I. COMUNIDAD DE MADRID

C) Otras Disposiciones

Consejería de Presidencia, Justicia y Portavocía del Gobierno

19 *RESOLUCIÓN de 12 de marzo de 2018, de la Dirección General de Calidad de los Servicios y Atención al Ciudadano, por la que se establecen las condiciones de uso de firma electrónica no criptográfica, en las relaciones de los interesados con los órganos de la Administración de la Comunidad de Madrid, sus Organismos Públicos y Entidades de Derecho Público.*

El artículo 10.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, enumera los sistemas válidos a efectos de firma, que los interesados podrán utilizar para relacionarse con las Administraciones Públicas. Estos sistemas, sea cual sea el utilizado, deben permitir acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados, así como la integridad e inalterabilidad del documento.

El citado precepto se refiere expresamente, en sus dos primeras letras, a los sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos reconocidos o cualificados de firma electrónica, a los sistemas de sello electrónico reconocido o cualificado y de sello electrónico avanzado basados en certificados electrónicos reconocidos o cualificados de sello electrónico. Pero además, en su letra c) se refiere a cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan.

Además, el artículo 10.3 de la Ley permite, si así lo dispone la normativa reguladora aplicable, la posibilidad de admitir los sistemas de identificación contemplados en esta Ley (artículo 9) como sistemas de firma, cuando permitan acreditar la autenticidad de la expresión de voluntad y consentimiento de los interesados.

El artículo 11 de la Ley, por su lado, regula el uso de los medios de identificación y firma en el procedimiento administrativo estableciendo que, con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo solo será necesario identificarse, limitando la obligatoriedad de la firma para los supuestos previstos en el apartado segundo del artículo: formular solicitudes, presentar declaraciones responsables o comunicaciones, interponer recursos, desistir de acciones y renunciar a derechos.

En este contexto legal, se debe señalar que la Comunidad de Madrid firmó el 30 de noviembre de 2014 un convenio con el Estado (MINHAP) para un aprovechamiento común de las soluciones tecnológicas básicas de administración electrónica. Uno de los servicios incluidos en dicho Convenio es Cl@ve firma, un sistema orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos, cuyo objetivo principal es que el interesado pueda identificarse ante la Administración mediante claves concertadas (usuario más contraseña), sin tener que recordar claves diferentes para acceder a los distintos servicios. Este sistema permite además la firma de documentos electrónicos, pero para ello el ciudadano tiene que realizar el proceso de emisión de un certificado electrónico centralizado, generando una identidad y contraseña que le permita acceder al mismo cada vez que ello sea necesario.

La evolución de los sistemas de firma que ofrece la Secretaría General de Administración General, dependiente de la Secretaría de Estado de Función Pública añade ahora otra prestación, dirigida a superar determinadas limitaciones del sistema de firma criptográfica, ofreciendo a los interesados la posibilidad de relacionarse electrónicamente con la administración sin la necesidad de que esa firma se encuentre basada en certificado electrónico alguno, mediante un sistema de medidas de seguridad, trazabilidad e integridad que garanticen la legalidad de los procedimientos que hagan uso de él.

Es necesario, por lo tanto, establecer los criterios de uso y las condiciones técnicas de implementación de los sistemas de firma electrónica no criptográfica, en aplicación del artículo 10.2.c) de la Ley 39/2015, de 1 de octubre, que se considerarán válidos a efectos de firma en la Administración de la Comunidad de Madrid, sus organismos públicos y entidades de derecho público.

BOCM-20180320-19

El artículo 14.1 del Decreto 130/2017, de 31 de octubre, del Consejo de Gobierno, por el que se establece la estructura orgánica de la Consejería de Presidencia, Justicia y Portavocía del Gobierno, atribuye a esta Dirección General las competencias en materia de administración electrónica. Específicamente, en la letra c) se atribuye la competencia para "fomentar el uso de las herramientas de administración electrónica por los empleados de la Comunidad de Madrid, extender su conocimiento y determinar un común denominador de uso" y en la letra e) la de "promover nuevos canales de acceso e identificación para el uso y fomento de la administración electrónica por parte de los ciudadanos".

Por lo tanto, y en virtud de lo anterior,

RESUELVO

Primero

Aprobación y publicación

1. Aprobar los términos y condiciones de uso de firma electrónica no criptográfica en las relaciones de los interesados con los órganos de la Comunidad de Madrid, sus organismos públicos y entidades de derecho público, de acuerdo con lo establecido en el artículo 10.2 de la Ley 39/2015, de 1 de octubre.
2. Ordenar su publicación en el BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID.

