NOR008 – Política de firma electrónica y de certificados

Clasificación de la Información:

Nivel del Documento	Procedimiento
Nombre del Fichero	NOR008 – Politica de firma electronica.docx
Tipo	Publico
Ámbito de Difusión	Comité de Seguridad del AYUNTAMIENTO DE PAIPORTA
Responsable	Responsable de Seguridad del AYUNTAMIENTO DE PAIPORTA

CONTROL DE FIRMAS

	FECHA	FIRMA
ELABORADO POR MARIA SANCHIS	18/02/2022	
APROBADO POR COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	18/02/2022	

CONTROL DE VERSIONES

VERSIÓN	FECHA	AUTOR	CAMBIOS
1.0	18/02/2022	María Sanchis	Versión inicial del documento.
2.0	17/09/2024	María Sanchis	Actualización del apartado 6 y 7.

ÍNDICE DE CONTENIDO

1. OBJETO 4
2. ALCANCE 4
3. NORMATIVA Y ESTÁNDARES DE APLICACIÓN 4
4. GLOSARIO 5
5. DATOS IDENTIFICATIVOS Y VALIDEZ DE LA POLÍTICA 5
6. REGLAS COMUNES 6
6.1. REGLAS DEL FIRMANTE 6
6.2. REGLAS DEL VERIFICADOR 8
7. REGLAS DE CONFIANZA 9
7.1. REGLAS DE CONFIANZA DE CERTIFICADOS ELECTRÓNICOS 9
7.2. REGLAS DE CONFIANZA PARA LOS SELLOS DE TIEMPO 9
7.3. REGLAS DE CONFIANZA PARA FIRMAS LONGEVAS 10
7.4. FIRMA BIOMÉTRICA 11
7.5. FIRMA CON PSEUDÓNIMO (OCULTA) 12
8. IDENTIFICACIÓN 12
8.1. MEDIANTE CERTIFICADO DE FIRMA ELECTRÓNICA 12
8.2. MEDIANTE “CL@VE PIN” Y “CL@VE PERMANENTE” 13
8.3. MEDIANTE CERTIFICADOS DE SELLO ELECTRÓNICO 13
9. GESTIÓN DE LA POLÍTICA DE FIRMAS 13
9.1. ARCHIVO Y CUSTODIA 14
9.2. CONSERVACIÓN A LARGO PLAZO 14
10. AUTENTICIDAD DE LOS DOCUMENTOS 15
10.1. CÓDIGO SEGURO DE VERIFICACIÓN (CSV) 15
10.2. PROCEDIMIENTO DE VERIFICACIÓN DE LOS DOCUMENTO CON CSV GENERADOS POR LA PLATAFORMA 15
11. POLÍTICA DE FIRMA DE LA ADMINISTRACIÓN GENERAL DEL ESTADO 18
12. ROLES Y RESPONSABILIDADES 18

1. OBJETO

El presente documento tiene por objeto la definición de los distintos mecanismos de identificación y firma admitidos en la sede electrónica y resto de subsistemas de la plataforma de administración electrónica SEDIPUALBA que utiliza el Ayuntamiento de Paiporta bajo convenio con la Diputación de Albacete. Esta plataforma integra los sistemas de gestión de expedientes y de archivo electrónico corporativo. De este modo se pretende establecer el esquema de referencia de la Organización para la identificación, la autenticación y el reconocimiento de firmas electrónicas basadas en certificados, recogidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Los objetivos perseguidos con el uso de certificados de firma electrónica son los siguientes:

- En la firma de documentos y contenidos electrónicos, garantizar la autenticidad, la integridad y el no repudio de los mismos.
- En la firma electrónica de transmisión de datos, garantizar la autenticación de los actores involucrados, así como la integridad del contenido del mensaje de datos y el no repudio de los mensajes en una comunicación telemática.

Los certificados electrónicos de firma electrónica podrán ser utilizados, asimismo, por parte de los ciudadanos y empleados públicos de la Organización, como medio de autenticación de la identidad, como medio de firma electrónica de documentos y de certificación de la integridad de un documento.

