Política de firma electrónica de NeoCheck

Control de Versiones

Versión	Autor	Revisión	Aprobado	Fecha	Descripción
1	Resp. SGSI	Resp. SGSI	Dirección	07/05/2024	Ficha Inicial

Contenido

Política de firma electrónica i
Contenido 1
1 INTRODUCCIÓN 3
1.1 Consideraciones Generales 4
1.2 Objeto de la política de firma electrónica 5
1.3 Referencias. 6
2 ALCANCE DE LA POLÍTICA DE FIRMA 8
2.1 Alcance la política de firma 8
2.2 Actores involucrados en la firma electrónica 8
2.3 Formatos admitidos de firma 8
2.4 Creación de la firma electrónica 9
2.5 Verificación de la firma electrónica 9
3 LA POLITICA DE FIRMA ELECTRÓNICA 11
3.1 Identificación de la política. 11
3.2 Periodos de validez y transición. 11
3.3 Identificación del gestor del documento de la política. 11
3.4 Reglas comunes 11
3.4.1 Reglas del firmante 12
3.4.1.1 Formato XAdES 12
3.4.1.2 Formato PAdES 12
3.4.2 Reglas del verificador 13
3.4.3 Reglas para los sellos de tiempo 13
3.4.4 Reglas de confianza para firmas longevas 14
3.4.4.1 Formato XAdES 15
3.4.4.2 Formato PAdES 15
3.4.5 Reglas para certificados admitidos por el “AYUNTAMIENTO / DIPUTACIÓN”. 16
3.4.6 Reglas para certificados empleados por el “AYUNTAMIENTO / DIPUTACIÓN” 16
3.4.7 Reglas para el mantenimiento y preservación de firmas electrónicas del “AYUNTAMIENTO / DIPUTACIÓN” 17
3.4.7.1 Resellado de firmas electrónicas 17
3.4.7.2 Mantenimiento de la validez jurídica de las firmas en fase de vigencia. 18
3.5 Reglas de confianza de certificados de atributos 19
3.6 Reglas de uso de algoritmos 19

3.7 Reglas específicas de compromisos 19
4 GESTIÓN DE LA POLÍTICA DE FIRMA 20
5 ARCHIVADO Y CUSTODIA 21

1 INTRODUCCIÓN

En esta Política de Firma Electrónica se desarrollan los siguientes elementos:

1. El objeto con el que se desarrolla la Política de firma electrónica.
2. Los datos identificativos de la política, sus periodos de validez y su transición a nuevas políticas y la asignación de responsabilidades para su gestión.
3. La definición de los conceptos clave en materia de firma electrónica y que son desarrollados a lo largo de la Política.
4. La normativa y estándares internacionales a la que está sujeta la Política de firma electrónica de **La organización** y en base a la cual se desarrolla.
5. El uso de certificados digitales:
    a. Certificados digitales admitidos: qué certificados digitales pueden utilizar otras personas o entidades para relacionarse telemáticamente
    b. Certificados digitales empleados: qué certificados digitales pueden utilizar los empleados de **La organización** en el ejercicio de sus funciones, y los sellos electrónicos están previstos para la actuación automatizada.
6. El ciclo de vida de los certificados empleados por **La organización"**, identificándose cómo pueden obtenerse estos cuando se necesiten y cómo se llevará el control de los certificados existentes y de su eventual revocación cuando dejen de ser necesarios.
7. La definición del sello de tiempo como elemento que permite dejar evidencia de la fecha y hora en que se ha producido un acto.
8. Las clases, tipos y niveles de firma, es decir, el cómo y en qué formato se generan las firmas electrónicas empleadas en el ámbito de La **organización** y el proceso seguido para su validación.
9. El mantenimiento y la preservación de firmas electrónicas para garantizar la introducción en los sistemas de gestión documental de **La organización** de documentos auténticos que garanticen la preservación de su validez jurídica a largo plazo mediante procesos de resellado de tiempo.
10. La identificación de los metadatos previstos en el Vocabulario de Metadatos de La organización para la gestión efectiva de firmas electrónicas.
11. La identificación de un subconjunto representativo de casos de uso de la firma electrónica que identifican posibles escenarios en los que los procedimientos de **La organización** pueden requerir el uso de firmas electrónicas vinculado a una normativa de firma electrónica concreta:
    a. Foliado de expedientes electrónicos.
    b. Firma electrónica de un documento electrónico.
    c. Digitalización certificada de documentos en papel.
    d. Copia auténtica electrónica de un documento firmado
    e. Procesos de firma automatizada.
    1. Tratamiento de documentos firmados electrónicamente y aportados por terceras partes

Para la elaboración de esta Política de Firma Electrónica se ha tenido en cuenta lo que el Esquema Nacional de Interoperabilidad establece al respecto y, muy concretamente, lo que se define en la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados digitales de la Administración, así como la del expediente electrónico en lo referente a la firma electrónica de los mismos.

