# NSG-1/14 - POLÍTICA DE FIRMA ELECTRONICA

**Departamento de Seguridad**

13/06/2018

# ÍNDICE

# 1 INTRODUCCIÓN

Esta política tiene el fin de desarrollar el derecho de la ciudadanía a relacionarse con la organización por medios electrónicos, para acceder a los servicios públicos y de este modo tramitar los diferentes procedimientos electrónicos puestos a su disposición.

Este documento determina la creación y validación de la firma electrónica, según los estándares técnicos europeos eIDAS, describiendo el alcance y uso de la firma electrónica con la intención de cumplir las condiciones legales vigentes.

# 2 ALCANCE DE LA POLÍTICA DE FIRMA

Se propone una política de firma electrónica, que detalla las condiciones generales para la generación, validación y conservación de la firma electrónica y una relación de formatos de objetos binarios y ficheros de referencia que deberán ser admitidos por los servicios electrónicos en las relaciones electrónicas de la organización con la ciudadanía y otras entidades

Para su identificación unívoca, la presente política de firma se identificará con un identificador único en forma de URI, que deberá incluirse obligatoriamente en la firma electrónica, empleando el campo correspondiente para identificar la política de firma y la versión con las condiciones generales y específicas de aplicación para su validación, determinando las condiciones que debe cumplir la firma electrónica en un momento determinado.

La presente política de firma estará disponible en formato legible, de modo que puedan ser aplicadas en un contexto concreto para cumplir con los requerimientos de creación y validación de firma electrónica.

## 2.1 Actores involucrados en la firma electrónica

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

- Firmante: persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.
- Verificador: entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por una política de firma concreta. Puede ser una entidad de validación de confianza o una tercera parte que esté interesada en la validez de una firma electrónica.
- Prestador de servicios de firma electrónica: la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
- Emisor de la política de firma: entidad que se encarga de generar y gestionar el documento de política de firma, por el cual se deben regir el firmante y el verificador en los procesos de generación y validación de firma electrónica.

## 2.2 Formatos admitidos de firma

El formato de los documentos electrónicos con firma electrónica avanzada y reconocida, aplicada mediante los certificados electrónicos admitidos por la organización y utilizados en el ámbito de las relaciones con o dentro de la misma se deberá ajustar a las especificaciones de los estándares europeos relativos a los formatos de firma electrónica y a la legislación española en el caso de firma electrónica reconocida.

La Dirección de la Organización será la encargada de publicar y actualizar, en la sede electrónica, la relación de las especificaciones relativas a los formatos admitidos por la presente política de firma.

La organización se basará en los estándares y formatos empleados por Izenpe, siguiendo la normativa aplicable a tal efecto.

Se tendrá en cuenta la legislación Europea en relación a los formatos de firma admitidos en la Unión Europea, en especial, aquellos definidos en los estándares europeos de firma electrónica.

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. 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.
- formato CAdES (CMS Advanced Electronic Signatures), según especificación técnica ETSI TS 101 733, versión 1.6.3 y versión 1.7.4. 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 firma.
- 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), dada su especial relevancia como un formato de firma visible directamente por el ciudadano mediante herramientas estándar.

La clase básica de firma electrónica para definir **una política de firma electrónica de interoperabilidad** es, según los estándares AdES, **la clase EPES.** A partir de este formato básico EPES es posible incluir suficiente información para validar la firma a largo plazo.

Si fuera necesario generar firmas con validación a largo plazo, se debería implementar un formato que incorporase propiedades adicionales, como información sobre revocación de certificados.

## 2.3 Creación de la firma electrónica

Izenpe presta el servicio de creación de firma electrónica y proporcionará las funcionalidades necesarias para soportar un proceso de creación de firmas basado en los siguientes puntos:

- Selección por parte del usuario firmante del fichero para ser firmado. Los formatos de fichero que deberán ser admitidos por las plataformas, están publicados en la sede electrónica, en el apartado documentos electrónicos admitidos.
  El firmante se asegurará de que el fichero que se quiere firmar no contiene contenido dinámico que afecte a su validez y que pudiese modificar el resultado de la firma a lo largo del tiempo.

