BASE DE DATOS DE Norma CEF.-
Referencia: NCL012933

RESOLUCIÓN de 23 de febrero de 2022, de la Secretaría General de Administración Digital, por la que se establecen las condiciones de uso de firma electrónica no criptográfica vinculada a «AutenticA», para la relación con la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.

(BOE de 7 de marzo de 2022)

AutenticA es un servicio, desarrollado y gestionado por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, para la autenticación y autorización de usuarios en el acceso a determinados procedimientos de administración electrónica en el ámbito de la Administración General del Estado y sus organismos públicos o entidades de derecho público vinculados o dependientes. Se trata de un servicio de identidad digital basado en un repositorio horizontal de usuarios procedentes de fuentes primarias con las que se sincroniza y, en la actualidad, ofrece una capa horizontal de autenticación con certificado electrónico, y otros medios de autenticación como usuario y contraseña, lo cual favorece la interoperabilidad y la seguridad del sistema.

Hasta el momento, en los procedimientos electrónicos y trámites en los que en la fase de identificación los interesados o usuarios son autenticados a través de AutenticA, en el momento de completar la actuación concreta que requiera firma electrónica de dicho interesado o usuario sólo pueden firmar electrónicamente por medio de firma electrónica avanzada basada en certificados cualificados.

El 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 (en adelante Reglamento eIDAS) y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, establecen las condiciones de uso de la firma electrónica avanzada basada en certificados cualificados. Esta firma se encuentra muy extendida en el ámbito de la administración digital (por ejemplo es el sistema de firma de la suite «@firma», entre otras aplicaciones) y se basa en tecnología y herramientas muy consolidadas. Sin embargo, la práctica ha demostrado que elevada variedad de equipos, de escritorio o en movilidad, versiones de sistemas operativos, navegadores y, en su caso, máquinas virtuales Java, provoca que, en determinadas circunstancias, la firma del interesado o usuario mediante certificados cualificados sea muy gravosa o, en el peor de los casos, no sea técnicamente viable.

Para dar respuesta a esta situación no deseada en caso de que se produzca y poder extender así el uso de los servicios electrónicos, se considera conveniente disponer, de forma complementaria a la firma electrónica avanzada, de un sistema de firma electrónica básica vinculada a AutenticA que no requiera el procedimiento de firma electrónica local y que, gracias a ello, pueda ser operativa en un contexto como el mencionado, sistema que resultará apropiado aun cuando se haya utilizado un certificado electrónico en el proceso de identificación.

A estos sistemas de firma electrónica han de reconocérsele efectos jurídicos y son conformes a lo establecido en el artículo 25.1 del Reglamento eIDAS, sin perjuicio de lo previsto en el artículo 27 de la propia norma, que regula las «Firmas electrónicas en servicios públicos».

Con relación a los potenciales usuarios de la firma electrónica no criptográfica a que se refiere esta Resolución, debe tenerse en cuenta un triple marco normativo:

En primer lugar, el artículo 43.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal. Así, la firma electrónica no criptográfica a que se refiere esta Resolución permitirá una mayor cobertura de los servicios de administración digital orientados a los empleados públicos de la Administración General del Estado, como es el caso de los provistos por la Sede Funciona, creada según Orden TFP/303/2019, de 12 de marzo, y su versión móvil, o bien en el Portal Funciona, a través de Red SARA, ofrecidos por el Sistema Integrado de Gestión de Personal y el Registro Central de Personal.

En segundo lugar, la disposición adicional primera del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por Real Decreto 203/2021, de 30 de marzo, establece la obligatoriedad de uso de medios electrónicos en los procesos selectivos para el acceso al empleo público en el ámbito de la Administración General del Estado, sus organismos públicos o entidades de derecho público vinculados o dependientes de la misma. La elección de puestos de primer destino, ofrecido por el Sistema Integrado de Gestión de Personal, para los aspirantes que hayan aprobado un proceso selectivo en este ámbito requiere su firma electrónica, que se llevará a cabo mediante los sistemas previstos en el artículo 10.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, bien mediante un certificado electrónico cualificado de firma electrónica a que se refiere el párrafo a) o bien un sistema de firma objeto de esta Resolución en aplicación de lo previsto en el párrafo c).

En tercer lugar, los sujetos obligados por la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo en la Administración General del Estado, se relacionan con la Oficina de Conflictos de Intereses exclusivamente por medios electrónicos para la presentación de todas las declaraciones y el resto de comunicaciones y documentos a través de la sede electrónica asociada del Portal FUNCIONA, de acuerdo con lo previsto en el artículo 3 y en la disposición final primera del Reglamento por el que se desarrollan los títulos Preliminar, II y III de la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado, aprobado por el Real Decreto 1208/2018, de 28 de septiembre.