1.1 Consideraciones Generales

La Ley 59/2003, de 19 de diciembre, de firma electrónica, define la firma electrónica distinguiendo los siguientes conceptos:

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

El nuevo **REGLAMENTO (UE) N o 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO** de 23 de julio de 2014 distingue los nuevos conceptos:

- **Firma electrónica:** los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar
- **Firma electrónica avanzada:** la firma electrónica que cumple los requisitos:
    - estar vinculada al firmante de manera única
    - permitir la identificación del firmante
    - haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y
    - estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.
- **Firma electrónica cualificada:** una firma electrónica avanzada que se crea mediante un dispositivo cualificado de
    - creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.
    - Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita.
    - Una firma electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será reconocida como una firma electrónica cualificada en todos los demás Estados miembros.

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

- **Identificación:** que posibilita garantizar la identidad del firmante de manera única.

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

Cuando se firman datos, 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 específica una política explícita o implícita.
Si el campo correspondiente a la normativa de firma electrónica está ausente y no se identifica ninguna normativa como aplicable, entonces se puede asumir que la firma ha sido generada o verificada sin ninguna restricción normativa, y en consecuencia, que no se le ha asignado ningún significado concreto legal o contractual. Se trataría de una firma que no especifica de forma expresa ninguna semántica o significación concreta y, por lo tanto, hará falta derivar el significado de la firma a partir del contexto (y especialmente, de la semántica del documento firmado).
La finalidad de una política de firma es reforzar la confianza en las transacciones electrónicas a través de una serie de condiciones para un contexto dado, el cual puede ser una transacción determinada, un requisito jurídico o un rol que asuma la parte firmante, entre otros.

1.2 Objeto de la política de firma electrónica

La política de firma electrónica tiene por objeto establecer el conjunto de criterios comunes asumidos por **La organización** en relación con la autenticación y la firma electrónica. En concreto establece las directrices a seguir por **La organización** al uso de la firma electrónica, en el seno de las aplicaciones informáticas corporativas, para garantizar la autenticidad, integridad y conservación de los documentos electrónicos firmados digitalmente.

Las condiciones establecidas tienen por objetivo:

- Establecer un marco de operaciones con las firmas electrónicas que fomente la interoperabilidad entre los actores involucrados.
- Dibujar un marco operativo similar al propuesto en la política marco de firma electrónica definida por la Administración General del Estado. Esta proximidad facilita la adopción de la operativa necesaria para la emisión y verificación de firmas electrónicas al basarse en un conjunto de condiciones comunes y conocidas.
- Definir con claridad las condiciones que ha de cumplir un firmante para que la generación de una firma tenga garantías.
- Dar garantías a un verificador de la validez de una firma electrónica realizada acorde con estas condiciones.

Este documento se ajusta a la estructura determinada en La Norma Técnica de Interoperabilidad de Política de firma electrónica y de certificados de la Administración, aprobada en la resolución de 19 de Julio de 2011 y publicada en el Boletín Oficial del Estado número 182 de sábado de 30 de Julio de 2011.

1.3 Referencias.

Para el desarrollo de su contenido, se ha tenido en cuenta las siguientes especificaciones técnicas:

- ETSI TS 101 903, v.1.2.2, v.1.3.2 y 1.4.1. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).
- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
- ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- ETSI TS 101 861 V1.3.1 Time stamping profile
- ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.
- ETSI TR 102 041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.
- ETSI TR 102 045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.
- ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.
- IETF RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
- IETF RFC 3125, Electronic Signature Policies.
- IETF RFC 3161 actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 5652, RFC 4853 y RFC 3852, Cryptographic Message Syntax (CMS).
- ITU-T Recommendation X.680 (1997): "Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation".

Para la normativa base se han seguido las siguientes referencias:

- Reglamento (UE) Nº 910/2014 Del Parlamento Europeo y del Consejo de 23 De Julio De 2014.
- 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).
- Ley 59/2003, de 19 de Diciembre, de firma electrónica.
- Ley 56/2007 o Ley para el Impulso de la Sociedad de la Información.
- Ley Orgánica 15/1999, de 13 de Diciembre, de protección de los datos de carácter personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de Diciembre, de protección de datos de carácter personal.
- Real Decreto 1553/2005, de 23 de Diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Ley 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

- 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.
- 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.
- 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.
- Descripción de los perfiles de certificados de la Ley 11/2007, que estarán asociados a esta política de firma: Perfiles de certificados en su última versión disponible.

2 ALCANCE DE LA POLÍTICA DE FIRMA

2.1 Alcance la política de firma

Este documento propone una política de firma electrónica, que detalla las condiciones generales para la validación de la firma electrónica y una relación de formatos de objetos binarios y ficheros de referencia que deberán ser admitidos por todas las plataformas implicadas en las relaciones electrónicas de **La organización** con los ciudadanos y con las Administraciones Públicas.