- El servicio de firma electrónica ejecutará una serie de verificaciones previas a la creación de la firma:
  - La firma electrónica puede ser validada para el formato del fichero específico que va a ser firmado, según la presente política.
  - Los certificados a utilizar han sido expedidos bajo una Declaración de Políticas de Certificación admitida. Se publicarán, en la sede electrónica, la relación de certificados electrónicos admitidos.
  - 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.

    Cuando una de estas verificaciones es errónea, el proceso de firma se interrumpirá.

    Si no fuese posible realizar estas comprobaciones, en el momento de la firma, los sistemas correspondientes podrán no aceptar el fichero firmado, o esperar un período de tiempo hasta que se pueda realizar la comprobación.

El servicio creará un fichero en formato XAdES, CADES 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:

- ".xsig", si la firma implementada se ha realizado según el estándar XAdES
- ".csig", si la firma implementada se ha realizado según el estándar CAdES

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

## 2.4 Verificación de la firma electrónica

El verificador puede utilizar cualquier método para verificar la firma creada según la presente política. Las condiciones mínimas que se deberán producir para validar la firma serán las siguientes:

- Garantía de que la firma es válida para el fichero específico que está firmado.
- Validez de los certificados en el momento en que se produjo la firma, si se trata de una clase de firma que incorpora información sobre revocación de certificados, o en caso contrario, validez de los certificados en el momento de la validación: certificados no revocados, suspendidos, o que hayan expirado, y la validación de la cadena de certificación (incluida la validación de todos los

certificados de la cadena). Esta información puede estar contenida en la propia firma en el caso de las firmas longevas.
- Certificado expedido bajo una Declaración de Prácticas de Certificación admitida en el momento en que se produjo la firma. El listado completo de certificados admitidos puede ser consultado en la sección correspondiente de la sede electrónica.
- Verificación, si existen, de los sellos de tiempo de los formatos implementados, incluyendo la verificación de los periodos de validez de los sellos.

### 2.5 Resellado de firmas

No aplica, no se realiza resellado de documentos.

## 3 POLÍTICA DE VALIDACIÓN DE FIRMA

En este apartado se especifican las condiciones que se deberán considerar por parte del firmante, en el proceso de generación de firma electrónica, y por parte del verificador, en el proceso de validación de la firma.

### 3.1 Periodo de validez

La presente Política de Firma Electrónica es válida desde la fecha de expedición del apartado anterior hasta la publicación de una nueva versión actualizada, pudiéndose facilitar un periodo de tiempo transitorio, en el cual convivan las dos versiones, que permita adecuar las diferentes plataformas de las administraciones públicas a las especificaciones de la nueva versión. Este periodo de tiempo transitorio deberá indicarse en la nueva versión, pasado el cual sólo será válida la versión actualizada.

### 3.2 Usos de firma electrónica

La firma electrónica es un mecanismo para securizar la información a través de los canales telemáticos existentes. El objetivo de la política de firma es indicar los usos que se contemplan para un ámbito y alcance concretos, especificando las condiciones requeridas y necesarias para cada uno de los usos que corresponda.

#### 3.2.1 Para transmisiones de datos

A la hora de transmitir los datos para los que sea necesaria la firma electrónica, proporcionando la seguridad en el intercambio y garantizando la autenticación de los actores involucrados en el proceso, así como la integridad del contenido del mensaje de datos enviado y el no repudio de los mensajes entre dos

servidores (punto a punto). La firma está asociada al protocolo de transporte, formando parte de los mecanismos de cifrado a implementar en una comunicación segura.

