



I. PRINCIPADO DE ASTURIAS

• OTRAS DISPOSICIONES

CONSEJERÍA DE EMPLEO, INDUSTRIA Y TURISMO

RESOLUCIÓN de 10 de noviembre de 2016, de la Consejería de Empleo, Industria y Turismo, por la que se aprueba la política de firma electrónica y certificados del Principado de Asturias.

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, 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".

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.

Adicionalmente, el artículo 18 establece que la Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para la autenticación y el reconocimiento mutuo de firmas electrónicas dentro de su ámbito de actuación, política que podrá ser utilizada como referencia por otras Administraciones Públicas para definir las políticas de certificados y firmas a reconocer dentro de sus ámbitos competenciales.

En desarrollo de dicha norma, con fecha 30 de mayo de 2012, la Comisión Permanente del Consejo Superior de Administración Electrónica aprobó la versión 1.9 de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y de sus organismos públicos (OID 2.16.724.1.3.1.1.2.1.9), publicándose en el Boletín Oficial del Estado de fecha 13 de diciembre de 2012.

En este contexto normativo, la Norma Técnica de Interoperabilidad de Política de firma Electrónica y de Certificados de la Administración, en su sección II.5 sobre interacción con otras políticas, establece que "cada organización valorará la necesidad y conveniencia de desarrollar una política propia frente a la posibilidad de utilizar una política marco existente".

Examinada la Política de Firma Electrónica y de Certificados de la Administración General del Estado, se considera que es coherente con el ordenamiento autonómico y plenamente asumible en sus aspectos técnicos, por lo que, con su adopción, la Administración del Principado de Asturias pretende dar un paso claro para favorecer la interoperabilidad entre Administraciones Públicas. Ello redundará de manera inmediata en la simplificación y racionalización de trámites para todos los sujetos que están obligados a relacionarse electrónicamente con la Administración así como para las personas físicas que elijan comunicarse con las Administraciones Públicas de esta forma.

En cuanto a la competencia para la aprobación de esta política del Principado de Asturias, 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 Principado de Asturias que fue aprobada por Resolución de 19 de septiembre de 2014 del Consejero de Economía y Empleo. Por ello, la Consejería que tiene atribuidas las competencias en materia de seguridad de los sistemas de información es la competente para aprobar esta política por aplicación del Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, que establece cuáles son los órganos competentes para aprobar normas en materia de seguridad de sistemas de información. Así, su artículo 11 atribuye la facultad para aprobar la Política de Seguridad a los órganos superiores, entendiéndose por tales los responsables directos de la ejecución de la acción del gobierno, central, autonómico o local, en un sector de actividad específico de acuerdo con las normas de organización de cada Administración.

Conforme a la atribución de competencias efectuada por el Decreto 6/2015, de 28 de julio, del Presidente del Principado de Asturias, de reestructuración de las Consejerías que integran la Administración de la Comunidad Autónoma, corresponden a esta Consejería las competencias en materia de gestión centralizada de los servicios informáticos y de comunicación de la Administración del Principado.

En consecuencia con lo expuesto, de conformidad con lo establecido en el artículo 38 de la Ley del Principado de Asturias 6/1984, de 5 de julio, del Presidente y del Consejo de Gobierno y el artículo 21 de la Ley del Principado de Asturias 2/1995, de 13 de marzo, sobre Régimen Jurídico de la Administración, por la presente



RESUELVO

Primero.—Aprobación de la Política de firma electrónica y certificados de la Administración del Principado de Asturias.

1. Aprobar la Política de firma electrónica y de certificados de la Administración del Principado de Asturias, adoptando la Política de Firma Electrónica y de Certificados de la Administración General del Estado (OID 2.16.724.1.3.1.1.2.1.9).
2. Aprobar las Reglas particulares de la Política de firma electrónica y certificados de la Administración del Principado de Asturias recogidas en el anexo a esta resolución.

Segundo.—Ámbito de aplicación.