2.2 Actores involucrados en la firma electrónica

Los actores identificados en los documentos firmados según esta política son:

- **Firmante:** entidad que gestiona el dispositivo de creación de firma y que firma en nombre propio o en nombre de la persona física o jurídica que representa.
  El nivel de compromiso del firmante se derivará a partir del contexto.
- **Verificador:** entidad que comprueba la validez de la firma aplicando las condiciones especificadas en esta política.
- **Prestador de certificados:** entidad que expide los certificados electrónicos y dispositivos de creación de firma requeridos por el firmante y que permite comprobar la identidad del firmante y la integridad de los datos firmados.
- **Gestor de la política de firma:** entidad encargada de la gestión, mantenimiento y actualización, de la política de firma.

2.3 Formatos admitidos de firma

El formato de los documentos electrónicos con firma electrónica avanzada, aplicada mediante los certificados electrónicos admitidos por las Administraciones Públicas y utilizados en el ámbito de las relaciones con o dentro de la Administración Pública, se deberá ajustar a las especificaciones de los estándares europeos relativos a los formatos de firma electrónica.

El Consejo Superior de la Administración Electrónica será la Entidad gestora encargada de publicar y actualizar la relación de las especificaciones relativas a los formatos admitidos por la presente política de firma.
Actualmente se consideran formatos admitidos:

- **formato XAdES (XML Advanced Electronic Signatures),** según especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2. Asimismo, se admitirá la última versión 1.4.1 a partir del 31-12-2013. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma1.

- **formato PAdES (PDF Advanced Electronic Signatures)**, según especificación técnica ETSI TS 102 778-3, versión 1.2.1 (se admitirán versiones posteriores siempre que no impliquen cambios significativos en la sintaxis de los tags usados en la presente política) y la ETSI TS 102 778-4 para el caso de firmas longevas en PADES (PAdES Long Term). En caso contrario se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

2.4 Creación de la firma electrónica

Para la creación de firmas electrónicas que se adecuen a esta política, los sistemas encargados de generar las firmas deberán cumplir:

- El usuario deberá poder comprobar la información que va a firmar. Es decir, antes de la realización de la firma el usuario deberá poder comprobar que está de acuerdo con el contenido que va a firmar en las condiciones o contexto en el que se realizará la firma (no repudio, compromiso, etc.).
- Antes de realizar la firma el sistema comprobará:
    - Que el certificado utilizado ha sido emitido por uno de los prestadores de certificación admitidos en esta política de firma (basado en una comprobación de la cadena de confianza).
    - Que el estado de validez del certificado es válido. Esta comprobación se deberá realizar sobre el periodo de validez del certificado y sobre el estado del certificado y toda su cadena de certificación (es decir, comprobar que no está revocado ni suspendido tanto el certificado firmante como todos los certificados de la cadena de confianza implicados).

En caso de que no se pueda realizar alguno de los pasos anteriores o su resultado sea erróneo no se deberá permitir continuar con el proceso de generación de la firma.
El resultado final del proceso de creación de firma será un fichero con una firma electrónica siguiendo uno de los formatos indicados en el punto anterior en su forma básica.

El servicio creará un fichero en formato XAdES o PAdES para aquellos escenarios en los que sea conveniente.

Se recomienda que el fichero resultante tenga una extensión única de forma que los visores de documentos firmados puedan asociarse a esa extensión, haciendo más fácil al usuario el manejo de este tipo de ficheros. Esta extensión podría ser:

o ".xsig", si la firma implementada se ha realizado según el estándar XAdES

En el caso de las firmas PAdES, al estar la firma incluida en un documento PDF, la extensión será aquella del formato PDF original.

2.5 Verificación de la firma electrónica

Para la comprobación de la validez de una firma electrónica generada según específica esta política, los sistemas encargados deberán asegurarse de:

- Comprobar que se cumple la integridad de la información firmada.
- Comprobar la validez de los certificados implicados. Esta comprobación se deberá realizar sobre el momento de validación si la firma no contiene una fecha de confianza, o sobre el histórico del estado de los certificados si hay una fecha de confianza disponible. Esta información estará contenida en la propia firma para las formas longevas.
- Comprobar que el certificado de firma ha sido emitido por uno de los prestadores de certificación admitidos en la política de firma que sea aplicable según la fecha en la que se generó la firma (si no hay fecha de confianza será sobre la política más actual disponible).

3 LA POLITICA DE FIRMA ELECTRÓNICA

3.1 Identificación de la política.

Los datos identificativos de la Política de Firma Electrónica son los que se incluyen a continuación:

2. Nombre del documento: Política de Firma Electrónica de **La organización**
3. Versión: 1.0
4. Fecha de aprobación: **xx** de **xxxxxx** de **xxxx**
5. Identificador (OID – Object IDentiifer) de la política

3.2 Periodos de validez y transición.

La presente Política de Firma Electrónica de **La organización** entrará en vigor en la fecha de su probación y será válida hasta que no sea sustituida o derogada por otra política posterior.