Por otra parte, en el presente documento se concretan los procedimientos a seguir por la Organización para la generación, validación y conservación de firmas electrónicas, así como las características y requisitos exigibles a los sistemas de firma electrónica, los certificados, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas de la Organización.

La presente política, de primer nivel normativo, proporciona respuesta a lo dispuesto por el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS) y, más en concreto, a las previsiones que siguen:

- Firma electrónica [mp.info.3]
- Marco organizativo. Procedimientos de seguridad [org.3].

2. ALCANCE

El ámbito de aplicación de la presente política será el de las firmas electrónicas realizadas por la Organización afectando a:

- Las relaciones de los ciudadanos con la Organización.
- Las relaciones de la Organización con otras Administraciones.

3. NORMATIVA Y ESTÁNDARES DE APLICACIÓN

En el documento “DOC007 – Registro de requisitos legales y normativa” se relaciona la normativa legal y los estándares que se han tenido en consideración para la elaboración de la presente norma.

4. GLOSARIO

TÉRMINO	DESCRIPCIÓN
Firma electrónica	Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
Política de firma electrónica	Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan las firmas electrónicas, incluyendo las características exigibles a los certificados de firma.
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 la política de firma concreta por la que se rige la plataforma de relación electrónica o el servicio concreto al que se esté invocando. Podrá ser una entidad de validación de confianza o una tercera parte que esté interesada en la validez de una firma electrónica.
Prestador de servicios de certificación (PSC)	Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
Emisor y gestor de la política de firma	Entidad que se encarga de generar y gestionar el documento de política de firma, por el cual se deben regir el firmante, el verificador y los prestadores de servicios en los procesos de generación y validación de firma electrónica.

5. DATOS IDENTIFICATIVOS Y VALIDEZ DE LA POLÍTICA

El presente documento de política de firma electrónica y de certificados tendrá un identificador único, asignándose los dos últimos dígitos a la versión que corresponda, al objeto de distinguir las versiones sucesivas que puedan existir cuando se realicen actualizaciones.

La presente política de firma electrónica y de certificados será válida desde la fecha de emisión indicada hasta que sea derogada o se publique una nueva versión. Los períodos de transición serán indicados en las nuevas versiones y, una vez transcurridos los plazos indicados, serán válidas únicamente las versiones actualizadas.

Además, en el caso de actualización de la presente política de firma electrónica y de certificados, se identificará el enlace URL donde encontrar las versiones anteriores para verificar una firma electrónica anterior a la política vigente.

	IDENTIFICADOR DE LA POLÍTICA
Nombre del documento	Política de Firma Electrónica y de Certificados del Ayuntamiento de Paiporta.
Versión	1.0

Identificación del documento	OID 2.16.724.1.3.1.1.2.1.0
URL de referencia	https://paiporta.sedipualba.es/
Fecha de emisión	11/0/2024
Ámbito de aplicación	Ayuntamiento de Paiporta

Al gestor de la presente política de firma electrónica y de certificados corresponde el mantenimiento, actualización y publicación electrónica de los criterios sobre firma electrónica.

	IDENTIFICADOR DEL GESTOR
Nombre del gestor de la Política	Área de Innovación del Ayuntamiento de Paiporta
Dirección de contacto	C/ Mestre Músic Vicent Prats i Tarazona, s/n Paiporta (Valencia, España) 46200

6. REGLAS COMUNES

Las reglas comunes establecen las 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.

Estas reglas se definen de acuerdo con los formatos de firma electrónica admitidos, teniendo en cuenta los diferentes usos de la firma electrónica basada en certificados, el uso de algoritmos y los procesos de creación y validación de firma.

6.1. REGLAS DEL FIRMANTE

El firmante será responsable de que el fichero que se quiere firmar no incorpora 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, se asegurará que no existe contenido dinámico dentro del fichero, como pueden ser macros.

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

- 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 como sigue.

    - Una referencia explícita al presente documento de política de firma 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. <xades:SigPolicyId> <xades:Identifier> ... </xades:Identifier>
    - 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 utilizara para su validación.