Por lo tanto, toda comunicación que se realice entre las diferentes partes de la organización y que requiera el uso de la política de firma definida en este documento deberá firmar los mensajes SOAP mediante una cabecera Web Service- Security (WSS) para que sean entendidos por la plataforma tecnológica de la organización.

### 3.2.2 De contenido

Este tipo de firma equivale, en el entorno digital, a la firma manuscrita tradicional, estando asociada directamente al contenido y garantizando la autenticidad de aquél.

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

En caso de intercambio, tanto la firma como el propio contenido irán anexos a la transmisión o intercambio, propiamente dicho. Así, los usos de la firma explicados no son complementarios, sino compatibles, pudiéndose utilizar de forma simultánea.

## 3.3 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.

### 3.3.1 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.

#### *3.3.1.1 Formato XAdES*

Se admitirán las firmas:
- XAdESenveloped
- XAdESdettached

El firmante deberá proporcionar, como mínimo, la información contenida en las siguientes etiquetas dentro del campo SignedProperties (campo que contiene una serie de propiedades conjuntamente firmadas a la hora de la generación de la firma XMLDsig), las cuales son de carácter obligatorio:

- SigningTime: indica la fecha y la hora. En el caso de firma en cliente sin acceder a servidor, será meramente indicativa (pues la fecha en el dispositivo cliente es fácilmente manipulable) y/o será utilizada con fines distintos a conocer la fecha y hora de firma. Las políticas particulares de firma electrónica podrán determinar características y restricciones particulares respecto a generación en cliente de las referencias temporales y sincronización del reloj.
- SigningCertificate: contiene referencias a los certificados y algoritmos de seguridad utilizados para cada certificado. Este elemento deberá ser firmado con objeto de evitar la posibilidad de sustitución del certificado.
- SignaturePolicyIdentifier: identifica la política de firma sobre la que se basa el proceso de generación de firma electrónica, y debe incluir los siguientes contenidos en los elementos en que se subdivide:
    - Una referencia explícita al presente documento de política de firma, o en su caso, al documento de política de firma particular de cada organismo, en el elemento xades:SigPolicyId. Para ello aparecerá el OID que identifique la versión concreta de la política de firma o la URL de su localización.
    - La huella digital del documento de política de firma correspondiente y el algoritmo utilizado, en el elemento <xades:SigPolicyHash>, de manera que el verificador pueda comprobar, calculando a su vez este valor, que la firma está generada según la misma política de firma que se utilizará para su validación.
- DataObjectFormat: define el formato del documento original, y es necesario para que el receptor conozca la forma de visualizar el documento.

La etiqueta CounterSignature, refrendo de la firma electrónica y que se puede incluir en el campo UnsignedProperties, será considerada de carácter opcional. Las siguientes firmas, ya sean serie o paralelo, se añadirán según indica el estándar XAdES, según el documento ETSI TS 101 903 v1.3.2.

#### *3.3.1.2 Formato CADES*

Se admitirán las firmas:

- Attached. Se adopta el tipo Signed Data con los datos incluidos (implícito) para la estructura del documento, especificado en los estándares CMS (IETF RCF 5652) y CAdES (ETSI TS 101 733), que mantiene el documento original y la firma en un mismo fichero.
- Dettached, que incluye el hash del documento original en la firma, en este caso, se almacenan en ficheros diferentes, la firma y el documento que se ha firmado.

Las siguientes etiquetas deberán ser firmadas y son de carácter obligatorio:

- Content-type: esta etiqueta especifica el tipo de contenido que debe serfirmado. Es una etiqueta obligatoria según el estándar CAdES.
- Message-digest: identifica el cifrado del contenido firmado OCTET STRING en encapContentInfo. Es una etiqueta obligatoria según el estándar CAdES.