Si se estima oportuno, una nueva versión de la Política de gestión documental podrá facilitar un período de tiempo transitorio para adecuar los diferentes sistemas de firma electrónica y validación utilizados por **La organización** las especificaciones de la nueva versión.

Este período de tiempo de transición se deberá indicar en la nueva versión y superado el mismo sólo será válida la versión actualizada.

3.3 Identificación del gestor del documento de la política.

A continuación se incluyen los datos identificativos del gestor de la Política de Firma Electrónica de **La organización**

1. Responsable de la política: Héctor Insausti Beruete
2. Dirección de contacto: Ronda Circunvalación 188, Castellón de la Plana
3. e-mail de contacto: hector.insausti@neocheck.com
4. Teléfono de contacto: 616646848

3.4 Reglas comunes

Las reglas comunes para los actores involucrados en la firma electrónica, firmante y verificador, son un campo obligatorio que debe aparecer en cualquier política de firma. 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, debiendo estar firmados, si son requisitos para el firmante, o no firmados, si son requisitos para el verificador.

3.4.1 Reglas del firmante

El firmante se hará responsable de que el fichero que se quiere firmar no contiene contenido dinámico que pudiese modificar el resultado de la firma durante el tiempo. Si el fichero que se quiere firmar no ha sido creado por el firmante, deberá asegurarse que no existe contenido dinámico dentro del fichero, como pueden ser macros.

3.4.1.1 Formato XAdES

La versión del estándar de firma para firmas XAdES deberá ser 1.3.2. El firmante deberá proporcionar la siguiente metainformación según está recogido en el estándar:

- SigningTime: indicará la fecha y hora a la que se realiza la firma. Debido a que no se incluye información sobre la fuente de origen de la hora, esta información se utiliza a título indicativo pero no vinculante.
- SigningCertificate: identificará mediante una referencia al certificado firmante. Su uso se justifica para evitar una sustitución del certificado.
- SignaturePolicyIdentifier: el uso de este campo se considerará opcional. Si no se indica o se indica una política implícita se asumirá que esta política de firma electrónica será la que se aplica de manera implícita en la firma. Si se incluye una política explícita deberá contener una referencia explícita que identifique de manera inequívoca la política de firma electrónica que se quiere aplicar.

Además se deberá incluir la huella digital del documento que describe la política. En el caso de referenciar a esta política será la huella digital de este documento.

Para las firmas electrónicas realizadas sobre otras firmas electrónicas se utilizará lo indicado en el estándar XAdES al respecto de CounterSignatures. Si las firmas se realizan en serie (cada nueva firma electrónica firma a la anterior) se utilizará el campo CounterSignature de la sección UnsignedProperties de la firma que está siendo firmada.

3.4.1.2 Formato PAdES

Se utilizará la Normativa ETSI 102 778 PADES para realizar las firmas en el formato PDF.
Siempre que sea posible se intentará adecuar la firma a los requerimientos AdES para que la firma electrónica realizada se asemeje a la producida en el estándar PAdES.
El firmante deberá incluir los campos:

- SigningTime: indicará la fecha y hora a la que se realiza la firma. Debido a que no se incluye información sobre la fuente de origen de la hora, esta información se utiliza a título indicativo pero no vinculante.
- SigningCertificate: identificará mediante una referencia al certificado firmante. Su uso se justifica para evitar una sustitución del certificado.
- SignaturePolicyIdentifier: el uso de este campo se considerará opcional. Si no se indica o se indica una política implícita se asumirá que esta política de firma electrónica será la que se aplica de manera implícita en la firma. Si se incluye una política explícita deberá contener una referencia explícita que identifique de manera inequívoca la política de firma electrónica que se quiere aplicar.

Además se deberá incluir la huella digital del documento que describe la política. En el caso de referenciar a esta política será la huella digital de este documento.

3.4.2 Reglas del verificador

El formato básico de firma electrónica avanzada no contempla ninguna información de validación más allá del certificado firmante, que se incluye en la etiqueta Signing Certificate, y de la política de firma que se indique en la etiqueta Signature Policy.
Los atributos que podrá utilizar el verificador para comprobar que se cumplen los requisitos de la política de firma según la cual se ha generado la firma, independientemente del formato utilizado (XAdES o PAdES), son las siguientes:

- **Signing Time**: sólo se utilizará en la verificación de las firmas electrónicas como indicación para comprobar el estado de los certificados en la fecha señalada, ya que únicamente se puede asegurar las referencias temporales mediante un sello de tiempo (especialmente en el caso de firmas en dispositivos cliente). 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.
- **Signing Certificate:** se utilizará para comprobar y verificar el estado del certificado (y,en su caso, la cadena de certificación) en la fecha de la generación de la firma, en el caso que el certificado no estuviese caducado y se pueda acceder a los datos de verificación (CRL, OCSP, etc) o bien en el caso de que el PSC ofrezca un servicio de validación histórico del estado del certificado.
- **Signature Policy:** se deberá comprobar, que la política de firma que se ha utilizado para la generación de la firma se corresponde con la que se debe utilizar para un servicio en cuestión.