Segundo

Efectividad

La presente Resolución producirá efectos a partir del día siguiente a su publicación en el BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID.

Madrid, a 12 de marzo de 2018.—La Directora General de Calidad de los Servicios y Atención al Ciudadano, PS (Resolución 28 de septiembre de 2017), la Viceconsejera de Presidencia y Justicia, Isabel Díaz Ayuso.

ANEXO

TÉRMINOS Y CONDICIONES DE USO DE LA FIRMA ELECTRÓNICA NO CRIPTOGRÁFICA EN LAS RELACIONES DE LOS INTERESADOS CON LOS ÓRGANOS ADMINISTRATIVOS DE LA ADMINISTRACIÓN DE LA COMUNIDAD DE MADRID, SUS ORGANISMOS PÚBLICOS Y ENTIDADES DE DERECHO PÚBLICO

I. *Objeto*

Los presentes términos y condiciones tienen como objeto determinar las circunstancias en las que un sistema de firma electrónica no basado en certificados electrónicos será considerado como válido en las relaciones de los interesados con los órganos administrativos de la Administración de la Comunidad de Madrid, sus organismos públicos, y entidades de derecho público, de acuerdo con el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre. Sin perjuicio, de otros sistemas de firma implantados, de acuerdo con el artículo 10.2.c) y 10.3 y que ofrezcan las garantías de seguridad suficientes para gestionar la integridad y el no repudio, según el principio de proporcionalidad recogido en el artículo 13.3, Gestión de Riesgos del Seguridad del Esquema Nacional de Seguridad.

II. *Ámbito de aplicación*

Los presentes términos y condiciones serán de aplicación a los órganos administrativos de la Comunidad de Madrid y organismos públicos y entidades de Derecho Público vinculados o dependientes, que dispongan nuevos sistemas de firma electrónica que no requieran certificado electrónico de los interesados, y sin perjuicio de la posibilidad de utilización en tales trámites de los sistemas de firma contemplados en el artículo 10.2.a) de la Ley 39/2015, de 1 de octubre.

BOCM-20180320-19

III. *Criterios para la utilización de sistemas de firma electrónica que no requieran certificado electrónico del interesado*

El esquema nacional de seguridad (en adelante ENS), regulado por el Real Decreto 3/2010, de 8 de enero, y modificado por Real Decreto 951/2015, de 23 de octubre, de modificación 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 constituye el marco legal que permite definir y establecer las medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los interesados y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

En la implantación de un sistema de firma electrónica que no utilice el certificado electrónico del interesado se deberá cumplir con el ENS para garantizar la seguridad de los datos y los servicios, como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.

El ENS establece la necesidad de categorizar los sistemas de información, siendo la categoría de un sistema de información, en materia de seguridad, la que permite modular el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

En aplicación de esta resolución, se podrán utilizar los referidos sistemas de firma cuando el sistema de información asociado al procedimiento haya sido categorizado, según el esquema nacional de seguridad, de categoría básica y aquellos de categoría media en los que se posibilite el uso de la firma no criptográfica.

IV. *Garantía de funcionamiento*

Cuando la actuación realizada por el interesado, en su relación con la Administración, implique la presentación de documentos a través de servicios electrónicos utilizando los sistemas de firma electrónica regulados en la presente redacción, se garantizará la integridad de la información presentada mediante el sellado realizado con el sello electrónico cualificado o reconocido del organismo competente, a la que se añadirá un sello de tiempo realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado, y su incorporación inmediata al sistema de información asociado a dicho procedimiento. El organismo deberá disponer de las medidas técnicas, organizativas y procedimentales necesarias para garantizar dicha integridad a lo largo del tiempo.

Asimismo, se garantizará también la integridad de la expresión de la voluntad y consentimiento del interesado, y con ésta la garantía del no repudio de la actuación de firma, mediante el sellado realizado con el sello electrónico cualificado o reconocido del organismo y la adición de un sello de tiempo realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado, de las evidencias de la autenticación del interesado que realiza el acto de la firma, así como del consentimiento explícito de aquel con el contenido firmado, almacenando dichas evidencias junto con la información presentada.

Se completará la garantía de la actuación de firma con la emisión por el Órgano competente de un justificante de firma sellado con su sello electrónico de órgano y generando el código seguro de verificación o CSV, que será el documento con valor probatorio de la actuación realizada, cuya integridad podrá comprobarse mediante consulta del documento electrónico original a través del servicio electrónico de Verificación de Documentos Electrónicos de la Comunidad de Madrid, en tanto no se acuerde la destrucción de dichos documentos con arreglo a la normativa que resulte de aplicación o por decisión judicial.

