I. DISPOSICIONES GENERALES

MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

8393 *Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital, por la que se establecen las condiciones de uso de firma electrónica no criptográfica, en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos.*

El artículo 10 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.

El citado precepto se refiere expresamente 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 y a cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan, recogiendo asimismo la posibilidad de admitir los sistemas de identificación contemplados en la Ley como sistemas de firma.

En cualquier caso, todos los sistemas de firma electrónica admitidos deberán garantizar el cumplimiento de los requisitos recogidos en el apartado primero del artículo 10 de la citada Ley. Esto es, que estos sistemas permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados, así como la integridad e inalterabilidad del documento.

A estos sistemas de firma electrónica han de reconocérsele efectos jurídicos y son conformes a lo establecido en el artículo 25.1 del Reglamento (UE) N o 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, sin menoscabo de lo recogido en el artículo 27 de la propia norma «Firmas electrónicas en servicios públicos».

El artículo 11 de la Ley 39/2015, de 1 de octubre 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 sólo será necesario identificarse, y 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. Esta importante novedad en la regulación aconseja establecer las cautelas mínimas que permitan normalizar el uso de estos sistemas evitando la heterogeneidad de su implementación técnica entre las Administraciones.

Así, y en aplicación de lo dispuesto en el artículo 10.3 de la Ley 39/2015, de 1 de octubre, que faculta a las Administraciones Públicas a admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados, siempre que así lo disponga la normativa reguladora, se procede con esta resolución a indicar los requisitos que se tienen que cumplir, no sólo con este objetivo, sino para asegurar también la integridad e inalterabilidad de los datos firmados, así como los requisitos para comprobar que se realizó dicho acto. Por lo tanto, se sientan las bases de uso de sistemas de identificación basados en la plataforma Cl@ve, para la realización de la firma, así como se

cve: BOE-A-2017-8393
Verificable en http://www.boe.es

establece una recomendación para recoger las evidencias de actos de relevancia jurídica, como las notificaciones, que si bien no necesitan firma, sí pueden necesitar unos requisitos de seguridad reforzados, manteniendo siempre el espíritu de la ley por el que no se haga en ningún caso más complejo para el ciudadano la recepción de la notificación o la realización de un trámite.

Es importante subrayar además, la complementariedad de esta resolución con el proyecto Cl@ve firma, que provee sencillos mecanismos para facilitar la firma electrónica criptográfica, de manera que se evitan los principales problemas, como la necesidad de disponer de hardware y/o software específico para realizar la firma en el ordenador del interesado, ya que toda esa complejidad queda resuelta por el sistema Cl@ve firma. Si bien este sistema es óptimo desde el punto de vista de uso de firma criptográfica, requiere que el ciudadano tenga activa la identificación por Cl@ve Permanente que le permite acceder a su certificado electrónico centralizado, en el caso de no tener activa esta identificación y siempre que el servicio lo permita esta nueva forma de firma no basada en certificado electrónico es una facilidad más para el ciudadano.

Por ello se ha tenido a bien el complementar este sistema de firma criptográfica sencilla para el ciudadano, con un sistema de medidas de seguridad, trazabilidad e integridad suficientes para los procedimientos que hagan uso de él, pero sin necesidad de recordar o tener activa una contraseña ni un certificado electrónico centralizado.

También resulta apropiado el uso de este sistema cuando, aun habiéndose utilizado un certificado electrónico en el proceso de identificación, no se quiera realizar una firma electrónica local con dicho certificado, para evitar los problemas de restricciones de compatibilidad de navegadores, máquinas virtuales Java y versiones de sistemas operativos.

Por tanto, el objeto de esta Resolución es establecer los criterios de uso y las condiciones técnicas de implementación de los sistemas de firma electrónica no criptográfica, previstos en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre, que se considerarán válidos a efectos de firma en la Administración General del Estado y sus organismos públicos, así como en aquellas otras Administraciones Públicas que adopten estos criterios y condiciones técnicas.