- ESS signing-certificate o ESS signing-certificate-v2: es una etiqueta que permite el uso de SHA-1 (sólo para ESS signing-certificate) y la familia de algoritmos SHA-2 como algoritmo de seguridad. Es una etiqueta obligatoria según el estándar CAdES.
- Signing-time: indica la fecha y hora de la firma. En el caso de firma en cliente sin acceder a servidor, será meramente indicativa (pues la fecha en el dispositivo cliente es fácilmente manipulable) y/o será utilizada con fines distintos a conocer la fecha y hora de firma. Las políticas particulares de firma electrónica podrán determinar características y restricciones particulares respecto a generación en cliente de las referencias temporales y sincronización del reloj. Es una etiqueta de carácter obligatorio según está política de firma.
- SignaturePolicyIdentifier: es una etiqueta que indica la política de firma sobre la que se basará la generación de la firma electrónica. El documento deberá incorporar la referencia (OID) a la política de firma particular aplicada y la huella digital del documento de política de firma correspondiente y el algoritmo utilizado, en el elemento SigPolicyHash, de manera que el verificador pueda comprobar, calculando a su vez este valor, que la firma está generada según la misma política de firma que se utilizará para su validación.

La etiqueta CounterSignature, refrendo de la firma electrónica, incluido en el campo de propiedades no firmadas, será considerada de carácter opcional. Las siguientes firmas se añadirán según indica el estándar CAdES.

#### *3.3.1.3 Formato PADES*

Se admitirán las firmas:

- PAdES-BES, PAdES-EPES: Define una firma CAdES-BES (ETSI TS 101 733) y otra CAdES-EPES (ETSI TS 101 733) que tienen como restricciones específicas la necesidad de que la clave /ByteRange del diccionario de firma abarque la totalidad del documento, la obligatoriedad de que la clave /SubFilter tenga el valor ETSI.CAdES.detached y la prohibición de utilizar la clave /Cert. Ambos tipos de firma admiten la posibilidad de incluir un sello de tiempo que las convierta, de hecho, en firmas CAdES-T (ETSI TS 101 733). Así pues, las características de las firmas PAdES-BES y PAdES-EPES son las mismas que las de las firmas CAdES-BES, CAdES-EPES y CAdES-T.

La versión de PAdES empleada en esta política, es la versión 1.2.1, admitiéndose implementaciones posteriores, siempre que no impliquen cambios significativos en los tags empleados. En ese caso, será necesario actualizar el presente documento de Política de Firma electrónica.

Los siguientes atributos deberán estar firmados y serán de carácter obligatorio:

- Content-type: especifica el tipo de contenido que debe ser firmado. Es obligatoria según el estándar PAdES.
- Message-digest: identifica el cifrado del contenido firmado OCTET STRING en encapContentInfo. Es obligatoria según el estándar PAdES.
- ESS signing-certificate o ESS signing-certificate-v2 es una etiqueta que permite el uso de SHA-1 (sólo para ESS signing-certificate) y la familia de algoritmos SHA-2 como algoritmo de seguridad. Es una etiqueta obligatoria según el estándar PAdES. Nunca se debe especificar el campo Cert del diccionario Signature.

- signature-policy-identifier: identifica la política de firma sobre la que se basa el proceso de generación de firma electrónica. El documento deberá incorporar el OID de la política de firma particular aplicada.

No está permitido el atributo Content-hints
Nunca se debe especificar el atributo SigningTime. El tiempo de la firma debe indicarse en el campo M en diccionario Signature, un atributo específico del PDF.

### 3.3.2 Reglas del verificador

El formato básico de firma electrónica avanzada no incluye ninguna información de validación más allá del certificado firmante, que está incluida en la etiqueta SigningCertificate, y de la política de firma que se indique en la etiqueta SignaturePolicy.

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, CAdES o PAdES), son las siguientes:

- SigningTime: 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.
- SigningCertificate: 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.).
- SignaturePolicy: 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 CounterSignature en el campo de propiedades no firmadas, donde se informa de los refrendos de firma generados.

El encargado de la verificación de la firma deberá definir sus procesos de validación y de archivado según los requisitos de la política de firma.

Existe un periodo de 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.

