BASE DE DATOS DE Norma CEF.-
Referencia: NFL020733

RESOLUCIÓN de 26 de mayo de 2021, de la Secretaría General para la Innovación y Calidad del Servicio Público de Justicia, por la que se habilita a Cl@veJusticia y se establecen sus condiciones de uso, como mecanismo de identificación y firma de los interesados en las actuaciones realizadas mediante presencia telemática con los órganos judiciales y demás órganos pertenecientes a la Administración de Justicia.

(BOE de 31 de mayo de 2021)

EXPOSICIÓN DE MOTIVOS

La presente Resolución se dicta con el objeto de dotar de mayor seguridad jurídica a las actuaciones que se realicen mediante presencia telemática entre el interesado y los órganos judiciales o demás órganos pertenecientes a la Administración de Justicia, en base a lo señalado en el artículo 14 de la Ley 3/2020, de 18 de septiembre, de medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia.

I

La Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, recoge los aspectos necesarios para dar cumplimiento de la legislación procesal respecto en lo relativo al uso de las nuevas tecnologías; si bien, tras la reforma operada por la Ley 3/2020, de 18 de septiembre, se establece, en los artículos 4.2 f) y 6.2 d), dentro de los derechos de los ciudadanos y de los profesionales en relación con la utilización de los medios electrónicos en la actividad judicial, el de «utilizar los sistemas de identificación y firma establecidos en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas». Además, en concreto, en el caso de los profesionales, se hará «siempre que dicho sistema le identifique de forma unívoca como profesional para cualquier trámite electrónico con la Administración en los términos establecidos por las leyes procesales».

II

Asimismo, en el capítulo II del título III de la citada Ley 18/2011, en el apartado 2 del artículo 14, sobre las formas de identificación y autenticación establece que «sin perjuicio de lo dispuesto en los artículos 4 y 6 de la presente Ley y en todo caso, con sujeción estricta a lo dispuesto por las leyes procesales, los ciudadanos y profesionales del ámbito de la Justicia podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con la Administración de Justicia (…) c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen».

Al hilo de esto, el apartado 1 del artículo 23 de la señalada ley dispone que, «en los supuestos en que para la realización de cualquier actuación por medios electrónicos se requiera la identificación o autenticación del ciudadano mediante algún instrumento de los previstos en el artículo 14 de los que aquél no disponga, tal identificación o autenticación será válidamente realizada por un funcionario mediante el uso del sistema de firma electrónica del que esté dotado.»

III

A la vista de lo expuesto, se debe atender, por tanto, a lo dispuesto en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas que regulan, respectivamente, los sistemas de identificación de los interesados en el procedimiento y los sistemas de firma admitidos en las Administraciones Públicas y, que la Ley 18/2011, de 5 de julio, recoge en el ámbito de la Administración de Justicia.

El artículo 9 de la Ley 39/2015, de 1 de octubre, en su apartado 2, establece que «Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas siguientes:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".

b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".

c) Sistemas de clave concertada y cualquier otro sistema, que las Administraciones consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios».

Por otra parte, en el artículo 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se enumeran los sistemas válidos a efectos de firma, que los interesados podrán utilizar para relacionarse con las Administraciones Públicas.

Este 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.

IV

A estos sistemas de firma electrónica han de reconocérsele efectos jurídicos y ser 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».

Así, y en aplicación de lo dispuesto en la Ley 18/2011, de 5 de julio, que acoge los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, y, concretamente, el apartado 3 del artículo 10 que facultaría a la Administración de Justicia 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 validar la utilización del sistema Cl@veJusticia en las actuaciones con presencia telemática del interesado, indicando 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@veJusticia, para la identificación del interesado y, en los casos que se exija, la realización de la firma, en de los actos procesales ante los órganos judiciales y demás órganos pertenecientes a la Administración de Justicia.

V

Es importante subrayar que el uso del sistema Cl@veJusticia requiere que el usuario esté registrado en Cl@ve, con Cl@vePIN de la AEAT, de forma que el procedimiento para la identificación y firma electrónicas basada en Cl@veJusticia, con las condiciones que esta Resolución establecen, cuente con todas las garantías necesarias ofrecidas por el propio ecosistema establecido a través de la normativa actual.

Esto incluye por tanto los dos procesos fundamentales basados en la propia identificación mediante Cl@vePIN, la propia identificación del interesado, y la firma no criptográfica, con las condiciones establecidas en 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.

Por ello se ha tenido a bien establecer este sistema de firma no 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 requiera realizar una firma electrónica local con dicho certificado, con el fin de evitar problemas de restricciones de compatibilidad de navegadores, máquinas virtuales Java y versiones de sistemas operativos.

VI

En consecuencia, 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.

