y responsabilidades para el archivado y custodia de las firmas electrónicas en sus diferentes aplicaciones.

2. Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, se podrán utilizar:

a) Firmas longevas mediante las que se añadirá información del estado del certificado asociado, incorporando un sello de tiempo, así como los certificados que conforman la

cve: BOE-A-2016-10146
Verificable en http://www.boe.es

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

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

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

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

a) En caso de almacenar los certificados y las informaciones de estado dentro de la firma, se sellarán también dichas informaciones, siguiendo las modalidades de firmas recogidas en la «Decisión de Ejecución UE 2015/1506 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público», o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior».

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

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

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

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

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

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

6. La definición de medidas y procedimientos para archivado y custodia de firmas/sellos electrónicos se realizará atendiendo con proporcionalidad a los diferentes usos de la firma electrónica contemplados en el alcance y ámbito de aplicación de la política.

cve: BOE-A-2016-10146
Verificable en http://www.boe.es

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

III *Reglas comunes*

III.1 Reglas comunes.

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

III.2 Formatos admitidos de firma electrónica.

1. Los formatos admitidos por las organizaciones para las firmas/sellos electrónicos basadas en certificados electrónicos, se ajustarán a:

a) la «Decisión de Ejecución UE 2015/1506» o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior».
b) lo establecido en la NTI de Catálogo de estándares.
c) los formatos CAdES, XAdES y PAdES en las versiones establecidas en la Norma Técnica de Interoperabilidad de Política de firma del 2011.

2. Los formatos de firma/sello electrónico serán

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

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.

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

1. Los formatos para la firma/sello electrónica de contenido se ajustarán a la «Decisión de Ejecución UE 2015/1506» o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) 910/2014»
2. Por compatibilidad con las políticas de firma anteriores, se permitirán aunque no se recomiendan los siguientes formatos::

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

3. 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 y sello. En cualquier caso, cada

cve: BOE-A-2016-10146
Verificable en http://www.boe.es

organización podrá definir en su política de firma y sello las consideraciones adicionales que considere respecto a la interpretación y utilización de diferentes perfiles y clases de los formatos siempre en consonancia con lo establecido en esta NTI.

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

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

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

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

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

III.5 Reglas de uso de algoritmos.

1. La política de firma y sello especificará las reglas de uso de algoritmos en los diferentes formatos así como la longitud de las claves asociadas a aquéllos de forma proporcional a las necesidades detectadas en los diferentes usos de la firma/sello electrónicos, cumpliendo en cualquier caso lo establecido en la NTI de Catálogo de estándares y lo previsto en las normas que se definan en aplicación del Reglamento (UE) 910/2014.

2. Para los entornos de seguridad regulados por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/ 2015, de 1 de octubre, de Régimen Jurídico del Sector Público, de aplicación en los procedimientos de administración electrónica, se ajustarán a la «Decisión de Ejecución UE 2015/1506» o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) 910/2014» o las especificaciones técnicas publicadas por los organismos de Estandarización Europeos. La definición de usos de algoritmos podrá contemplar diferentes posibilidades según lo establecido en las guías aplicables, como la norma CCN-STIC 807 del Esquema Nacional de Seguridad relativa al uso de criptografía, las normas ETSI TS 119 312 'Criptographic Suites for secure electronic signatures', o aquellas que las sustituyan.

3. Para los entornos de alta seguridad, de acuerdo con el criterio del Centro Criptológico Nacional (CCN) serán de aplicación las recomendaciones revisadas de la CCN-STIC 405 así como en la norma CCN-STIC 807 del Esquema Nacional de Seguridad relativa al uso de criptografía.

III.6 Reglas de creación de firma electrónica.

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

cve: BOE-A-2016-10146
Verificable en http://www.boe.es

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

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

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

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

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

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

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

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

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

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

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

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

b) Certificado del firmante.

c) Cadena de validación.

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

e) Formato del objeto original.

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

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

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

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

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

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

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

cve: BOE-A-2016-10146
Verificable en http://www.boe.es

III.7 Reglas de validación de firma/sello electrónicos.