1. La política de firma aprobada será de aplicación, en el ámbito competencial de la Administración del Principado de Asturias, a los siguientes casos:

- a) Las relaciones electrónicas de la Administración del Principado de Asturias 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 de la Administración del Principado de Asturias siempre que se permita o sea de obligación por aplicación de cualquier norma sectorial.
- c) Las relaciones electrónicas de la Administración del Principado de Asturias con el resto de Administraciones y entidades públicas.

2. La firma electrónica realizada en el ámbito de historia clínica y receta electrónica deberá atender a la normativa y requisitos que se establezcan en las disposiciones de interoperabilidad nacionales y europeas en el ámbito sanitario.

3. Los organismos, empresas y entes públicos que integran el sector público autonómico de acuerdo con el artículo 4 del Texto refundido del régimen económico y presupuestario del Principado de Asturias, podrán solicitar a través de la Dirección General competente en materia de tecnologías de la información y las comunicaciones, su adhesión a la política de firma que se regula en esta resolución.

Para garantizar la interoperabilidad de los sistemas de información y las relaciones electrónicas entre la Administración del Principado de Asturias y los organismos, empresas y entes públicos que integran el sector público autonómico, las normas o reglas específicas relativas a la firma electrónica que se puedan aprobar por los citados organismos deberán ser compatibles con la presente política de firma.

Tercero.—Atribuciones de la Dirección General competente en materia de tecnologías de la información y las comunicaciones.

1. La Dirección General competente en materia de tecnologías de la información y las comunicaciones adoptará las medidas y dictará las instrucciones necesarias para el desarrollo, ejecución y aplicación de la Política de firma electrónica y certificados de la Administración del Principado de Asturias.

2. El mantenimiento, actualización y publicación electrónica de la Política de firma electrónica y certificados de la Administración del Principado de Asturias corresponderá a la citada Dirección General.

Cuarto.—Adaptación de los sistemas existentes.

Los sistemas de información existentes que requieran adaptaciones específicas dispondrán de un plazo de tres meses para efectuarlas y dar cumplimiento a lo dispuesto en esta resolución.

Quinto.—Efectos

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

En Oviedo, a 10 de noviembre de 2016.—El Consejero de Empleo, Industria y Turismo, Francisco Blanco Ángel.—Cód. 2016-12081.

Anexo

REGLAS PARTICULARES DE LA POLÍTICA DE FIRMA ELECTRÓNICA Y CERTIFICADOS DE LA ADMINISTRACIÓN DEL PRINCIPADO DE ASTURIAS

ÍNDICE

1. Certificados admitidos.
2. Tipos de certificados.
3. Certificados de empleado público.
4. Certificados de sede.



5. Certificados de sello electrónico.
6. Certificados de organismos, empresas y entes públicos.
7. Sellos de tiempo.
8. Condiciones para salvaguardar la validez de las firmas.
9. Plataformas y sistemas de información.

1. Certificados admitidos.

En general, se admitirán los certificados incluidos en la relación de proveedores y certificados admitidos por la plataforma @firma. En particular, la relación de prestadores y certificados admitidos en el ámbito de la Administración del Principado de Asturias se encuentra publicada en la sede electrónica del Principado de Asturias (<https://sede.asturias.es/>)

Excepcionalmente y dependiendo del proceso administrativo afectado, pueden darse condiciones en las que se acepten o no ciertos prestadores o certificados.

2. Tipos de certificados.

Se definen las instrucciones de uso general de las distintas tipologías de certificados, en uso de la facultad otorgada a la Administración del Principado de Asturias 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 Principado de Asturias deberán aceptar y adaptarse a los nuevos tipos de certificados, ya que es posible que reciban certificados con las nuevas clasificaciones. Dicha adaptación deberá ser valorada por cada servicio y su aplicación se ajustará a la normativa de aplicación a este anexo.

3. Certificados de empleado público.

Las solicitudes de certificados de empleado público para las Consejerías del Principado de Asturias que fueran a gestionarse a través de la Dirección General competente en materia de tecnologías de la información y las comunicaciones (en adelante DGTIC) deberán remitirse a la citada Dirección General que será la encargada de recibir la solicitud y 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.