- DataObjectFormat: define el formato del documento original, y es necesario para que el receptor conozca la forma de visualizar el documento.

Las etiquetas restantes que pueden agregarse en el campo SignedProperties serán consideradas de carácter opcional, sin perjuicio de su consideración obligatoria en políticas particulares, siempre basadas en la política marco:

- SignatureProductionPlace: define el lugar geográfico donde se ha realizado la firma del documento.
- SignerRole: define el rol de la persona en la firma electrónica. Al menos uno de estos elementos ClaimedRoles o CertifiedRoles deben estar presentes en este campo: o “supplier” o “emisor”: cuando la firma la realiza el emisor.
    - “customer” o “receptor”: cuando la firma la realiza el receptor.
    - “third party” o “tercero”: cuando la firma la realiza una persona o entidad distinta al emisor o al receptor.
- CommitmentTypeIndication: define la acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, ...)
- AllDataObjectsTimeStamp: contiene un sello de tiempo, calculado antes de la generación de la firma, sobre todos los elementos contenidos en ds:Reference.

- IndividualDataObjectsTimeStamp: contiene un sello de tiempo, calculado antes de la generación de la firma, sobre algunos de los elementos contenidos en ds:Reference.

6.2. REGLAS DEL VERIFICADOR

El encargado de la verificación de la firma será responsable de definir los procesos de validación y de archivado, de conformidad con los requisitos de la política de firma particular a la que se ajusta el servicio y con lo establecido en la NTI de Política de gestión de documentos electrónicos.

El formato básico de firma electrónica avanzada no incluye ninguna información de validación más allá del certificado firmante, que está incluido 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, CAdES 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 haya caducado y se pueda acceder a los datos de verificación (CRL, OCSP, etc) o bien en el caso de que el prestador de servicios de certificación (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.

Existe un tiempo de espera, conocido como periodo de precaución o periodo de gracia, para comprobar el estado de revocación de un certificado.

El encargado de la verificación podrá esperar este plazo para validar la firma o realizarla en el mismo momento y revalidarla después. El periodo desde que se realiza la firma o el sellado de tiempo deberá, 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 plazos podrán variar en función del Prestador de Servicios de Certificación.

7. REGLAS DE CONFIANZA

7.1. REGLAS DE CONFIANZA DE CERTIFICADOS ELECTRÓNICOS

Para ejecutar la firma electrónica de contenido se consideraran válidos aquellos certificados reconocidos de conformidad con la Ley 59/2003, de 19 de diciembre, y con la Directiva 1999/93/CE de 13 de diciembre de 1999, así como las nuevas tipologías de certificados definidos en la Ley 11/2007, de 22 de junio y los sistemas de firma y certificados electrónicos de acuerdo con el artículo 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En consecuencia, con lo anterior, los certificados admitidos son los que siguen:

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 cualificados de servicios electrónicos de confianza"[1].

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 cualificados de servicios electrónicos de confianza".

b) Otros sistemas que la Organización pueda considerar válido para realizar determinados trámites o procedimientos de su ámbito de competencia, en los términos y condiciones que se establezcan.

Los certificados de firma electrónica de empleado público emitidos por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM) se consideran válidos para la realización de firma electrónica por parte de los empleados de la Organización y, en consecuencia, garantizan la identificación y firma de los participantes en la tramitación de cuantos procedimientos electrónicos se determinen.

La relación de sellos electrónicos utilizados por el Ayuntamiento de Paiporta, indicando las características de los certificados electrónicos y los prestadores que los expiden será pública y accesible a través de su sede electrónica. Adicionalmente, la verificación de los sellos y certificados electrónicos, incluyendo el de la propia sede, se podrá efectuar a través de la "Aplicación de VALIdación de firma y certificados Online y Demostrador de servicios de @firma"[2] u otros sistemas reconocidos de validación electrónica.

