Política de firma y sello electrónicos y de certificados del Ayuntamiento de Bilbao

Aprobada por Acuerdo de Junta de Gobierno con fecha

28 de octubre de 2020

Índice

POLÍTICA DE FIRMA Y SELLO ELECTRÓNICOS Y DE CERTIFICADOS DEL AYUNTAMIENTO DE BILBAO

En este documento, para facilitar su lectura, se utiliza el término 'Política' para referirse a la 'Política de firma y sello electrónicos y de certificados del Ayuntamiento de Bilbao'.

Con el mismo objetivo, en algunas ocasiones, se utiliza el término 'firmante', tanto para referirse a la persona firmante como a la creadora de un sello y se usa el término 'firma', tanto para referirse a la firma electrónica como al sello electrónico.

1 Introducción a la Política

La Ordenanza de Administración electrónica del Ayuntamiento de Bilbao, aprobada en el año 2010, facilita el desarrollo de un modelo propio de administración electrónica en nuestro contexto, es decir, adecuado a la realidad de la sociedad, de la organización municipal y de la disponibilidad y madurez de las tecnologías.

La presente Política desarrolla dicho modelo en lo referente a la firma y sello electrónicos basados en certificados, como complemento de lo dispuesto en la siguiente legislación:

a) 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.
b) 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 (en adelante, Reglamento eIDAS)
c) 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.
d) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
e) Ley 40/2015, de Régimen Jurídico del Sector Público.
f) 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.

2 Objetivo, ámbito de aplicación y alcance

2.1 Objetivo de la Política

El objetivo de la presente Política es facilitar el uso de firmas electrónicas y sellos electrónicos seguros e interoperables entre los distintos actores que intervienen en la Administración pública.

2.2 Ámbito de aplicación de la Política

Esta Política se circunscribe a los sistemas de firma y sello electrónicos basados en certificados previstos en la Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y se aplicará a las entidades de la Administración municipal, así como a las relaciones desarrolladas a través de medios electrónicos entre la Administración municipal y las personas físicas y jurídicas, tanto privadas como públicas.

2.3 Alcance de la Política

La Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones públicas establece una separación entre identificación y firma electrónica, así como la simplificación de los medios para acreditar una u otra, de modo que, con carácter general, sólo será necesaria la primera, y se exigirá la segunda cuando deba acreditarse la voluntad y consentimiento de la persona interesada.

Según dicha Ley, las Administraciones Públicas están obligadas a verificar la identidad de las personas interesadas en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente. Las personas interesadas podrán identificarse electrónicamente ante las Administraciones Públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad. El Ayuntamiento de Bilbao mantendrá actualizada en su sede electrónica la lista de sistemas de identificación válidos.

Siguiendo con la Ley 39/2015, las personas interesadas podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento. En el caso de que las personas interesadas optaran por relacionarse con el Ayuntamiento de Bilbao a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica reconocida o cualificada y avanzada, basados en certificados electrónicos reconocidos o cualificados de firma electrónica, expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación». A estos efectos, se entienden comprendidos entre los citados certificados electrónicos reconocidos o cualificados los de persona jurídica y de entidad sin personalidad jurídica.
b) Sistemas de sello electrónico reconocido o cualificado y de sello electrónico avanzado, basados en certificados electrónicos reconocidos o cualificados de sello electrónico incluidos en la «Lista de confianza de prestadores de servicios de certificación».

Por otra parte, el Reglamento eIDAS instaura un nuevo paradigma: únicamente las personas físicas están capacitadas para firmar electrónicamente. Por tal motivo, Reglamento no prevé la emisión de certificados de **firma** electrónica a favor de personas jurídicas o entidades sin personalidad jurídica. A éstas se reservan los **sellos** electrónicos, que permiten garantizar la autenticidad e integridad de sus documentos, tales como facturas electrónicas, y activos digitales, sin perjuicio de poder actuar por medio de los certificados de firma de persona física con atributo de representante.

El **alcance** de esta Política es detallar las condiciones para la firma y sello electrónicos basados en certificados, puesto que son mecanismos cuya implantación, a través de estándares completamente

desarrollados, permiten un uso interoperable. El resto de sistemas de firma, al no estar basados en un conjunto de estándares tan completo o desarrollado, carecen de mecanismos generalmente reconocidos para su uso bajo el marco de una política. No obstante, la Política no excluye otros sistemas de firma reconocidos en la legislación (CSV, claves concertadas u otros sistemas no criptográficos) para los que se aplicaría lo establecido en la Ley 39/2015, de 1 de octubre, la Ley 40/2015, de 1 de octubre, y resto de normativa vigente aplicable.

2.4 Identificación de personas y entidades involucradas

Las personas y entidades involucradas 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) **Creadora de un sello**: Una persona jurídica que crea un sello electrónico.
c) **Verificadora**: 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) **Prestadora 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) **Emisora y gestora 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 creador de sello, el verificador y los prestadores de servicios en los procesos de generación y validación de firma electrónica.

