

I. DISPOSICIONES GENERALES

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

17170 *Resolución de 20 de octubre de 2022, de la Secretaría General de Administración Digital, por la que se modifica la de 14 de julio de 2017, 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.*

Por medio de la Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital, se establecen 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, del Procedimiento Administrativo Común de las Administraciones Públicas, 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. La relativa generalidad del artículo 10.2.c) en su redacción inicial aconsejaba establecer las cautelas mínimas que permitieran normalizar el uso de estos sistemas evitando la heterogeneidad de su implementación técnica entre las Administraciones.

Desde la fecha de la publicación de la resolución se han desarrollado numerosos sistemas de firma electrónica no criptográfica ajustados a sus condiciones por parte de órganos y organismos de la Administración General del Estado, así como de otras Administraciones Públicas que, aun no estando comprendidas en el ámbito de aplicación de la resolución previsto en el apartado II de su anexo, han aplicado sus previsiones voluntariamente.

El sistema definido en 2017 se basa en la identificación fehaciente del interesado y en la captura y almacenamiento de las evidencias que permitan acreditar aquella, así como la autenticidad de la expresión de la voluntad y consentimiento del interesado y la integridad e inalterabilidad de los datos firmados. En relación con la identificación del interesado, la resolución establece la utilización de la plataforma Cl@ve, con un nivel de calidad en la autenticación sustancial o alto. No obstante, esta condición ha supuesto una limitación en el uso de este sistema de firma electrónica no criptográfica, excluyendo al colectivo de usuarios registrados en Cl@ve con nivel básico.

Asimismo, desde el punto de vista normativo, en el periodo transcurrido desde 2017 han tenido lugar dos modificaciones del artículo 10 de la Ley 39/2015, de 1 de octubre. La primera modificación tuvo lugar por medio del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones y se desarrolló por medio del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, que desarrolla las previsiones en la materia tanto de la Ley 39/2015, de 1 de octubre, como de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. En el artículo 29 del Reglamento, en desarrollo del mencionado artículo 10 de la Ley 39/2015, de 1 de octubre, se regulan los sistemas de firma electrónica de las personas interesadas admitidos por las Administraciones Públicas y régimen de uso.

La segunda modificación del mencionado artículo 10 se ha llevado a cabo por medio de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, tras la cual, de acuerdo con la redacción del artículo 10.2.c) en vigor, en el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios

electrónicos, se considerarán válidos a efectos de firma, además de los sistemas previstos en los apartados a) y b) del artículo 10.2 (...) «cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todos los procedimientos en todos sus trámites, aun cuando adicionalmente se permita alguno de los previstos al amparo de lo dispuesto en la letra c)».

Asimismo, recientemente ha tenido lugar la aprobación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, cuyo artículo 40 establece que la categoría de seguridad de un sistema de información modulará el equilibrio entre la importancia de la información que maneja y 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; y que la determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I de dicho Real Decreto. Asimismo, el artículo 14 establece que cada organización que desarrolle e implante sistemas para el tratamiento de la información o la prestación de servicios realizará su propia gestión de riesgos por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema (para ello, sin perjuicio de lo dispuesto en el anexo II del Real Decreto, se empleará alguna metodología reconocida internacionalmente), concluyendo en su apartado 3 que las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Teniendo en cuenta estas consideraciones, con la modificación que ahora se introduce en la Resolución de 2017 se pretende ampliar genéricamente el uso de este sistema de firma no criptográfica a todos los usuarios registrados en CI@ve, siendo el órgano gestor del procedimiento el que, en función de la categorización de seguridad del sistema y en aplicación del principio de proporcionalidad previsto en el artículo 14.3 del Real Decreto 311/2022, de 3 de mayo, establezca el nivel mínimo de seguridad en la identificación necesario para admitir este sistema de firma en cada procedimiento concreto.

Por último, el Real Decreto-ley 18/2022, de 18 de octubre, por el que se aprueban medidas de refuerzo de la protección de los consumidores de energía y de contribución a la reducción del consumo de gas natural en aplicación del «Plan + seguridad para tu energía (+SE)», así como medidas en materia de retribuciones del personal al servicio del sector público y de protección de las personas trabajadoras agrarias eventuales afectadas por la sequía, introduce por medio de su disposición final tercera una nueva Disposición adicional octava en la Ley 39/2015, de 1 de octubre, que con el título «Resoluciones de Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital que establezcan las condiciones de uso de sistemas de identificación y/o firma no criptográfica» establece que «Cuando se trate de sistemas establecidos por medio de Resolución de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital para su ámbito competencial con objeto de 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, sus organismos públicos y entidades de Derecho Público vinculados o dependientes, no será preciso el transcurso del plazo de dos meses para la eficacia jurídica del sistema a que se refiere el artículo 10.2.c) de la presente ley, adquiriendo eficacia jurídica al día siguiente de la publicación de la Resolución, salvo que esta disponga otra cosa.»

En virtud de lo anterior, y de acuerdo con lo previsto en el artículo 9.2.k) del Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital,

Esta Secretaría General de Administración Digital, dispone:

Primero.

Modificar el anexo de la 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, en los términos que se indican a continuación:

Uno. El apartado I queda redactado como sigue:

«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 de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, de acuerdo con lo previsto en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas Sin perjuicio, de otros sistemas de firma implantados, de acuerdo con el artículo 10.2.c) y 10.4 y que ofrezcan las garantías de seguridad suficientes para gestionar la integridad y el no repudio, según el principio de proporcionalidad previsto en el artículo 14.3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.»

Dos. El apartado III queda redactado como sigue:

«III. Criterios para la utilización de sistemas de firma electrónica no criptográfica. El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, constituye el marco normativo 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 cumplirá con el Esquema Nacional de Seguridad 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.

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 electrónica avanzada, cuando así lo disponga la normativa reguladora aplicable.»

Tres. El párrafo V.1. del apartado V queda redactado como sigue:

«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 deberá ser inmediatamente previa al acto de firma.»

Cuatro. El apartado 1 del apartado VI queda redactado como sigue:

«VI.1 Garantías en el proceso de firma. Para garantizar el no repudio de la firma por parte del interesado firmante, 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 interesado 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 concreta, para lo cual conservará, por cada firma y, por tanto, por cada proceso de autenticación, la siguiente información:

- a) Fecha y hora de la autenticación.
- b) Nombre y apellidos del interesado.
- c) DNI/NIF/NIE del interesado.
- d) Sistema de identificación empleado (certificado electrónico, Cl@ve PIN o Cl@ve Permanente) y nivel de seguridad de identificación.
- e) Resultado exitoso de la autenticación.
- f) 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 servicios de Identificación.
- g) Fecha y hora de la firma.
- h) Resumen criptográfico de los datos firmados, con un algoritmo de hash que cumpla las especificaciones del esquema nacional de seguridad.
- i) Referencia al justificante de firma, mediante el CSV asociado a dicho justificante.

La información a que se refieren los párrafos anteriores será sellada con un certificado de sello electrónico, conforme al artículo 19 del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo. Adicionalmente, se añadirá un sello de tiempo realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado, y será almacenada, 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 o servicio electrónico que requiere dicha firma.»

Segundo.

Ordenar la publicación de esta Resolución en el «Boletín Oficial del Estado».

Tercero.

De acuerdo con la habilitación prevista en la disposición adicional octava de la Ley 39/2015, de 1 de octubre, la presente resolución entrará en vigor el día de su publicación en el «Boletín Oficial del Estado».

Madrid, 20 de octubre de 2022.—El Secretario General de Administración Digital,
Juan Jesús Torres Carbonell.