En virtud de lo anterior, y de acuerdo con el Real Decreto 424/2016, de 11 de noviembre, por el que se establece la estructura orgánica básica de los Departamentos ministeriales,

Esta Secretaría General de Administración Digital, en el ejercicio de las competencias atribuidas para la definición de estándares, de directrices técnicas y de gobierno TIC, de normas de seguridad y calidad tecnológicas y de la información a los que deberán ajustarse todas las Unidades de la Administración General del Estado y sus organismos públicos, dispone:

Primero.

1. Aprobar los términos y condiciones de uso de firma electrónica no criptográfica en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos, de acuerdo con el artículo 10.2 de la Ley 39/2015, de 1 de octubre, que se incluyen como anexo.
2. Ordenar su publicación en el «Boletín Oficial del Estado».

Segundo.

La presente Resolución entra en vigor a partir del día siguiente a su publicación en el «Boletín Oficial del Estado».

Madrid, 14 de julio de 2017.–El Secretario General de Administración Digital, Domingo Javier Molina Moscoso.

cve: BOE-A-2017-8393
Verificable en http://www.boe.es

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 General del Estado y sus organismos públicos

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 General del Estado y sus organismos públicos, 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 Administración General del Estado y organismos públicos y entidades de Derecho Público vinculados o dependientes, que habiliten nuevos sistemas de firma electrónica no criptográfica destinados a ser usados por los interesados en sus relaciones con los mismos, 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.

III. *Criterios para la utilización de sistemas de firma electrónica no criptográfica*

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 no criptográfica 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 norma, se podrán utilizar sistemas de firma electrónica no criptográfica 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 no sea necesario utilizar la firma avanzada, cuando así lo disponga la normativa reguladora aplicable.

IV. *Garantía de funcionamiento*

Cuando la actuación realizada por el interesado, en su relación con la Administración, implique la presentación en una sede electrónica de documentos electrónicos utilizando

cve: BOE-A-2017-8393
Verificable en http://www.boe.es

los sistemas de firma electrónica contemplados en la presente Resolución, se garantizará la integridad de la información presentada mediante el sellado realizado con el sello electrónico cualificado o reconocido del organismo competente para la gestión del procedimiento, 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, 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 necesarias para la verificación de la identidad, recopiladas inmediatamente antes del acto de la firma, así como, posteriormente, del consentimiento explícito del interesado con el contenido firmado, almacenando dichas evidencias en el sistema de información junto con la información presentada. La integridad y conservación de los documentos electrónicos almacenados y de sus metadatos asociados obligatorios quedará garantizada a través del sellado con el sello electrónico cualificado o reconocido del organismo y del resto de medidas técnicas que aseguren su inalterabilidad.

El organismo responsable del procedimiento emitirá 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. La integridad de los documentos electrónicos autenticados mediante CSV podrá comprobarse mediante el acceso directo y gratuito a la sede electrónica del organismo y en el punto de acceso general de la Administración General del Estado, 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 autenticidad de la expresión de la voluntad y consentimiento del interesado*

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

1. La autenticación del interesado, inmediatamente previa a la firma utilizando la plataforma Cl@ve, de identificación electrónica.
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.

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

V.1. Autenticación del interesado. La identificación y autenticación del interesado deberá hacerse, en todo caso, a través de la plataforma Cl@ve, sistema de identificación, autenticación y firma electrónica basado en claves concertadas, común para todo el sector público administrativo estatal, aprobado por Acuerdo de Consejo de Ministros de 19 de septiembre de 2014.

Dicha autenticación del interesado con el sistema Cl@ve, inmediatamente previa al acto de firma, deberá de hacerse con un nivel de calidad en la autenticación sustancial o alto.

V.2. Verificación previa de los datos a firmar. El interesado debe ser consciente de los datos que va a firmar y deberá ofrecérsele de un modo visible la posibilidad de consultarlo en un formato legible y, preferiblemente, con el mismo formato del documento que posteriormente se entregue al interesado como justificante de la firma.