1. Las políticas de firma y sello definirán las condiciones particulares bajo las que, en su ámbito, será posible validar la firma electrónica de un documentosiguiendo los requisitos establecidos en el artículo 32.1 del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

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

3. Las condiciones mínimas que se producirán para la validación de la firma/sello serán las siguientes:

a) Garantía de que la firma es válida para el fichero específico que está firmado.

b) Validez de los certificados:

i. El instante de tiempo que se tomará como referencia para la validación será:

1) El momento en que se produjo la firma/sello si se da alguno de los siguientes supuestos:

a. los servicios de los prestadores facilitan los históricos de estado de los certificados y la firma/sello lleva un sello de tiempo válido en el momento de la verificación.

b. se trata de firmas/sellos longevos que incluyen las evidencias de la validez de la firma electrónica en el momento de la generación o primera validación, y dichas evidencias se encuentran selladas con un sello de tiempo válido.

2) En otros casos, el momento de la validación.

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

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

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

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

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

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

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

c) Política de firma y sello sobre la que se basa el proceso de generación de firma electrónica. Se utilizará para identificar, mediante su hash y su identificador (OID), que la

cve: BOE-A-2016-10146
Verificable en http://www.boe.es

política de firma y sello que se ha utilizado para la generación de la firma se corresponde con la que se utilizará para el servicio en cuestión.

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

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

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

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

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

IV *Reglas de confianza*

IV.1 Reglas de confianza para los certificados electrónicos.

1. Las políticas de firma y sello, marco o particulares, podrán fijar limitaciones y restricciones específicas para los certificados electrónicos que admiten en cada uno de los servicios que corresponda, si el uso destinado del certificado establecido en su Política de Certificación no está acorde al ámbito de la Política de firma y sello, siempre en consideración de la normativa aplicable en cada caso.

2. Se presumirán válidos los certificados cualificados que usen los ciudadanos en las firmas y sellos electrónicos. Si una administración apreciara algún aspecto que cuestionara esta validez lo hará saber al ciudadano que dispondrá del plazo previsto en la normativa de procedimiento administrativo para subsanar lo que corresponda o ratificar por otra vía los documentos firmados electrónicamente. El firmante no podrá alegar que ha utilizado una firma inválida con arreglo a una determinada Declaración de Prácticas de Certificación como condición en la que se base un recurso de nulidad o anulabilidad de un acto.

3. Los certificados válidos para ejecutar la firma/sello electrónicos de contenido serán los certificados electrónicos cualificados de firma y sello según el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

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

cve: BOE-A-2016-10146
Verificable en http://www.boe.es

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

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

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

IV.2 Reglas de confianza para sellos de tiempo.

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

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

a) ETSI EN 319 422 V1.1.1Time-stamping protocol and time-stamp token profiles.

b) ETSI EN 319 421 V1.1.1 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

O en las que las sustituyan.

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

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

IV.3 Reglas de confianza para firmas longevas.

1. En el caso de firmas longevas, el firmante o el verificador de la firma incluirá un sello de tiempo que permita garantizar que el certificado era válido en el momento en que se realizó la firma. En el caso de que sea incluida por el firmante, se podrá realizar una vez haya trascurrido el periodo de precaución o periodo de gracia.

2. Para la conversión de una firma electrónica a firma electrónica longeva:

a) Se verificará la firma electrónica, validando la integridad de la firma acorde a las reglas de validación de firma de electrónica del epígrafe III.7.

b) Se realizará un proceso de completado de la firma electrónica que consistirá en la obtención y almacenamiento de las referencias a:

i. Certificados: Incluyendo los certificados del firmante y de la cadena de certificación tanto del firmante como del sello de tiempo.

ii. Informaciones de estado de los certificados, CRLs o las respuestas OCSP.

c) Aplicación del sellado de tiempo a las referencias a los certificados y a las informaciones de estado.

cve: BOE-A-2016-10146
Verificable en http://www.boe.es

3. Para la incorporación a la firma de la información completa de validación, se usará validación mediante CRLs u OCSP.

4. Las políticas de firma y sello contemplarán la definición de formatos y consideraciones de uso de firmas longevas conforme a las necesidades específicas de su ámbito de aplicación y a la normativa específica aplicable.

cve: BOE-A-2016-10146
Verificable en http://www.boe.es