2.5 Usos de la firma y sello electrónicos

La firma electrónica, como mecanismo para la seguridad de la información, podrá aplicarse en:

a) **Firma de transmisiones de datos**, como herramienta para proporcionar seguridad al intercambio de datos, 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. Equivale, en el entorno electrónico, a la firma manuscrita tradicional.

En caso de transmisión de un contenido firmado, tanto el contenido como su firma irán anexos a la transmisión, la cual, a su vez, podría ir firmada. Así, ambos usos de la firma son compatibles, pudiéndose utilizar de forma simultánea.

La firma electrónica de la Administración municipal se realizará, siempre que sea posible, mediante sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, basado en certificado electrónico reconocido o cualificado. En caso de no ser posible, se realizará mediante firma electrónica de la persona que actúe como titular del órgano o como empleada pública.

Los usos concretos de la firma electrónica serán definidos en la Política de gestión de documentos electrónicos del Ayuntamiento de Bilbao, la cual detalla los procesos de la gestión de documentos en el marco de la Administración municipal.

3 Identificación del documento de política y responsable de su gestión

3.1 Identificación

a) Nombre del documento: Política de firma y sello electrónicos y de certificados del Ayuntamiento de Bilbao

b) Versión: 1.0

c) URI (Uniform Resource Identifier) de referencia de la política:

https://www.bilbao.eus/eudala/normativa/politica_firma.pdf

https://www.bilbao.eus/eudala/araudia/sinadura_politika.pdf

d) Fecha de expedición: 28-10-2020

e) Ámbito de aplicación: el contenido en los artículos 2 (ámbito subjetivo) y 3 (ámbito objetivo) de la Ordenanza de Administración Electrónica.

3.2 Periodo de validez y las consideraciones respecto a los periodos de transición que procedan

La presente Política es válida desde la fecha de expedición, que se indica dentro de los datos de identificación del documento, hasta la publicación de una nueva versión actualizada.

En caso de publicar una nueva versión de la Política, se facilitará un periodo de tiempo transitorio, en el que convivan las dos versiones y que permita adecuar las diferentes plataformas de la Administración municipal a las especificaciones de la nueva versión. Este periodo de tiempo transitorio deberá indicarse en la nueva versión y pasado dicho periodo sólo será válida la versión actualizada.

3.3 Responsable de la gestión

a) Nombre del gestor de la política: Área de Cultura y Gobernanza.

b) Dirección de contacto. Plaza Ernesto Erkoreka nº1. 48007 Bilbao.

4 Reglas comunes

4.1 Formatos admitidos de firma y sello electrónicos

La firma electrónica de transmisiones de datos estará basada en estándares recogidos en la Norma Técnica de Interoperabilidad de Catálogo de estándares. Para transmisiones de datos basadas en Servicios Web, se recomienda la aplicación de firmas electrónicas según el estándar WS-Security: SOAP Message Security de OASIS; en particular, con la especificación estándar X.509 Certificate Token Profile.

Los formatos para la firma 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».

El perfil de formato que se utilizará para la generación de firmas de contenido será “BES”.

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

4.2 Reglas de uso de algoritmos

En lo relativo al uso de algoritmos, se cumplirá lo establecido en la Norma Técnica de Interoperabilidad de Catálogo de estándares y lo previsto en las normas que se definan en aplicación del Reglamento (UE) 910/2014.

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.

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.

4.3 Reglas de creación de firma o sello electrónicos

La presente Política define las condiciones particulares bajo las que, en su ámbito, se generará la firma electrónica.

La plataforma que preste el servicio de creación de firma electrónica proporcionará la funcionalidad necesaria para soportar un proceso de creación de firmas basado en los siguientes puntos:

a) Selección por parte de la persona usuaria firmante del fichero, formulario u otro objeto binario para ser firmado. Los formatos de ficheros atenderán a lo recogido en la Norma Técnica de

Interoperabilidad de Catálogo de estándares. La persona firmante se asegurará de que el fichero que se quiere firmar no incluye contenido dinámico que afecte a su validez y que pudiese modificar el resultado de la firma a lo largo del tiempo.

b) El servicio de firma electrónica ejecutará las siguientes verificaciones previas a la creación de la firma:
    a. La firma electrónica puede ser validada para el formato del fichero específico que va a ser firmado.
    b. 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, según corresponda en función del formato utilizado.

La vinculación de la persona 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 de la persona firmante.
c) Cadena de validación.
d) Formato del objeto original.

Como datos opcionales, la firma electrónica podrá incluir:

a) Lugar geográfico donde se ha realizado la firma del documento.
b) Rol de la persona firmante en la firma electrónica.
c) Acción de la persona 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.

En caso de creación de firmas electrónicas por distintas personas firmantes sobre un mismo objeto, donde la segunda firmante ratifica la firma de la primera, se utilizará la etiqueta correspondiente, CounterSignature, para contabilizarlas.