7.2. REGLAS DE CONFIANZA PARA LOS SELLOS DE TIEMPO

El sello electrónico 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

[1] https://sede.serviciosmin.gob.es/prestadores/paginas/inicio.aspx

[2] https://valide.redsara.es/valide/inicio.html

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 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".

7.3. REGLAS DE CONFIANZA PARA FIRMAS LONGEVAS

Los estándares XAdES (ETSI TS 101 903) en sus diferentes versiones 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. La información podrá ser incluida por el firmante o por el verificador, y deberá hacerse transcurrido el periodo de precaución o 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.
- los 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 deberá usar validación mediante OCSP (Online Certificate Status Protocol), 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 generara un elevado volumen de información, alternativamente a la información de validación indicada anteriormente, se podrá incluir en la firma longeva referencias a dicha información. 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 la información de validación, se utilizará 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, adicionalmente a las referencias a la información de validación, 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.

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.

7.4. FIRMA BIOMÉTRICA

La firma biométrica se considerará, a todos los efectos, equivalente a la firma manuscrita y se realizará en presencia de un empleado público que garantizará la identidad del firmante.

Se seguirá el siguiente procedimiento:

1. El empleado público solicita el DNI al firmante y comprueba que sus datos identificativos se corresponden con los que constan en el sistema.

2. El sistema compone el documento de firma combinado:

2.1. Se eliminan los espacios en blanco, obteniendo su forma canónica según el procedimiento estándar del W3C (https://www.w3.org/TR/xmlc14n11/).

2.2. Se calcula el hash SHA3-512.

3. Se informa al firmante acerca de los datos a firmar:

3.1. Por un lado, se muestran en la pantalla del dispositivo de firma tanto el hash calculado como la fecha y hora del PC al que está conectado.

3.2. Por otro lado, ese mismo hash y la correspondiente relación de documentos PDF a firmar se pondrán a disposición del firmante a través de una pantalla de visualización, para su cotejo, antes de solicitarle que firme.

4. El firmante realiza la firma.

5. El empleado público comprueba que la firma trazada corresponde con la firma que consta en el DNI y la acepta.

6. El sistema almacena el fichero de firma generado por el dispositivo y el dibujo de la firma.

7. El sistema sella electrónicamente el documento XML correspondiente a la firma biométrica, con el siguiente formato, que contiene el hash mostrado en la pantalla del dispositivo antes de firmar y el contenido del fichero de firma generado, así como los datos personales del firmante y los datos personales del empleado que recoge la firma.

Por motivos de seguridad de la información y protección de los datos de carácter personal, ni la firma biométrica ni el sello de tiempo serán accesibles públicamente mediante el CSV. Sí lo será el trazo de la firma, al igual que sería visible la rúbrica de la firma manuscrita en un documento en papel.

Los administradores de la sede podrán acceder a la información de forma completa en caso de que fuera necesario.

7.5. FIRMA CON PSEUDÓNIMO (OCULTA)

La firma con pseudónimo (u oculta) en el ámbito de la presente política consiste en una firma electrónica o biométrica cuyos datos no están disponibles públicamente al verificar el correspondiente CSV. Entre estos datos se encuentran la firma propiamente dicha y los datos identificativos del firmante (NIF, nombre y apellidos).

Únicamente los administradores de la sede pueden obtener todos los datos relativos a esta firma, en caso de ser necesario. El resto de personas únicamente podrán visualizar el pseudónimo utilizado en la firma.

8. IDENTIFICACIÓN

Se reconocen los siguientes sistemas de identificación de terceros en su relación con el Ayuntamiento de Paiporta en el ámbito de la presente política.

8.1. MEDIANTE CERTIFICADO DE FIRMA ELECTRÓNICA

Al objeto de comparecer ante la sede y relacionarse con la plataforma se admite la identificación basada en los siguientes tipos de certificados:

- Certificado de persona física, incluido el de empleado público.

- Certificado de representante.
- Certificado jurídico.