V. *Acreditación de la identidad y de la autenticidad de la expresión de la voluntad y consentimiento del interesado*

Para acreditar la identidad del interesado, en todo caso, se deberán utilizar medios de identificación que garanticen niveles de seguridad sustancial o alto, conforme a definición de estos niveles en el Reglamento número 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica.

Para acreditar la autenticidad de la expresión de la voluntad y consentimiento del interesado se requerirá:

BOCM-20180320-19

1. Verificación de la identidad del interesado a quien le corresponde el acto de la firma en el momento inmediatamente previo del propio acto, mediante una nueva autenticación o utilizando mecanismos de contraste de garanticen la verificación.

2. La verificación previa por parte del interesado de los datos a firmar.

Estos datos se obtendrán a partir de aquella información presentada por el ciudadano y de cuya veracidad se hace responsable, así como de los documentos electrónicos que, eventualmente, presente en el procedimiento.

El interesado debe ser consciente de los datos que va a firmar y deberá ofrecérsele de un modo visible la posibilidad de consultarlos en un formato legible.

3. La acción explícita por parte del interesado de manifestación de consentimiento y expresión de su voluntad de firma.

Se deberá requerir la expresión explícita del consentimiento y la voluntad de firma del interesado en el procedimiento, mediante la inclusión de frases que manifiesten dicha expresión de manera inequívoca, además de la exigencia de actuación de aceptación por parte del interesado.

4. Para garantizar el no repudio de la firma por parte del ciudadano, el sistema de firma deberá acreditar la vinculación de la expresión de la voluntad y los datos firmados con la misma persona.

Se deberán considerar mecanismos que permitan contrastar la identidad del interesado en el momento mismo de proceder a la firma, no autorizando la realización de ésta ante cualquier situación que cuestione dicho contraste.

Asimismo, la garantía de no repudio exige que el sistema de firma asegure una adecuada trazabilidad que permita la auditoría de la actuación realizada – autenticación, expresión de voluntad y consentimiento y actuación de firma.

Con el mismo propósito de auditoría para asegurar la garantía de no repudio, los proveedores de identificación deberán salvaguardar las evidencias de las actuaciones de autenticación durante el plazo mínimo de cinco años. Corresponderá al sistema de firma la custodia de las referencias a tales evidencias, y la solicitud de las mismas, conforme al procedimiento y condiciones establecidas, a aquellos proveedores, si fuere necesario.

VI. *Garantía de la integridad de los datos y documentos firmados*

1. Sellado de la información presentada. Una vez acreditada la expresión de la voluntad y el consentimiento y para firmar del interesado, se deberán establecer los mecanismos para garantizar la integridad e inalterabilidad de los datos y, en su caso, de los documentos electrónicos presentados por el interesado, para lo cual el sistema de firma sellará los datos a firmar, con un sello de órgano y la adición de un sello de tiempo realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado, y la pondrá a disposición del sistema de información asociado al procedimiento electrónico que requiere la firma.

2. Justificante de firma. En el proceso de firma se entregará al interesado un justificante de firma, que será un documento legible, de acuerdo con la norma técnica de interoperabilidad de catálogo de estándares y preferiblemente en formato PDF y que deberá cumplir estos requisitos:

— Garantizar la autenticidad del organismo emisor mediante un sellado electrónico con el certificado de sello del mismo, en formato PAdES en el caso de que el justificante tenga el formato PDF.
— Contener los datos del firmante, entre los que se incluirán datos de la evidencia de la autenticación, y, en el caso de que el documento firmado haya pasado por un Registro de entrada, los datos identificativos de su inscripción en el Registro.
— Contener los datos a firmar expresamente por el interesado. Si se ha anexado algún documento electrónico se incluirá una referencia al mismo.
— Garantizar el instante en que se realizó la firma, mediante sello de tiempo del justificante, realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado.
— Garantizar la autenticidad del justificante de firma, incluyendo en el justificante de firma un código seguro de verificación (CSV), y garantizando que este justificante se pueda consultar en línea mediante un sistema de cotejo de CSV cuya dirección se incluya en el propio justificante de firma.

BOCM-20180320-19

— Alternativamente, la autenticidad del organismo emisor y del justificante de firma se podrá garantizar mediante dos documentos: uno de ellos con sellado electrónico del justificante en formato PAdES (en el caso de que el justificante tenga formato PDF) y otro con la utilización de un código seguro de verificación (CSV) del justificante.

(03/9.982/18)

BOCM-20180320-19