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

4.4 Reglas de validación de firma o sello electrónicos

Las condiciones mínimas que se producirán para la validación de la firma serán las siguientes:

a) Garantía de que la firma es válida para el fichero específico que está firmado.
b) Validez de los certificados:
    a. El instante de tiempo que se tomará como referencia para la validación será:
        i. El momento en que se produjo la firma si se da alguno de los siguientes supuestos:
            1. los servicios de los prestadores facilitan los históricos de estado de los certificados, y la firma lleva un sello de tiempo válido en el momento de la verificación.
            2. se trata de firmas longevas que incluyen las evidencias de la validez de la firma electrónica en el momento de la generación o primera validación, y dichas evidencias se encuentran selladas con un sello de tiempo válido.
        ii. En otros casos, el momento de la validación.
    b. Se comprobará que los certificados no fueron revocados ni suspendidos y que no han expirado.
    c. 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.
    d. 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.
    e. 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.

5 Reglas de confianza

5.1 Reglas de confianza para los certificados electrónicos

La sede electrónica del Ayuntamiento de Bilbao, para identificarse ante la ciudadanía y garantizar una comunicación segura, deberá utilizar un certificado reconocido o cualificado de autenticación de sitio web o medio equivalente. La entidad responsable de la gestión de dicho certificado es el Centro Informático del Ayuntamiento de Bilbao, BilbaoTIK.

El Ayuntamiento de Bilbao promoverá la utilización de los medios de identificación y firma electrónicas más extendidos en el ámbito social y establecerá acuerdos con las entidades de certificación correspondientes. Así mismo, mantendrá actualizada en su sede electrónica la lista de certificados electrónicos válidos para que la ciudadanía se identifique en la sede web, así como para firmar solicitudes y documentos anexos. Es responsable de dicha actualización la Jefatura de Sección de Gestión de

Proyectos del Área de Cultura y Gobernanza o unidad administrativa que, en su caso, gestione la sede electrónica municipal.

Se presumirán válidos los certificados cualificados que use la ciudadanía en las firmas y sellos electrónicos. Si el Ayuntamiento de Bilbao apreciara algún aspecto que cuestionara esta validez, lo hará saber a la persona interesada, 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. La persona 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.

Los certificados válidos para ejecutar la firma electrónica de contenido serán los certificados electrónicos cualificados de firma y sello según el Reglamento eIDAS.

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 eIDAS.

5.2 Reglas de confianza 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 a utilizar 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 ente 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 de la persona 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”.

5.3 Reglas de confianza para firmas longevas

Los estándares de firma electrónica avanzada XAdES, CAdES y PAdES 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 la persona firmante como por el ente verificador, y se recomienda hacerlo después de trascurrido el periodo de precaución o periodo de gracia.

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 apartado 'Reglas de validación de firma o sello electrónicos'.
b) Se realizará un proceso de completado de la firma electrónica que consistirá en la obtención y almacenamiento de las referencias a:
    - Certificados: Incluyendo los certificados de la persona firmante y de la cadena de certificación tanto de la firmante como del sello de tiempo.
    - 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.

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

6 Archivado y custodia

Toda firma electrónica se almacenará en el Sistema de Gestión de Documentos, de manera vinculada a su documento electrónico correspondiente, el cual atenderá a lo establecido en la Política de gestión de documentos electrónicos del Ayuntamiento de Bilbao.

La validez a largo plazo de una firma electrónica puede verse comprometida por razones como:

a) La caducidad o revocación del certificado utilizado para realizar la firma
b) Debilidades en los algoritmos criptográficos utilizados.
c) Caducidad de otros certificados usados en la firma o el resellado

El Ayuntamiento de Bilbao debe tener un servicio para mantener las evidencias de validez de las firmas longevas. Este servicio utilizará mecanismos de resellado de tiempo, para añadir, cuando el anterior sellado este próximo a su caducidad, un sello de tiempo con un algoritmo más robusto. También se utilizarán mecanismos de resellado, con un algoritmo más robusto, en el caso de obsolescencia de los algoritmos o formatos. La responsabilidad del correcto funcionamiento del servicio será de la unidad responsable del repositorio de documentos.

En el caso de que, en un futuro, los recursos necesarios para realizar el resellado de documentos superen los recursos del Ayuntamiento de Bilbao destinados a tal fin, será suficiente con el resellado de la firma longeva del índice del expediente electrónico.

Cuando la firma, los sellos de tiempo y los certificados no puedan garantizar la autenticidad y la evidencia de los documentos electrónicos a lo largo del tiempo, éstas les sobrevendrán a través de su conservación

y custodia en los repositorios y archivos electrónicos, así como de los metadatos de gestión de documentos y otros metadatos vinculados, de acuerdo con las características que se definirán en la Política de gestión de documentos electrónicos.

7 Gestión de la política de firma y sello

La unidad gestora de la Política la mantendrá actualizada atendiendo a:

a) Modificaciones motivadas por necesidades propias de la administración municipal.
b) Cambios en políticas relacionadas.
c) Cambios en los certificados electrónicos emitidos por los prestadores de servicios de certificación referenciados en la Política.

Para facilitar la validación de firmas electrónicas creadas atendiendo a versiones anteriores de la Política, se mantendrá un repositorio con el historial de versiones anteriores que provea la ubicación de cada versión.