	Política de Firma Electrónica	Identificador: 17-mp.info.6
		Versión: 00
		Fecha: 04/02/19
		Página 1 de 8

1. INFORMACIÓN DEL DOCUMENTO

FECHA	VERSIÓN	DESCRIPCIÓN DE CAMBIOS
04/02/19	00	Versión inicial documento

Control de versiones de Política de Firma Electrónica

VERSIÓN	CLASIFICACIÓN DEL DOCUMENTO	ELABORADO POR	REVISADO POR	APROBADO POR
00	Interno	Responsable de Seguridad	Comité de Seguridad	Comité de Seguridad
		Firma:	Firma:	Firma:
		Fecha:	Fecha:	Fecha:

Estado de Política de Firma Electrónica

ÍNDICE

1. INFORMACIÓN DEL DOCUMENTO	1
ÍNDICE.....	2
2. INTRODUCCIÓN	3
3. OBJETIVO.....	3
4. ALCANCE	4
5. EFECTOS	4
6. NORMAS PARTICULARES POLÍTICA DE FIRMA ELECTRÓNICA	4
4.1 CERTIFICADOS ADMITIDOS	5
4.2 TIPOS DE CERTIFICADOS.....	5
4.3 CERTIFICADOS DE EMPLEADO PÚBLICO AL SERVICIO DE LA ADMINISTRACIÓN	5
4.4 CERTIFICADOS DE SEDE	6
4.5 CERTIFICADOS DE SELLO ELECTRÓNICO	6
4.6 SELLOS DE TIEMPO	6
4.7 PLATAFORMAS Y SISTEMAS DE INFORMACIÓN.....	7
4.8 CONDICIONES PARA SALVAGUARDAR LA VALIDEZ DE LAS FIRMAS.....	7

2. 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 Siero, 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 Siero.

Para dar cumplimiento al mp.info.4 Firma Electrónica del 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 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 aquélla soporte.
- Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación: Certificados; Datos de verificación y validación.

3. OBJETIVO

Aprobar la Política de firma electrónica y certificados del Ayuntamiento de Siero recogidas en el presente documento.

4. ALCANCE

Esta Política se aplicará a los sistemas de información del Ayuntamiento de Siero y sus organismos autónomos, 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 Siero, 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.

En adelante, cuando se haga referencia al Ayuntamiento de Siero, se entenderán incluidos sus organismos autónomos.

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

- a) Las relaciones electrónicas del Ayuntamiento de Siero con los ciudadanos y proveedores en todos los servicios y procedimientos puestos a su disposición en la respectiva sede electrónica 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.

- b) Las relaciones electrónicas entre los distintos órganos y empleados del Ayuntamiento.
- c) Las relaciones electrónicas del Ayuntamiento de Siero con el resto de Administraciones y entidades públicas.

5. EFECTOS

La presente Política surtirá efectos a partir del día siguiente al de su publicación en el Boletín Oficial del Principado de Asturias.

6. NORMAS PARTICULARES POLÍTICA DE FIRMA ELECTRÓNICA

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

- Certificados admitidos.
- Tipos de certificados.
- Certificados de empleado público.
- Certificados de sede.
- Certificados de sello electrónico.

- Certificados de organismos, empresas y entes públicos.
- 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 Siero 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), 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 del Ayuntamiento de Siero 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 AL SERVICIO DE LA ADMINISTRACIÓN

Las solicitudes de certificados de empleado público para la Administración Municipal se gestionarán a través del DEPARTAMENTO TIC 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 Unidad que vaya a necesitar el uso de certificado digital facilitando la información que proceda en cada caso a requerimiento del Departamento TIC.

El Departamento TIC será responsable de los certificados que adquiera, gestione y custodie de forma centralizada, con el objetivo de controlar de forma exhaustiva su uso.

	Política de Firma Electrónica	Identificador: 17-mp.info.6
		Versión: 00
		Fecha: 04/02/19
		Página 6 de 8

4.4 CERTIFICADOS DE SEDE

En la Administración Municipal los certificados de sede electrónica sólo podrán utilizarse para la identificación de las respectivas sedes electrónicas. De esta forma, queda prohibido su uso para la firma de contenido de documentos electrónicos.

Para la correcta identificación de la sede electrónica, el certificado deberá hacer referencia al nombre del dominio: ayto-siero.es.

4.5 CERTIFICADOS DE SELLO ELECTRÓNICO


Los certificados de sello electrónico se utilizarán exclusivamente para la actuación administrativa automatizada definida en la normativa vigente. La creación de sellos electrónicos se realizará mediante resolución del órgano responsable de su utilización y se publicará en la sede electrónica. Las solicitudes de certificado de sello electrónico deberán remitirse al Departamento TIC que será la encargada de gestionarlas y coordinar la tramitación con el proveedor del certificado. La solicitud deberá incluir el órgano o entidad titular del certificado de sello, el nombre de la persona titular del mismo, los motivos de la petición, el uso previsto y la propuesta de la resolución de creación, debiendo estar firmada por el órgano competente. El Departamento TIC será responsable de los certificados que adquiera, gestione y custodie de forma centralizada. Se podrán autorizar excepciones a la adquisición, gestión y custodia centralizada cuando existan razones económicas, técnicas u organizativas que así lo aconsejen. En estos casos, Departamento TIC puede asesorar en la fase de adquisición. Para nuevos usos de los certificados de sello electrónico aprobados en actuaciones administrativas automatizadas deberán enviar a Departamento TIC la solicitud aprobada por el órgano competente, indicando la actuación específica que se realizará, sus principales características así como la propuesta de modificación de la resolución que afecta al sello y que contempla los nuevos usos.

El órgano competente titular del certificado es responsable de informar al Departamento TIC la necesidad de renovación o revocación de sus certificados. A partir de esa comunicación el Departamento TIC procederá a gestionar con la entidad certificadora su renovación o revocación. En caso de cese de la persona física titular de un sello electrónico, el Departamento TIC contactará con el responsable del órgano afectado para determinar el titular del nuevo sello electrónico de órgano, o, si procede, vincular el sello al órgano.

4.6 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

	Política de Firma Electrónica	Identificador: 17-mp.info.6
		Versión: 00
		Fecha: 04/02/19
		Página 7 de 8

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 Siero 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 Siero 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.

4.7 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 (entre ellos, @firma, Valide), 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.

4.8 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.

	Política de Firma Electrónica	Identificador: 17-mp.info.6
		Versión: 00
		Fecha: 04/02/19
		Página 8 de 8

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 CADES, 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 Siero.
- Se almacenarán los documentos firmados con los formatos de firma mencionados en la presente Política.
- El Ayuntamiento 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.
- Los certificados están almacenados en un repositorio custodiado por el Departamento TIC. Cada certificado estará protegido con mecanismos de autenticación seguros. Los certificados se despliegan a los usuarios a través de una directiva del dominio del Ayuntamiento (instalándolos en el navegador de Internet como no exportables) Se les facilitará a los usuarios las condiciones de uso del certificado.
- Todo documento que salga del entorno seguro de administración de documentos, para que se mantenga su validez jurídica en el tiempo, se proveerá de una firma electrónica, como mínimo, en formato AdES-T con política de firma con carácter de copia auténtica del original.