Las Secretarías Generales Técnicas serán las encargadas de la solicitud de nuevos certificados, y de la petición de su renovación o revocación. Estas solicitudes se dirigirán a la DGTIC. Esta obligación deberá tenerse en cuenta especialmente durante los procesos de ceses y nombramientos de altos cargos vinculados a las modificaciones de las estructuras orgánicas, puesto que en los certificados de este personal figura su cargo. Se deberá facilitar la lista de personal de cada Consejería que vaya a necesitar el uso de certificado digital facilitando la información que proceda en cada caso a requerimiento de la DGTIC.

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

4. Certificados de sede.

En la Administración del Principado de Asturias 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: (*.asturias.es)

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 para las Consejerías del Principado de Asturias deberán remitirse a la DGTIC 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.

La DGTIC 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, la DGTIC puede asesorar en la fase de adquisición.

Para nuevos usos de los certificados de sello electrónico aprobados en actuaciones administrativas automatizadas dentro del ámbito de las Consejerías, las Secretarías Generales Técnicas deberán enviar a la DGTIC 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 a la DGTIC de la necesidad de renovación o revocación de sus certificados. A partir de esa comunicación la DGTIC procederá a gestionar con la entidad certificadora su renovación o revocación.

En caso de cese de la persona física titular de un sello electrónico, la Secretaría General Técnica competente deberá contactar con el responsable del órgano afectado para determinar el titular del nuevo sello electrónico de órgano, o, si procede, vincular el sello al órgano.

6. Certificados de organismos, empresas y entes públicos del sector público.

La DGTIC gestionará las solicitudes de certificados efectuadas por los organismos, empresas y entes públicos. Se aplicarán las normas señaladas en este anexo para la tramitación de la adquisición de los distintos tipos de certificado, su renovación y revocación.

La DGTIC será responsable de los certificados que adquiera, gestione y custodie de forma centralizada para estos organismos y entidades. 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, la DGTIC puede asesorar en la fase de adquisición.

7. Sellos de tiempo.

La Administración del Principado de Asturias 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 en la Administración del Principado de Asturias 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.

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.

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.

- Se utilizará como mínimo AdES-X para aquellos documentos y expedientes cuyo calendario de conservación establezca una eliminación de los mismos igual o menor de 5 años.
- Se utilizará la modalidad de firma AdES-A para el resto de documentos. Esta permite la adición de sellos de tiempo periódicos para garantizar la integridad de la firma archivada o guardada para futuras verificaciones (A de Archivo).
- Se debe utilizar PAdES-LTV, formato de firma longeva, para documentos en PDF. Este perfil permite prorrogar por tiempo indefinido la validez de las firmas en formato PDF.

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 del Principado de Asturias 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 del Interoperabilidad para la transferencia de documentos y expedientes al Sistema de Información y Gestión de Archivos del Principado de Asturias.
- Se almacenarán los documentos firmados con los formatos de firma mencionados en el presente anexo.
- La Política de Gestión de Documentos del Principado de Asturias 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 (SIGIA) 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. Con respecto a las firmas vinculadas a aquellos documentos y expedientes cuyo calendario de conservación



implique la obligatoriedad de su conservación por un período superior a 5 años o aquel que determine la Política de Gestión de Documentos de la Administración del Principado de Asturias, deberán aplicar mecanismos de resellado y formatos de firmas longevas, acordes con la presentes instrucciones.

- El tratamiento de los documentos y sus firmas podrán ser auditados en el marco del cumplimiento del Esquema Nacional de Seguridad.
- La administración de los certificados y las informaciones de estado se realizará en un depósito específico en el entorno de gestión de documentos, debidamente relacionados. Se incluirán metadatos específicos adecuados a la fase de conservación en que se encuentren. Asimismo, podrán producirse procesos de conversión o migración de formatos de documentos para preservar su longevidad.
- 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.

9. 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 de la DGTIC 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 del Principado de Asturias y estar configurados, en la medida de sus posibilidades, para el cumplimiento de lo relativo a la creación y validación de firmas electrónicas.