

INFORMACIÓN DEL DOCUMENTO

FECHA	VERSIÓN	DESCRIPCIÓN DE CAMBIOS
22/08/22	01	Versión inicial documento
01/10/24	02	Se revisa el contenido del documento, se adecua al ENS (Real Decreto 311/2022)

Control de versiones de Política de firma electrónica

VERSIÓN	CLASIFICACIÓN DEL DOCUMENTO	ELABORADO POR	REVISADO POR	APROBADO POR
02	Público	Responsable del Sistema	Responsable de Seguridad	Comité de Seguridad
				Firma:

Estado de Procedimiento de Política de firma electrónica

Firma 1 de 1
 Judith Castro Gómez
 26/11/2024
 Concejal Económico, G
 Fondos Europeos y O AAPP

Para consultar la autenticidad de este documento consulte la siguiente página web

Código Seguro de Validación f789a173c47740b0ba709ad33f119dc3001

Url de validación <https://sede.aytopalencia.es/absis/idi/arx/idiarxabsaweb/castellano/asp/verificadorfirma.asp>

Metadatos Origen: Origen administración Estado de elaboración: Original



Índice

INFORMACIÓN DEL DOCUMENTO.....	1
1 INTRODUCCIÓN.....	3
2 ALCANCE.....	4
3 EFECTOS.....	4
4 NORMAS PARTICULARES POLÍTICA DE FIRMA ELECTRÓNICA.....	4
4.1 Certificados admitidos.....	5
4.2 Tipos de certificados.....	5
4.3 Certificados de empleado público.....	5
4.4 Sellos de tiempo.....	6
4.5 PLATAFORMAS Y SISTEMAS DE INFORMACIÓN.....	6
4.6 Condiciones para salvaguardar la validez de las firmas.....	7

Firma 1 de 1	Judith Castro Gómez	26/11/2024	Concejal Económico, G Fondos Europeos y O AAPP
--------------	---------------------	------------	---

Para consultar la autenticidad de este documento consulte la siguiente página web

Código Seguro de Validación f789a173c47740b0ba709ad33f119dc3001

Url de validación <https://sede.aytopalencia.es/absis/idi/arx/idiarxabsaweb/castellano/asp/verificadorfirma.asp>

Metadatos Origen: Origen administración Estado de elaboración: Original



1 INTRODUCCIÓN

Una Política de firma electrónica y de certificados es el “conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, se verifican y se gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma”, según la definición del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.

Con carácter general, una política de firma electrónica es un documento legal que contiene una serie de normas relativas a la firma electrónica, organizadas alrededor de los conceptos de generación y validación de firma, en un contexto particular (contractual, jurídico, legal), definiendo las reglas y obligaciones de todos los actores involucrados en el proceso. El objetivo es determinar la validez de la firma electrónica para una transacción en particular, especificando la información que debe incluir la persona firmante en el proceso de generación de la firma y la información que se debe comprobar en el proceso de validación.

El artículo 18 del citado Real Decreto 4/2010, de 8 de enero, establece que las Administraciones Públicas aprobarán y publicarán una política de firma electrónica y de certificados partiendo de la norma técnica aprobada al efecto que es la Norma Técnica de Interoperabilidad de Política de Firma y Certificados de la Administración aprobada por Resolución de fecha 19 de julio de 2011 de la Secretaría de Estado para la Función Pública.

En cuanto a la competencia para la aprobación de esta política del Ayuntamiento de Palencia, teniendo en cuenta que la misma está constituida, entre otras, por un conjunto de normas de seguridad, para determinar cómo se generan, verifican y gestionan firmas electrónicas, debe considerarse consustancial a la Política de Seguridad del Ayuntamiento de Palencia.

Para dar cumplimiento al mp.info.3 Firma Electrónica del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad se cumplirá con los siguientes puntos:

- Se empleará cualquier tipo de firma electrónica de los previstos en la legislación vigente.
- Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.
- Se emplearán algoritmos y parámetros acreditados por el Centro Criptológico Nacional.
- Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquella soporte.
- Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación: Certificados; Datos de verificación y validación.

Se definen las acciones a llevar a cabo para la protección de aplicaciones del Ayuntamiento de Palencia.

Firma 1 de 1
 Judith Castro Gómez
 26/11/2024
 Concejal | Económico, G
 Fondos Europeos y O AAPP

Para consultar la autenticidad de este documento consulte la siguiente página web

Código Seguro de Validación f789a173c47740b0ba709ad33f119dc3001

Url de validación <https://sede.aytopalencia.es/absis/idi/arx/idiarxabsaweb/castellano/asp/verificadorfirma.asp>

Metadatos Origen: Origen administración Estado de elaboración: Original



2 ALCANCE

Esta Política se aplicará a los sistemas de información del Ayuntamiento de Palencia, que estén relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo.