Si se han realizado varias firmas del mismo documento, se seguirá el mismo proceso de verificación que con la primera firma, comprobando la etiqueta Counter Signature en el campo de propiedades no firmadas, donde se informa de los refrendos de firma generados.

Será responsabilidad del encargado de la verificación de la firma definir sus procesos de validación y de archivado según los requisitos de la política de firma particular a la que se ajusta el servicio.

Existe un tiempo de espera, conocido como periodo de precaución o periodo de gracia, para comprobar el estado de revocación de un certificado. El verificador puede esperar este tiempo para validar la firma o realizarla en el mismo momento y revalidarla después. Esto se debe a que puede existir una pequeña demora desde que el firmante inicia la revocación de
un certificado hasta que la información del estado de revocación del certificado se distribuye a los puntos de información correspondientes. Se recomienda 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 o el tiempo máximo de actualización del estado del certificado en el servicio OCSP. Estos tiempos podrán ser variables según el Prestador de Servicios de Certificación.

3.4.3 Reglas para los sellos de tiempo

El sello de tiempo asegura que los datos, la firma del documento que va a ser sellado o la información del estado de los certificados incluidos en la firma electrónica, se generaron antes de

una determinada fecha. El formato del sello de tiempo deberá cumplir las recomendaciones de IETF, RFC 5816, “Internet X.509 Public Key Infrastructure; Time-Stamp Protocol (TSP)”.
Los elementos básicos que componen un sello digital de tiempo son:
1. Datos sobre la identidad de la autoridad emisora (identidad jurídica, clave pública autilizar en la verificación del sello, número de bits de la clave, el algoritmo de firma digital y la función hash utilizados).
2. Tipo de solicitud cursada (si es un valor hash o un documento, cuál es su valor y datos de referencia).
3. Parámetros del secuenciador (valores hash "anterior", "actual" y "siguiente").
4. Fecha y hora UTC.
5. Firma digital de todo lo anterior con la clave pública y esquema de firma digital especificados.

El sellado de tiempo puede ser añadido por el emisor, el receptor o un tercero y se debe incluir como propiedad no firmada en el campo Signature Time Stamp.

El sellado de tiempo debe realizarse en un momento próximo a la fecha incluida en el campo Signing Time y, en cualquier caso, siempre antes de la caducidad del certificado del firmante.

La presente política admite sellos de tiempo expedidos por prestadores de servicios de sellado de tiempo que cumplan las especificaciones técnicas ETSI TS 102 023, “Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities”.

3.4.4 Reglas de confianza para firmas longevas

Los estándares XAdES (ETSI TS 101 903) y PAdES (ETSI TS 102 778-4) contemplan la posibilidad de incorporar a las firmas electrónicas informaciónadicional para garantizar la validez de una firma a largo plazo, una vez vencido el periodo de validez del certificado. Esta información puede ser incluida tanto por el firmante como por el verificador, y se recomienda hacerlo después de trascurrido el periodo de precaución o periodo de gracia. Existen dos tipos de datos a incluir como información adicional de validación:

- la información del estado del certificado en el momento en que se produce la validación de la firma o una referencia a los mismos.
- certificados que conforman la cadena de confianza.

En el caso de que se deseen generar firmas longevas, se recomienda incluir la información de validación anterior, y añadirle un sello de tiempo. En estos tipos de firma la validez de la firma resultante viene determinada por la duración del sello de tiempo que se añade a la firma longeva.

En el caso que se desee incorporar a la firma la información de validación, se recomienda usar validación mediante OCSP, ya que mediante este método las propiedades o atributos a incluir son de menor tamaño.

Si la consulta al estado de validación de la firma se realiza mediante un método que resulta en una información muy voluminosa que aumenta de forma desproporcionada el tamaño de la firma,

opcionalmente, en lugar de la información de validación indicada anteriormente, se pueden incluir en la firma longeva referencias a dicha información.

3.4.4.1 Formato XAdES

Dentro del formato de firma XAdES, el formato extendido XAdES-C incorpora estas entre otras propiedades no firmadas:

- **CompleteCertificateRefs** que contiene referencias a todos los certificados de la cadena de confianza necesaria para verificar la firma, excepto el certificado firmante.
- **CompleteRevocationRefs** que contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación de los certificados.

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.

El formato XAdES-XL además de la información incluida en XAdES-X, incluye dos nuevas propiedades no firmadas
- CertificateValues,
- RevocationValues

Estas propiedades incluyen, no solo las referencias a la información de validación sino también la cadena de confianza completa y la CRL o respuesta OCSP obtenida en la validación. Para los atributos CertificateValues y Revocation-Values se recomienda hacer la validación por OCSP ya que estos valores pueden ser muy voluminosos en caso de realizar la validación mediante CRL.