Por tanto, en virtud de lo anterior, en ejercicio de las competencias que se le asignan en el artículo 3 del Real Decreto 453/2020, de 10 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Justicia, esta Secretaría General para la Innovación y Calidad del Servicio Público de Justicia ha resuelto adoptar las siguientes disposiciones.

Primera.

Aprobar la utilización y condiciones de uso de Cl@veJusticia, como sistema de identificación y firma electrónica no criptográfica a efectos de identificación y firma de los interesados, en las actuaciones realizadas mediante presencia telemática, con los órganos judiciales y los demás órganos pertenecientes a la Administración de Justicia, de acuerdo con los artículos 4.2 f), 6.2 d), 14 y 23 de la Ley 18/2011, de 5 de julio, en relación con los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, que se incluyen como anexo a la presente resolución.

Segunda.

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

Madrid, 26 de mayo de 2021. El Secretario General para la Innovación y Calidad del Servicio Público de Justicia, Francisco de Borja Vargues Valencia.

ANEXO

Términos y condiciones de uso de Cl@veJusticia como sistema de identificación y firma electrónica no criptográfica a efectos de identificación y firma de los interesados, en las actuaciones realizadas por mediante presencia telemática, con los órganos judiciales y los demás órganos pertenecientes a la Administración de Justicia

I. *Objeto*

Los presentes términos y condiciones tienen como objeto determinar las circunstancias en las que Cl@veJusticia es válido como un sistema de identificación y firma electrónica no basado en certificados electrónicos para la identificación y firma de los interesados en las relaciones con los órganos judiciales y los demás órganos pertenecientes a la Administración de Justicia, de acuerdo con los artículos 4.2 f), 6.2 d), 14 y 23 de la Ley 18/2011, de 5 de julio, en relación con los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, cuando éstos se realicen mediante presencia telemática.

II. *Ámbito de aplicación*

Los presentes términos y condiciones serán de aplicación a las actuaciones realizadas mediante presencia telemática de los interesados con los órganos judiciales y demás órganos dependientes de Justicia, que habiliten Cl@veJusticia como sistema de identificación y firma electrónica no criptográfica destinados a ser usados por los interesados en sus relaciones con los mismos.

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, Cl@veJusticia se podrá utilizar como sistema de identificación se categorizada con el mismo nivel de seguridad que ofrece Cl@vePIN de la AEAT que actúa en todo momento como generador, almacenamiento y custodio de las evidencias del proceso de identificación.

En este sentido, todos los sistemas asociados que se apoyen en el sistema de Cl@veJusticia para le realización de firma electrónica no criptográfica deberán tener las medidas de seguridad implantadas al nivel establecido en el análisis de riesgos de cada sistema y procesos asociados.

Se deberá, por tanto, adecuar el uso de Cl@veJusticia con Cl@vePIN al nivel requerido de identificación.

Se establecen, además, los niveles sustancial o alto como los únicos válidos para la identificación mediante Cl@veJusticia(Cl@vePIN) en las interacciones con los órganos judiciales y los demás órganos pertenecientes a la Administración de Justicia, de acuerdo con los artículos 4.2 f), 6.2 d), 14 y 23 de la Ley 18/2011, de 5 de julio, en relación con los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, cuando éstos se realicen mediante presencia telemática, para la realización de firma electrónica no criptográfica, lo que deriva en la exigencia de un registro en Cl@vePIN de los interesados en los niveles equivalentes.

La determinación de uno u otro nivel vendrá derivado por el sistema de información sobre el que se recogerán las evidencias fruto de la interacción telemática cuyos efectos tendrán correspondencia en actuaciones procesales o administrativas recogidos en aquellos.

IV. *Garantía de funcionamiento*

A todos los efectos, la utilización de Cl@veJusticia, como sistema de identificación y firma electrónicas, en las actuaciones realizadas ante la Administración de Justicia, mediante presencia telemática, reviste de todas las garantías necesarias, surtiendo todos los efectos que el acto procesal o trámite lleve aparejados por la normativa procesal o administrativa aplicable.

Los sistemas de información en los que se recojan las evidencias de la interacción efectuada entre el interesado y el funcionario por medios telemáticos ofrecerán las garantías de autenticidad e integridad de todo intercambio efectuado, y conservará las evidencias electrónicas mediante sistemas de firma criptográfica o equivalentes, de forma que se aseguren su inalterabilidad y autenticidad.

Todos los intercambios de información y de documentación serán validados por el funcionario que está realizando la actuación por presencia telemática, de modo que la incorporación de la documentación en su caso, al sistema de gestión, se realizará de acuerdo a las propias garantías de autenticidad e integridad del sistema de información que, en su caso, apliquen.