Todos los miembros del Ayuntamiento de Palencia, afectados por el alcance del ENS, tienen la obligación de conocer y cumplir esta “**Política de Firma Electrónica**” siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

La política de firma aprobada será de aplicación, en el ámbito competencial de la Administración Municipal, a los siguientes casos:

- Las relaciones electrónicas del Ayuntamiento de Palencia con los ciudadanos y proveedores en todos los servicios y procedimientos puestos a su disposición en la respectiva Sede Electrónica incluida O.V.C. siempre que sea obligada o se permita la firma electrónica con certificado digital.
- Los ciudadanos podrán utilizar sistemas de identificación y firma no basados en el uso de certificados electrónicos reconocidos en aquellos trámites administrativos para los que resulten suficientemente seguros, teniendo en cuenta los datos e intereses afectados y con base en la evaluación del principio de proporcionalidad definido en el Esquema Nacional de Seguridad.
- Las relaciones electrónicas entre los distintos órganos y empleados del Ayuntamiento de Palencia.
- Las relaciones electrónicas del Ayuntamiento de Palencia con el resto de Administraciones y Entidades Públicas.

3 EFECTOS

La presente Política surtirá efectos a partir del día siguiente al de su publicación.

4 NORMAS PARTICULARES POLÍTICA DE FIRMA ELECTRÓNICA

Las Normas particulares de la Política de firma electrónica y certificados del Ayuntamiento de Palencia se estructuran en los siguientes puntos:

- Certificados admitidos.
- Tipos de certificados.
- Certificados de empleado público.
- Sellos de tiempo.



- Plataformas y sistemas de información.
- Condiciones para salvaguardar la validez de las firmas.

4.1 Certificados admitidos

En general, se admitirán los certificados incluidos en la relación de proveedores y certificados admitidos por la plataforma @firma, indicados en <https://administracionelectronica.gob.es/ctt/afirma>.

4.2 Tipos de certificados

Se definen las instrucciones de uso general de las distintas tipologías de certificados, en uso de la facultad otorgada al Ayuntamiento de Palencia dentro de su ámbito de competencias. Partiendo del documento denominado “**Plataforma @Firma. Cambios asociados al reglamento eIDAS**” disponible en el Portal de Administración Electrónica (PAE) (https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2016/Marzo/Noticia-2016-03-18-Cambios-en-Plataforma--firma-asociados-al-reglamento-eIDAS-.html#.Y8aXy3bMIdU), serán admitidos todos los certificados relacionados en el documento a excepción de los clasificados en el punto 2 (No reconocidos) y que pueden incluir certificados de persona física, de componente y SSL.

Igualmente, los certificados clasificados a extinguir se seguirán manteniendo hasta su caducidad o revocación. Los sistemas de información y servicios electrónicos de la Ayuntamiento de Palencia deberán aceptar y adaptarse a los citados tipos de certificados. Dicha adaptación deberá ser valorada por cada servicio y su aplicación se ajustará a la normativa de aplicación.

4.3 Certificados de empleado público

Las solicitudes de certificados de empleado público para la Administración Municipal se gestionarán a través del Departamento Innovación, Nuevas Tecnologías e Informática y éste se encargará de coordinar la tramitación con el proveedor del certificado.

La solicitud deberá incluir el órgano titular del certificado, el tipo de certificado, el nombre de la persona titular del mismo si procede, los motivos de la petición y el uso previsto. Los diferentes Responsables de la unidad del usuario son los encargados de la solicitud de nuevos certificados, y de la petición de su renovación o revocación.

Se deberá facilitar la lista de personal de cada Servicio o Departamento que vaya a necesitar el uso de certificado digital facilitando la información que proceda en cada caso a requerimiento del Departamento Innovación, Nuevas Tecnologías e Informática.

El Departamento Innovación, Nuevas Tecnologías e Informática ayudará en el caso que fuera necesario al usuario a la instalación y puesta en funcionamiento del Certificado Digital pero será cada usuario el responsable de su gestión su propio certificado.

Firma 1 de 1
Judith Castro Gómez
26/11/2024
Concejal I Económico, G
Fondos Europeos y O AAPP

Para consultar la autenticidad de este documento consulte la siguiente página web	
Código Seguro de Validación	f789a173c47740b0ba709ad33f119dc3001
Url de validación	https://sede.aytopalencia.es/absis/idi/arx/idiarxabsaweb/castellano/asp/verificadorfirma.asp
Metadatos	Origen: Origen administración Estado de elaboración: Original



4.4 Sellos de tiempo

La Administración Municipal deberá según la normativa de aplicación asociar a los documentos administrativos firmados con certificados electrónicos una de las siguientes modalidades de referencia temporal:

- “Marca de tiempo” entendiéndose por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello de tiempo.
- “Sello de tiempo”, entendiéndose por tal la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

Para ello el Ayuntamiento de Palencia se tomará como autoridad de sellado de tiempo (TSA) corporativa, la plataforma de Sellado de Tiempo TS@ de @firma (en su versión basada en servicios web) ofrecida por el actual ministerio de Hacienda y Administraciones Públicas y accesible a través de la red SARA.