3.4.4.2 Formato PAdES

Con el fin de permitir el upgrade de firmas a LTV es necesario incluir la siguiente extensión en el diccionario Catalog:
<</ESIC
<</BaseVersion /1.7
/ExtensionLevel 1
>>
>>
La validación de firmas LTV implicaría la verificación de esta extensión y la existencia de los atributos requeridos (sellos de tiempo, respuestas OCSP o CRLs y certificados).

Se recomienda usar validación mediante OCSP, ya que el tamaño de la información de validación a añadir será menor.
Se recomienda añadir un sello de tiempo que incluya 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.

3.4.5 Reglas para certificados admitidos por el "AYUNTAMIENTO / DIPUTACIÓN".

El mecanismo de firma electrónica se sustenta en la existencia de Autoridades de Certificación que emiten certificados digitales y permiten comprobar que un certificado concreto ha estado correctamente emitido y que continúa siendo válido en el momento de su uso, es decir, de la firma de un documento o de la identificación fehaciente de una persona, entidad o proceso en un entorno digital.

La relación entre la Autoridad de Certificación y la entidad que valida el certificado es una relación que se fundamenta en la confianza: los certificados serán aceptados sólo en la medida en que la entidad que lo ha de validar confíe en la honestidad de la Autoridad de Certificación.

En este contexto, **La organización** debe, según la Ley 15/2015, admitir todos los certificados digitales emitidos por los prestadores de servicios de certificación que hayan realizado la comunicación prevista en el artículo 30.2 de la Ley 59/2003 en el Ministerio de Industria, Energía y Turismo y que cumplan con los estándares de calidad y niveles de seguridad establecidos por dicho Ministerio.

No obstante, en este ámbito de **La organización** está utilizando la plataforma **ValidatedID"** para la validación de los certificados, por lo que la aceptación efectiva de certificados vendrá condicionada por la actualización de los servicios de dicha plataforma.
Debido a ello, aunque la Ley 15/2015 exime de esta responsabilidad, en la Sede Electrónica de **La organización** se publicará la lista de certificados admitidos que se irá actualizando hasta que puedan ser admitidos todos los certificados digitales reconocidos por el Ministerio de Industria, Energía y Turismo, momento en que se procederá a su despublicación. Para su facilidad de gestión y mantenimiento actualizado, este listado se vinculará con el listado publicado por el Centro de Transferencia de Tecnología en el documento "Anexo – Proveedores de servicios de Certificación" accesible a través del Portal de Administración electrónica en el siguiente enlace:
https://administracionelectronica.gob.es/PAe/aFirma-Anexo-PSC

3.4.6 Reglas para certificados empleados por el "AYUNTAMIENTO / DIPUTACIÓN"

Los empleados de **La organización** que deban firmar documentos digitalmente o tener acceso a determinados servicios o aplicaciones donde se requiera un alto nivel de autenticación, necesitarán certificados digitales. Para este propósito **La organización** utilizará certificados de empleado.
En lo referente a los sellos electrónicos, de órgano y de Sede electrónica, **La organización** utilizará la plataforma ValidatedID.
Todos estos certificados digitales son solicitados de forma centralizada desde **La organización**. Para mayor detalle nos referimos al siguiente apartado de esta Política referente al ciclo de vida de los certificados digitales empleados por **La organización**.
En lo que respecta al uso de certificados digitales de servidor, los utilizados para el intercambio seguro de información entre Administraciones públicas se utilizará también los de la **xxxxx**, o en su defecto, cualquiera de los emitidos por otras autoridades de certificación que ya tengan un alto nivel de instalación, de sus claves públicas, en los navegadores.

Cabe señalar que si bien estos certificados no generan actos jurídicos, se ha considerado oportuno incorporarlos a esta política.
Finalmente, los certificados utilizados por **La organización** han sido comunicados al Ministerio de Industria, Energía y Turismo, por parte de la **"ValidatedID** o Autoridad de Certificación correspondiente, de acuerdo a lo que prevé el artículo 30.2 de la Ley 59/2003, de Firma Electrónica.

3.4.7 Reglas para el mantenimiento y preservación de firmas electrónicas de **La organización**

3.4.7.1 Resellado de firmas electrónicas

El objetivo principal de esta función es garantizar la firma electrónica a lo largo del tiempo mediante un proceso consistente en renovar el sello de fecha y hora, añadiendo un nuevo eslabón a la cadena de evidencias electrónicas de la firma electrónica que ya está en el documento.
Para poder aplicar dicho proceso es necesario que las firmas estén en un formato que permita añadir sellos de tiempo sucesivos. Estas son las firmas del tipo AdES-A, XAdES-A en el caso de documentos en formato XML o PAdES-LTV en el caso de documentos en formato PDF. En el caso de que una firma no esté en estos formatos, previo al resellado se completará la firma, que en cualquier caso estará como mínimo en un formato XAdES-T o PAdES-T, a uno de los formatos que se acaban de indicar.
Este será un proceso que se realizará:

- En el momento en que esté a punto de caducar el último sello de tiempo aplicado a la firma electrónica a preservar.
- Excepcionalmente, cuando se detecte una posible obsolescencia tecnológica de los algoritmos o de las claves utilizadas para la generación de una firma electrónica.