### 3.3.3 Reglas para los sellos de tiempo

El sello de tiempo asegura que tanto los datos originales del documento que va a ser sellado como la información del estado de los certificados, en caso de que se hayan incluido 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:

- Datos sobre la identidad de la autoridad emisora (identidad jurídica, clave pública a utilizar en la verificación del sello, número de bits de la clave, el algoritmo de firma digital y la función hash utilizados).
- Tipo de solicitud cursada (si es un valor hash o un documento, cuál es su valor y datos de referencia).
- Parámetros del secuenciador (valores hash "anterior", "actual" y "siguiente").
- Fecha y hora UTC.
- Firma digital de todo lo anterior con la clave pública y esquema de firma digital especificados.

El sellado de tiempo y la información de validación pueden ser añadidos por el emisor, el receptor o un tercero y se deben incluir como propiedades no firmadas en el campo SignatureTimeStamp.

El sellado de tiempo debe realizarse en un momento próximo a la fecha incluida en el campo SigningTime 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”.

### 3.3.4 Reglas de confianza para firmas longevas

Los estándares CAdES (ETSI TS 101 733), XAdES (ETSI TS 101 903) y PAdES (ETSI TS 101 733) contemplan la posibilidad de incorporar a las firmas electrónicas información adicional 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 deberá 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.

#### *3.3.4.1 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 los certificados.

El formato XAdES-X 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

En el caso que se desee incorporar a la firma esta información de validación, se recomienda usar el formato XADES-A, que añade un sello de tiempo a la información anterior

#### *3.3.4.2 Formato CAdES*

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

- complete-certificate-references que contiene referencias a todos los certificados de la cadena de confianza necesaria para verificar la firma
- complete-revocation-references que contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación de la firma.

El formato CAdES-X Long además de la información incluida en CAdES-C, incluye dos nuevos atributos certificate-values y revocation-values que 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 en las firmas longevas se recomienda hacer la validación por OCSP ya que estos valores pueden ser muy voluminosos en caso de realizar la validación mediante CRL.

#### *3.3.4.3 Formato Pades*

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 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 cada organismo o entidad dentro de la CAE, 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.

## 3.5 Reglas de uso de algoritmos

Para los entornos de seguridad genérica se tomará la referencia a la URN (Uniform Resource Name) en la que se publican las funciones de hash y los algoritmos de firma utilizados por la especificación XAdES, CADES 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 signatures: Part 1: Hash functions and asymmetric algorithms”.

La presente política admite como válidos los algoritmos de generación de hash, codificación en base64, firma, normalización y transformación definidos en el estándar 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).

Para la generación de los sellos de tiempo, se hará uso de sistemas de sellado de tiempo que utilicen una Autoridad de Sellado de Tiempo (Time Stamping Authority o TSA). La TSA recibe el documento a sellar, le añade el tiempo actual y lleva a cabo un proceso de firma electrónica mediante un criptosistema asimétrico.

## 3.6 Reglas específicas de compromisos

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

## 3.7 Referencias

- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- 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.
- Reglamento (UE) Nº 910/2014 sobre identificación electrónica y servicios de confianza (eIDAS)

# 4 HISTORIAL DE REVISIONES

| Revisión | Fecha | Modificaciones |
|---|---|---|
| 01 | 12/06/18 | Primera versión |

Bizkaia
lantik

Sabino Arana, 44
48013 BILBAO (Bizkaia)

Tel: (+34) 944 068 900
Fax: (+34) 944 068 800

e-mail: lantik@bizkaia.eus
http://lantik.bizkaia.eus

**ER-2023/2005**
El Diseño, el Desarrollo y el Mantenimiento de Aplicaciones Informáticas.
**ER-0739/2006**
La Compra de Bienes y Servicios y el Suministro e Instalación de Equipamiento Informático para la Diputación Foral de Bizkaia.
**ER-0811/2008**
La Atención al Cliente.