Únicamente se reconocerán certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’, accesible en el momento de aprobación de la presente política a través de la siguiente dirección: https://sedeaplicaciones.minetur.gob.es/Prestadores/

8.2. MEDIANTE “CL@VE PIN” Y “CL@VE PERMANENTE”

Se admite la identificación de las personas físicas mediante el sistema Cl@ve, en sus modalidades de “Cl@ve PIN” y “Cl@ve permanente”, para la realización de cualquier trámite.

Cl@ve es un sistema orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos. Su objetivo principal es que el ciudadano pueda identificarse ante la Administración mediante claves concertadas (usuario más contraseña), sin tener que recordar claves diferentes para acceder a los distintos servicios.

El sistema Cl@ve fue aprobado por Acuerdo del Consejo de Ministros, en su reunión del 19 de septiembre de 2014, y sus condiciones de utilización son determinadas por la Dirección de Tecnologías de la Información y las Comunicaciones.

Más información, accesible en el momento de aprobación de la presente política, a través de la siguiente dirección: https://clave.gob.es/

8.3. MEDIANTE CERTIFICADOS DE SELLO ELECTRÓNICO

A la hora de la integrar aplicaciones de terceros con la plataforma de administración electrónica y garantizar su identificación se admitirán exclusivamente certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.

No se admitirán certificados de sello a efectos de comparecencia del titular del mismo en la sede electrónica (acceso a notificaciones electrónicas, acceso a la carpeta ciudadana para consultar estado de tramitación, comparecencia en el trámite, etc.) ni para la presentación de solicitudes o la realización de cualquier otro trámite administrativo.

9. GESTIÓN DE LA POLÍTICA DE FIRMAS

El mantenimiento, actualización y publicación electrónica del presente documento corresponderá al Área de Innovación del Ayuntamiento de Paiporta.

El Área de Innovación del Ayuntamiento de Paiporta mantendrá, en los portales destinados a tal función, tanto la versión actualizada del presente documento como un repositorio con el historial de las versiones anteriores de la política de firma electrónica para el organismo.

En el caso de actualización del presente documento, se identificará el lugar donde un validador puede encontrar las versiones anteriores para verificar una firma electrónica anterior a la política vigente.

En el momento de la firma se incluirá la referencia del identificador único de la versión del presente documento de política de firma electrónica sobre el que se ha basado, el cual determina las condiciones que debe cumplir la firma electrónica en un momento determinado. El campo destinado para incluir esta referencia será, en los formatos de firma avanzada (XAdES, CAdES y PAdES), el campo SignaturePolicyIdentifier.

9.1. ARCHIVO Y CUSTODIA

Las transmisiones de datos firmadas se almacenarán el tiempo que resulte imprescindible para la acreditación de su validez a largo plazo.

El contenido firmado, para garantizar la fiabilidad de una firma electrónica y que ésta tenga efectos jurídicos frente a terceros a lo largo del tiempo, deberá ser complementada con la información del estado del certificado asociado en el momento en que la misma se produjo, así como los certificados que conforman la cadena de confianza incorporando sellos de tiempo para los elementos añadidos. Toda esta información se almacenará en el repositorio de no repudio.

En dicho repositorio, se almacenarán todas las firmas del contenido, tanto las realizadas con certificado de persona física o jurídica como con sello de órgano o equivalente, ya hayan sido realizadas internamente en el ámbito de las aplicaciones del organismo (se almacenarán en el momento de su creación) como en el exterior (se almacenarán en el momento de su validación).

En cualquiera de los casos, se almacenará como mínimo la firma y un sello de tiempo.

En el repositorio de no repudio se almacenará, como mínimo, la firma con sello de tiempo (formatos XAdEST/CAdES-T/PAdES-EPES con atributo signature-time-stamp). Si se necesitara conservación a largo plazo de la firma, se almacenará en formato XAdES-A/CAdES-A/PAdES-LTV que asegura la totalidad del documento y las firmas contenidas.

Se procederá al resellado de las firmas cuando así sea preciso o cualesquiera otras medidas técnicas necesarias.