El proceso de resellado de tiempo de firmas electrónicas partirá, tal y como se acaba de establecer, de documentos firmados de forma longeva con firmas de tipo AdES-A o PAdES-LTV ya que su estructura permite esta posibilidad. Sobre estas firmas se incorporará un nuevo sello de tiempo generado con un certificado digital específico de sellado de tiempo de reciente emisión y, por tanto, que disponga de un período de validez superior al de la firma a resellar, así como de una longitud de clave y algoritmo criptográfico que no estarán comprometidos según es describe en el siguiente subapartado.
En definitiva, el resellado consiste, pues, en mantener la validez de la firma incorporando nueva información criptográfica, concretamente sellos de fecha y hora, en la misma estructura de la firma electrónica.
La organización reconoce a través de esta política la existencia de la posibilidad de aplicar medidas de seguridad suficientes que eviten cualquier modificación malintencionada de documentos sin emplear técnicas de resellado de tiempo, asegurando así su integridad y no repudio. Sin embargo, el **La organización** opta por el método descrito en este subapartado ya que facilita la disponibilidad de evidencias suficientes de la preservación, reguladas por la Ley 59/2003, de firma electrónica, que de otra manera habría que justificar con un complejo sistema de evidencias electrónicas.

3.4.7.2 Mantenimiento de la validez jurídica de las firmas en fase de vigencia.

La firma electrónica otorga validez jurídica a los documentos electrónicos. No obstante, esta validez está sujeta a los siguientes riesgos que deben gestionarse debidamente con tal de mantener la validez jurídica de un documento electrónico durante las fases de tramitación y vigencia y, en su caso, de archivo. Estos
riesgos son:

1) **Caducidad del certificado digital con el que se firma un documento electrónico.** Puede cuestionarse la validez de un documento electrónico a partir del día que caduque el certificado digital que lo firmó, si no se puede acreditar con total garantía la fecha en que se generó dicha firma, la cual debe ser evidentemente posterior a la fecha de emisión del certificado digital y anterior a la fecha de revocación o caducidad del certificado digital. Para garantizar el momento en que se generó la firma electrónica, ésta debe ser completada con un sello de tiempo emitido por una Autoridad de Certificación, siempre antes de la caducidad o revocación del certificado digital que la emitió.

   En aquellas situaciones en que este riesgo pueda materializarse, **La organización** realizará firmas como mínimo de formato AdES-T, tanto a nivel de PDFs como de XML.

2) **Validez del certificado digital en el momento de generarse la firma electrónica.** Puede cuestionarse la validez de un documento electrónico si no existe la evidencia suficiente de que el certificado digital estaba vigente el día que se generó la firma electrónica, es decir, no estaba revocado. Para guardar la evidencia de que un certificado digital en una fecha determinada, la de la firma, no estaba revocado es necesario completar la firma con la información de la validación de este aspecto contra la Autoridad de Certificación emisora del certificado en el mismo momento de emisión de la firma.

   En este sentido hay que tener en cuenta que las Autoridades de Certificación, en el momento en que un certificado digital caduca, eliminan las evidencias de revocación de su lista de certificados revocados por lo que si no se guarda la evidencia mencionada, una vez caducado el certificado con el que se emitió la firma electrónica, no existirá la certeza de que el certificado no estaba revocado en el momento de generarla.

   En aquellas situaciones en que este riesgo pueda materializarse, **La organización**, realizará firmas de formato AdES-XL, tanto a nivel de PDFs como de XML, o superiores, pudiendo ser XAdES-A, en el caso de XML o PAdES-LTV en el caso de PDF.

3) **Obsolescencia tecnológica de la longitud de las claves criptográficas contenidas en el certificado digital y con las que se generan las firmas electrónicas.** Un documento electrónico puede dejar de tener validez jurídica a partir del día en que se ponga en duda la seguridad de las claves criptográficas con las que se firmó. En este escenario podrían reproducirse de forma incontrolada firmas generadas con las claves puestas en duda y, por lo tanto, todas las firmas generadas con la tecnología obsoleta se pondrían en duda. Para resolver este aspecto se requiere de claves criptográficas de mayor longitud y generar sucesivos refirmas a partir de firmas electrónicas que permitan incorporar estos sellos de tiempo.

En aquellas situaciones en que este riesgo pueda materializarse, igual que en el caso anterior, **La organización** realizará firmas de formato AdES-XL, tanto a nivel de PDFs como de XML, o superiores, pudiendo ser XAdES-A, en el caso de XML o PAdES-LTV en el caso de PDF.

3.5 Reglas de confianza de certificados de atributos

Esta política de firma no fija ninguna regla específica respecto a los certificados de atributos.

Las políticas de firma particulares de suborganismo o entidad dentro cada organismo o entidad dentro de **La organización** basadas en la presente política marco, podrán fijar reglas específicas para cada uno de los servicios que prestan, siendo necesario cumplir sus requisitos para que la firma sea válida en ese contexto.