Como medida de contingencia el Ayuntamiento de Palencia podría utilizar en caso de fallo de la plataforma @firma la plataforma de sellado de tiempo de la FNMT o de otro proveedor de sello de tiempo equivalente.

La utilización de sellos de tiempo prevendrá de la posibilidad de repudio posterior. Los casos en los que se debe aplicar un sello de tiempo a la actuación administrativa son:

- Cuando lo establezca una norma de rango legal o reglamentaria.
- Cuando así esté definido para el procedimiento administrativo de que se trate.
- Cuando el sistema afectado esté clasificado como de nivel alto según el Esquema Nacional de Seguridad.

4.5 PLATAFORMAS Y SISTEMAS DE INFORMACIÓN

Para la creación y validación de firmas se recomienda el uso de los servicios publicados en el Catálogo de Servicios de Administración Digital (@firma), así como la Plataforma de Sellado de Tiempos @TSA. Los sistemas de información que se integren o vayan integrarse con las plataformas y sistemas del Ayuntamiento y usen firma electrónica deberán integrarse con el módulo Común de Firma Digital en su versión más actualizada. Todos los sistemas integrados firmarán la totalidad de sus documentos con política de firma por defecto. Las aplicaciones microinformáticas y otras herramientas de escritorio, incluyendo el correo electrónico, aplicaciones ofimáticas y navegadores de Internet, entre otros, deberán tener instalados los certificados de las autoridades de certificación admitidas en la Administración Municipal y estar configurados, en la medida de sus posibilidades, para el cumplimiento de lo relativo a la creación y validación de firmas electrónicas.

Firma 1 de 1	Judith Castro Gómez
26/11/2024	Concejal Económico, G Fondos Europeos y O AAPP

Para consultar la autenticidad de este documento consulte la siguiente página web

Código Seguro de Validación f789a173c47740b0ba709ad33f119dc3001

Url de validación <https://sede.aytopalencia.es/absis/idi/arx/idiarxabsaweb/castellano/asp/verificadorfirma.asp>

Metadatos Origen: Origen administración Estado de elaboración: Original



4.6 Condiciones para salvaguardar la validez de las firmas

El almacenamiento de los certificados y las informaciones de estado se asociarán al documento resultante de la firma electrónica y se procederá a sellar estos metadatos, aplicando como mínimo las modalidades de firmas AdES -X o -A.

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

Las plataformas de firma electrónica adoptadas en el ámbito de la Administración Municipal deberán disponer de mecanismos de resellado, para añadir, de forma periódica, un sello de fecha y hora de archivo utilizando un algoritmo robusto en el momento de ser firmado.

Los sistemas de información deberán contemplar las funcionalidades necesarias para garantizar la validez en el tiempo de los documentos firmados por el sistema hasta su archivo. Para ello se tendrá en cuenta lo establecido en la Política de gestión de documentos y el Esquema Nacional de Interoperabilidad para la transferencia de documentos y expedientes al Sistema de Información del Ayuntamiento de Palencia.

Se almacenarán los documentos firmados con los formatos de firma mencionados en la presente Política.

El Ayuntamiento de Palencia establecerá los criterios de archivo y custodia aplicable a los documentos, con independencia de su formato electrónico o físico.

El Sistema corporativo de Gestión e Información de Archivos deberá aplicar las medidas de seguridad que garanticen en el tiempo la validez de las firmas y los certificados de los documentos archivados y custodiados.

El tratamiento de los documentos y sus firmas podrán ser auditados en el marco del cumplimiento del Esquema Nacional de Seguridad.

Cada usuario se le informará de la posibilidad de disponer de una copia de seguridad de su certificado, ubicada en su cuenta de correo electrónico corporativo. Cada certificado estará protegido con mecanismos de autenticación seguros. Cada usuario dispondrá e instalará su Certificado Digital, y si fuera necesario, seguirá las indicaciones y recomendaciones del Departamento de Innovación y Nuevas Tecnologías. Se les informará a los usuarios las condiciones de uso del certificado.

Firma 1 de 1	Judith Castro Gómez
26/11/2024	Concejal Económico, G Fondos Europeos y O AAPP

Para consultar la autenticidad de este documento consulte la siguiente página web

Código Seguro de Validación f789a173c47740b0ba709ad33f119dc3001

Url de validación <https://sede.aytopalencia.es/absis/idi/arx/idiarxabsaweb/castellano/asp/verificadorfirma.asp>

Metadatos Origen: Origen administración Estado de elaboración: Original