V.3. Expresión del consentimiento y de la voluntad de firma de los interesados. Las aplicaciones que hagan uso de un sistema de firma, ajustado a los criterios de uso y

cve: BOE-A-2017-8393
Verificable en http://www.boe.es

condiciones técnicas de esta Resolución, deberán requerir de forma expresa la expresión del consentimiento y la voluntad de firma del interesado en el procedimiento, mediante la inclusión de frases que pongan aquéllos de manifiesto de manera inequívoca, y la exigencia de acciones explícitas de aceptación por parte del interesado (por ejemplo, mediante una casilla junto al texto «Declaro que son ciertos los datos a firmar/muestro mi conformidad con el contenido del documento y confirmo mi voluntad de firmar» que el interesado debe marcar, y un botón «Firmar y enviar» que debe pulsar para realizar la firma).

VI. *Garantía de no repudio*

VI.1. Garantías en el proceso de firma. 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. Para ello se volverá a solicitar la autenticación del ciudadano en el momento de proceder a la firma.

Asimismo, la garantía de no repudio exige que el sistema de firma asegure una adecuada trazabilidad en el caso de que sea necesario auditar una operación de firma en particular, para lo cual obtendrá, por cada firma y por tanto por cada proceso de autenticación, la siguiente información:

– Fecha y hora de la autenticación.
– Nombre y apellidos del interesado.
– NIF/NIE del interesado.
– Proveedor de identidad empleado (certificado electrónico, Cl@vePIN o Cl@vePermanente) y nivel de seguridad de identificación (sustancial o alto).
– Resultado de la autenticación (con éxito o fallida).
– Respuesta devuelta y firmada por la plataforma Cl@ve. Esta respuesta deberá incluir el campo opcional que contiene la respuesta devuelta y firmada por el Proveedor de Identificación.
– Fecha y hora de la firma.
– Resumen criptográfico de los datos firmados, con un algoritmo de hash que cumpla las especificaciones del esquema nacional de seguridad.
– Referencia al justificante de firma, mediante el CSV asociado a dicho justificante.
– Dirección IP origen desde la que se realizó la firma.

Esta información será sellada con un certificado electrónico cualificado o reconocido de sello del organismo, 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 será almacenada por el sistema de información asociado al procedimiento electrónico para el que se requiere la firma, como evidencia de la verificación de la identidad previa al acto de la firma, vinculada a los datos firmados.

En el caso de que los datos de identificación obtenidos en la autenticación inmediatamente anterior a la firma no coincidan con los datos de identificación obtenidos en autenticaciones previas, el sistema de firma no permitirá la realización de la misma, informando de esa eventualidad al sistema de información asociado al procedimiento electrónico que requiere dicha firma.

VI.2. Gestión de las evidencias de autenticación. A pesar de que el sistema de firma proporcionará a los sistemas de información asociados al procedimiento electrónico que requiere la firma la información relativa a la autenticación vinculada a dicha firma, en ocasiones puede ser necesario, por motivos de auditoría, recuperar las evidencias completas del proceso de autenticación.

Al utilizar el sistema Cl@ve como mecanismo de identificación y autenticación, las evidencias últimas no residen en el propio sistema de firma, sino en los sistemas de los proveedores de servicios de identificación integrados en Cl@ve.

Con objeto de que los proveedores de esos servicios de identificación puedan recuperar las evidencias necesarias para acreditar la realización de la identificación y

cve: BOE-A-2017-8393
Verificable en http://www.boe.es

autenticación previas ligadas a la realización de una firma en el sistema, se deberá facilitar a dichos proveedores la información de autenticación almacenada como evidencia de la verificación previa de la identidad en los sistemas de información asociados al procedimiento administrativo que requiere la firma, descrita en el apartado VI.1.

A tal efecto, los proveedores de servicios de identificación deberán salvaguardar dichas evidencias durante el plazo mínimo de cinco años. La solicitud de certificación de dichas evidencias se realizará conforme al procedimiento y las condiciones que se publicarán en el portal de Administración electrónica.

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

VII.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.

VII.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 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.

– 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.

cve: BOE-A-2017-8393
Verificable en http://www.boe.es