3.6 Reglas de uso de algoritmos

Para los entornos se tomará la referencia a la URN en la que se publican las funciones de hash y los algoritmos de firma utilizados por las especificaciones XAdES y PAdES, como formatos de firma adoptados, de acuerdo con las especificaciones técnicas ETSI TS 102 176-1 sobre "Electronic Signatures and Infraestructures (ESI); Algorithms and parameters for secure electronic signature". Todo ello sin perjuicio de los criterios que, al respecto, se hayan adoptado en el Esquema Nacional de Seguridad, desarrollado a partir del artículo 42 de la Ley 11/2007, por el Real Decreto 3/2010, de 6 de noviembre.

La presente política admite como válidos los algoritmos de generación de hash, codificación en base64, firma, normalización y transformación definidos en los estándares XMLDSig y CMS.

Se podrán utilizar cualquiera de los siguientes algoritmos para la firma electrónica: RSA/SHA1 (formato que se recomienda reemplazar en el medio plazo por algoritmos más robustos), RSA/SHA256 y RSA/SHA512 que es recomendado para archivado de documentos electrónicos (very long term signatures).

3.7 Reglas específicas de compromisos

Esta política de firma no fija ninguna regla respecto a compromisos específicos.

Las políticas de firma particulares de cada organismo o entidad dentro de **La organización**, basadas en la presente política marco, podrán fijar reglas específicas para cada uno de los servicios que prestan, siendo necesario cumplir sus requisitos para que la firma sea válida en ese contexto.

4 GESTIÓN DE LA POLÍTICA DE FIRMA

El mantenimiento, actualización y publicación de la política de firma será realizado por **La organización**
En caso de que se emita un nuevo documento se identificará este con un número superior de versión. Si los cambios se consideran de carácter menor se incrementará el número menor de versión. Si los cambios son de carácter mayor se incrementará el número mayor de versión y se pondrá a cero el número menor. Será **La organización"**, la responsable de categorizar el carácter de los cambios en el nuevo documento.
Los documentos de política de firma en todas sus versiones estarán disponibles para los validadores a través de la web de **La organización**. De esta forma, una vez que el validador identifique la versión de la política de firma que aplica a la firma que verifica, podrá aplicar las normas específicas válidas para esa firma.

Cada documento de política indica el periodo de validez en el que aplica. Para identificar qué versión de política aplica deberá buscarse la versión de la política superior cuyo plazo de validez aplique a la fecha de generación de la firma que se verifica. Si la versión de política se encuentra explicitada en la firma deberá comprobarse que tal versión es congruente con lo indicado anteriormente.

5 ARCHIVADO Y CUSTODIA

Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, esta deberá ser complementada con la información del estado del certificado asociado en el momento en que la misma se produjo y/o información no repudiable incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.

Esto implica que, si queremos tener una firma que pueda ser validada a lo largo del tiempo, la firma electrónica que se genera ha de incluir evidencias de su validez para que no pueda ser repudiada. Para este tipo de firmas deberá existir un servicio que mantenga dichas evidencias, y será necesario solicitar la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

Las condiciones que se deberán dar para considerar una firma electrónica longeva son las siguientes:

1) En primer lugar, deberá verificarse la firma electrónica producida o verificada, validando la integridad de la firma, el cumplimiento de los estándares XAdES o PAdES, y las referencias.
2) Deberá realizarse un proceso de completado de la firma electrónica, consistente en lo siguiente:
   a) Obtener las referencias a los certificados, así como almacenar los certificados del firmante.
   b) Obtener las referencias a las informaciones de estado de los certificados, como las listas de revocación de certificados (CRLs) o las respuestas OCSP, así como almacenarlas.
3) Al menos, deben sellarse las referencias a los certificados y a las informaciones de estado.

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

- en caso de almacenar los certificados y las informaciones de estado dentro de la firma, se recomienda sellar también estas informaciones, siguiendo las modalidades de firmas AdES –X o -A.

Para proteger la firma electrónica frente a la posible obsolescencia de los algoritmos y poder seguir asegurando sus características a lo largo del tiempo de validez, se deberá seguir uno de los siguientes procesos, de acuerdo con las especificaciones técnicas para firmas electrónicas de tipo XAdES o PAdES:

- las plataformas de firma electrónica adoptadas en el ámbito de **La organización** deberán disponer de mecanismos de resellado, para añadir, de forma periódica, un sello de fecha y hora de archivo con un algoritmo más resistente.
- la firma electrónica deberá almacenarse 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 criptográfico).

Es necesario que con posterioridad las firmas puedan renovarse (refirmado o countersignature) y permitan actualizar los elementos de confianza (sellos de tiempo), garantizando la fiabilidad de la firma electrónica.

Para el archivado y gestión de documentos electrónicos se seguirán las recomendaciones de las guías técnicas de desarrollo del Esquema Nacional de Interoperabilidad (Real Decreto 4/2010, de 8 de enero).