El organismo responsable del procedimiento emitirá un justificante de firma sellado con su sello electrónico.

V. *Procedimiento general para la 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. Todo el proceso mediante interacción telemática debe contar con continuidad suficiente en la interacción mediante medios telemáticos debiendo, por tanto, garantizar una correcta transmisión bidireccional de audio y vídeo, en su caso.

Por tanto, ante problemas que pudieran alterar el resultado de una identificación basada en ClaveJusticia, deberá procederse a la re-identificación mediante dicho sistema.

2. Una autenticación previa del interesado, realizada a través de la plataforma Cl@veJusticia, en el momento de la manifestación de la voluntad contenido del acto procesal.

La identificación y autenticación del interesado deberá hacerse, en todo caso, a través de la plataforma Cl@veJusticia, que utiliza Cl@vePIN, de la AEAT, sistema de identificación, autenticación y firma electrónica basado en Cl@ves 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@veJusticia, inmediatamente previa al acto de firma, deberá de hacerse con un nivel de calidad en la autenticación sustancial o alto.

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

Estos datos se obtendrán a partir de aquella información que realice el funcionario al interesado en la atención por mediante presencia telemática, así como de los documentos electrónicos que, eventualmente, presente en el procedimiento.

El interesado debe ser consciente de los datos que va a firmar, por lo que deberá realizarse una recapitulación por parte del funcionario en un lenguaje comprensible que recogerá, a su vez, el documento-acta que elabore el sistema posteriormente se entregará al interesado como justificante de la firma y de la interacción efectuada.

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

Las aplicaciones que hagan uso de este sistema de firma, ajustado a los criterios de uso y 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 «Usted, D/D.ª [Nombre del Interesado], con DNI/NIE [Número], en la fecha y hora de la grabación de este acto, consiente en la solicitud siguiente:

Trámite/Procedimiento.

Datos principales del trámite/procedimiento, explicados en lenguaje comprensible para el ciudadano.

Y solicito para ello, como garantía de la firma electrónica básica efectuada a distancia, se proceda a la identificación segura de mi persona a través de Cl@vePIN.»

Para llevar a cabo la propia operación de firma se volverá a solicitar la autenticación del ciudadano mediante Cl@veJusticia mediante actuación directa del funcionario, lo que dará las garantías necesarias de autenticidad, trazabilidad, disponibilidad, integridad y no repudio, además de otras garantías establecidas en los puntos siguientes.

VI. *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, mediante actuación directa del funcionario.

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, Cl@veJusticia 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@veJusticia.
Fecha y hora de la firma.
Resumen seguro de los datos firmados, con un algoritmo de hash que cumpla las especificaciones del esquema nacional de seguridad.
Grabación de la interacción telemática.
En su caso, información sobre los datos intercambiados durante la interacción
Información de carácter técnico sobre la calidad de la interacción telemática
Actividad del funcionario y del ciudadano sobre los espacios de interacción comunes a los intervinientes de la interacción telemática
Fecha y hora de inicio y de fin de la interacción
Identidad del funcionario

En caso de que hubiera más de un interviniente en la interacción telemática, cuando aplique a los efectos de firma, se deberán guardar este conjunto de evidencias, para cada uno de ellos, reflejándose el orden de firma que el trámite exija legalmente.

Esta información deberá salvaguardarse con plenas garantías utilizando técnicas criptográficas o análogas que permitan garantizar la inalterabilidad a lo largo del tiempo, y la inalterabilidad del momento en que se generaron.

Además, se deberá conformar, en forma de acta, un documento que deberá ofrecer un resumen de los datos anteriores, con referencias a las evidencias, que 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.

VII. *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.

Cl@veJusticia recogerá todas las interacciones efectuadas con el sistema de información base de Cl@veJusticia, cl@vePIN de la AEAT, y las custodiará de acuerdo a las condiciones técnicas establecidas de nivel alto del ENS.

Al utilizar el sistema Cl@veJusticia como mecanismo de identificación y autenticación, las evidencias del sistema de información base no residen en el propio sistema de firma, sino en los sistemas de los proveedores de servicios de identificación integrados en Cl@vePIN de la AEAT, si bien se recogen estas en el sistema Cl@veJusticia, usuario de aquel.

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

VIII. *Justificante de firma*

En el proceso de firma se entregará al interesado un acta de evidencias electrónicas en la que se recojan todas las evidencias digitales de la realización del acto por mediante presencia telemática, 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 o del sistema en sí 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 documentos con sellado electrónico del justificante en formato PAdES (en el caso de que el justificante tenga formato PDF) y, en su caso, con la utilización de un código seguro de verificación (CSV) del justificante. La presente circular producirá sus efectos desde el momento de su firma.