9.2. CONSERVACIÓN A LARGO PLAZO

Para proteger la firma electrónica frente a la posible obsolescencia de los algoritmos y poder seguir asegurando sus características de validez, se almacenarán en un depósito seguro, garantizando su protección contra falsificaciones y asegurando la fecha exacta en que se guardaron. Las operaciones de fechado se garantizan mediante el repositorio de no repudio.

Para garantizar la conservación a largo plazo se utilizarán mecanismos de sellado y resellado de tiempo. Las firmas guardadas en el repositorio de no repudio deben ser selladas.

Los casos en los que se necesitará realizar un resellado de las firmas selladas y almacenadas en el repositorio de no repudio, serán los que siguen:

- Cuando alguno de los algoritmos utilizados en un sello de tiempo usado para sellar una firma haya sido declarado obsoleto. El resellado, en ese caso, lo realizará una autoridad de sellado que use algoritmos actuales, seguros y adaptados a esta situación.

- Cuando el certificado de la autoridad de sellado que ha sido usado para sellar una firma haya sido revocado, caducado o esté próximo a caducar. En este caso se utilizará una autoridad de sellado cuyo certificado sea válido y tenga un periodo de validez adecuado.

10. AUTENTICIDAD DE LOS DOCUMENTOS

La autenticidad de las firmas electrónicas y documentos producidos en el ámbito de esta política se acreditará y verificará en las siguientes condiciones.

10.1. CÓDIGO SEGURO DE VERIFICACIÓN (CSV)

El código seguro de verificación de un documento identifica biunívocamente a un documento y un conjunto de firmas y/o sellos electrónicos.

Consta de hasta 20 dígitos alfanuméricos, y su conocimiento permite el acceso a un documento PDF sellado electrónicamente por el certificado de sello de esta sede para garantizar la autenticidad e interoperabilidad. En él se incluye el documento íntegro originalmente firmado y la correspondiente información de las firmas.

El PDF sellado será conforme la especificación técnica ETSI TS 102 778-3 versión 1.2.1 y ETSI TS 102 778-4.

El CSV proporcionará acceso a la siguiente información:

- Documento CSV.
- Documento original.
- Firmas electrónicas en formato XAdES.
- Otra información relativa al documento firmado (identificación de los firmantes, fecha y hora de las firmas, título del documento, etc.).

10.2. PROCEDIMIENTO DE VERIFICACIÓN DE LOS DOCUMENTO CON CSV GENERADOS POR LA PLATAFORMA

Se garantizará que cualquiera, empleado público de esta administración o tercera parte independiente, tenga la capacidad de comprobar por un lado la validez, autenticidad e integridad de los documentos con CSV generados en el ámbito de esta política y, por otro, la validez, autenticidad e integridad de la información y firmas asociadas a éstos.

Para realizar la verificación se deberán utilizar medios o dispositivos informáticos en condiciones seguras (no comprometidos o libres de software malicioso).

Cuando se acceda mediante un navegador web a la dirección de la sede electrónica, lugar dónde se podrán verificar los documentos CSV, se deberá comprobar que no muestra ninguna alerta sobre la validez del certificado SSL.

A continuación, se detallan los diferentes procedimientos de verificación.

Una vez se esté en posesión del documento en papel con CSV se seguirán los siguientes pasos para su verificación:

1. Acceder mediante un navegador web a la dirección de verificación de CSV de la sede electrónica (asimismo reflejada en el propio documento):

https://paiporta.sedipualba.es/csv/

2. Introducir el código CSV impreso en el margen del documento.

3. Comprobar que la sede electrónica indica que existe un documento con ese CSV y que al descargarlo coincide con el documento impreso (deben ser idénticos).

10.2.1. VERIFICACIÓN DE DOCUMENTOS CON CSV ENTREGADOS EN FORMATO ELECTRÓNICO (PDF)

Una vez se esté en posesión del documento electrónico con CSV se seguirán los siguientes pasos para su verificación:

1. Validar las firmas del documento CSV mediante la aplicación VALIDe de la Administración General del Estado o mediante un programa lector de documentos PDF con la capacidad de verificar firmas electrónicas en formato PAdES LTA-level:

   1.1. Si el CSV consta de 20 dígitos: comprobar que la aplicación acredita que la firma es válida y que el documento está firmado mediante un certificado de sello electrónico incluido en el listado al que se hace referencia en el apartado 7 de la presente política. Si la firma contiene sellado de tiempo, éste también debe presentarse como válido (PAdES LTA-level).

   1.2. Si el CSV consta de menos de 20 dígitos: comprobar que la aplicación acredita que las firmas son válidas. Si la firma contiene sellado de tiempo, éste también debe presentarse como válido.

2. Adicionalmente, comprobar que el documento CSV existe en la sede electrónica:

   2.1. Acceder mediante un navegador web a la dirección de verificación de CSV de la sede electrónica (asimismo reflejada en el propio documento): https://paiporta.sedipualba.es/csv/

2.2. Introducir el código CSV impreso en el margen del documento.

2.3. Comprobar que la sede electrónica indica que existe un documento con ese CSV y que al descargarlo coincide con el documento electrónico (deben ser idénticos).

10.2.2. VERIFICACIÓN DE DOCUMENTOS DE FIRMA ELECTRÓNICA XAdES

Los documentos de firma XAdES producidos en el ámbito de esta política estarán asociados a sus correspondientes documentos originales o a sus correspondientes documentos CSV.

La autenticidad y validez de las firmas electrónicas XAdES se acreditará y verificará siguiendo el siguiente procedimiento:

1. Recabar la siguiente información:

- Documento original.
- Fichero de firma electrónica en formato XAdES-A.
- Título del documento.
- Información del firmante.
- Código aleatorio (salt o sal) con la que se generó la huella firmada en el documento XAdES-A.

2. Validar el fichero de firma electrónica mediante la aplicación VALIDe de la Administración General del Estado. Al ser un formato estándar, se pueden usar otras herramientas con capacidad de validación de firmas.

3. Comprobar que la firma validada en el punto anterior se corresponde con el documento firmado:

3.1. Calcular el hash SHA3-512 sobre el resultado de concatenar el documento binario original + el título del documento codificado en UTF-8 + la información del firmante codificado en UTF-8 + la “sal”.

3.2. Abrir el fichero XAdES-A y comprobar que el elemento en la ruta XPath /ds:Signature/ds:Object/documentos_firmados contiene un elemento documento_firmado con el hash calculado anteriormente y la "sal" utilizada (ambos codificados en Base64).

3.3. Comprobar que el XPath anterior se encuentra incluido en alguna de las referencias del elemento SignedDataObjectProperties, y por tanto firmado.

En caso de que todas las comprobaciones anteriores hayan resultado satisfactorias, quedaría probado que el documento original se corresponde con la firma XAdES-A, la cual garantiza la integridad del documento, su autenticidad y el no repudio.

Dado que la validación de la firma XAdES resulta un procedimiento complejo, se publicará una herramienta que de forma automática permita verificar su correspondencia con el documento original firmado.

Adicionalmente, el código fuente de esta herramienta se publicará sin restricciones de acceso en un repositorio al efecto. De esta manera los terceros que dispongan de los medios y conocimientos tecnológicos precisos podrán generar la herramienta que les permita verificar de forma autónoma e independiente la validez de los documentos producidos en el ámbito de esta política.

11. POLÍTICA DE FIRMA DE LA ADMINISTRACIÓN GENERAL DEL ESTADO

Se considerarán válidos, y por tanto se admitirán, todos aquellos mecanismos de identificación y firma reconocidos en la Política de firma electrónica y de certificados de la Administración General del Estado, así como todos aquellos documentos producidos o resultantes de los mismos.

12. ROLES Y RESPONSABILIDADES

ROL	DESCRIPCIÓN
Responsable de Seguridad	• Colaborar con el gestor de la política de firma en la especificación en el mantenimiento y actualización del presente documento.
Responsable del Sistema	• Colaborar con el gestor de la política de firma en el mantenimiento, actualización y publicación electrónica del presente documento