El Esquema Nacional de Seguridad (en adelante ENS) regulado por el Real Decreto 3/2010, de 8 de enero, 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 firmantes 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 virtud de lo anterior, y de acuerdo con el 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, en el ejercicio de las competencias atribuidas para definición de estándares, de directrices técnicas y de gobierno TIC (Tecnologías de la Información y las Comunicaciones), de normas de calidad e interoperabilidad de aplicación a las Administraciones Públicas y el desarrollo y aplicación de lo dispuesto en el 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 y sus Normas Técnicas de Interoperabilidad, y con el informe favorable preceptivo y vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior previsto en el art. 10.2.c) de la Ley 39/2015, de 1 octubre, evacuado el 25 de enero de 2022, dispone:

Primero.

1. Aprobar los términos y condiciones de uso de la firma electrónica no criptográfica vinculada a AutenticA, de acuerdo con lo previsto en el artículo 43.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el artículo 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los títulos Preliminar, II y III de la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado, y sus respectivos desarrollos reglamentarios, así como en la Disposición adicional segunda de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

2. Ordenar su publicación en el «Boletín Oficial del Estado».

Segundo.

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

Madrid, 23 de febrero de 2022. El Secretario General de Administración Digital, Juan Jesús Torres Carbonell.

ANEXO

Términos y condiciones de uso de la firma electrónica no criptográfica vinculada a AutenticA

Primero. *Objeto.*

Los presentes términos y condiciones tienen como objeto determinar los supuestos en que un sistema de firma electrónica no basada en certificados electrónicos vinculada al servicio AutenticA podrá ser utilizado en el ámbito de la Administración General del Estado, sus organismos públicos o entidades de derecho público vinculados o dependientes de la misma, de acuerdo con lo previsto en el artículo 43.2 de la Ley 40/2015, de 1 de octubre, el artículo 10 de la Ley 39/2015, de 1 de octubre, y los títulos Preliminar, II y III de la Ley 3/2015, de 30 de marzo. Todo ello sin perjuicio, de otros sistemas de firma implantados, 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 del Real

Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, que regula el análisis y gestión de los riesgos en dicho ENS.

Segundo. *Ámbito de aplicación.*

La firma electrónica no criptográfica vinculada a AutenticA prevista en esta Resolución se podrá utilizar en actuaciones o procedimientos de administración electrónica que permitan el uso de la firma electrónica básica, entre otros:

a) Los servicios de administración digital provistos por la Sede Funciona, creada según Orden TFP/303/2019, de 12 de marzo, y su versión móvil, o bien en el Portal Funciona, a través de Red SARA, que están orientados a los empleados públicos de la AGE, ofrecidos por el Sistema Integrado de Gestión de Personal y el Registro Central de Personal.

b) El servicio de elección de puestos de primer destino, ofrecido por el Sistema Integrado de Gestión de Personal, para los aspirantes que hayan aprobado un proceso selectivo.

c) Los servicios de declaraciones y comunicaciones del personal alto cargo, disponibles en la Sede Funciona, y dirigidas a la Oficina de Conflictos de Intereses, conforme al Real Decreto 1208/2018, de 28 de septiembre, por el que se aprueba el Reglamento por el que se desarrollan los títulos preliminar, II y III de la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado.

d) En cualquier servicio disponible en la Sede Funciona que permita la relación con la Administración General del Estado, por parte de empleados públicos en situación de excedencia o servicios especiales.

e) En el servicio TRAMA, de gestión de permisos e incidencias y control de presencia de personal, gestionado por la Secretaría General de Administración Digital.

Tercero. *Criterios para la utilización de la firma no criptográfica vinculada a AutenticA.*

En aplicación del Real Decreto 3/2010, de 8 de enero, se podrá utilizar un sistema de firma electrónica no criptográfica vinculada a AutenticA cuando el sistema de información asociado al procedimiento o servicio electrónico haya sido categorizado, según el ENS, 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.

Cuarto. *Garantía de funcionamiento.*

1. Cuando la actuación realizada por el usuario del servicio AutenticA, en su relación con la Administración General del Estado y sus organismos públicos y entidades de Derecho Público vinculados o dependientes de la misma, implique la presentación en una sede electrónica o sede electrónica asociada de documentos electrónicos utilizando un sistema de firma electrónica contemplado en la presente Resolución, se garantizará la integridad de la información presentada mediante el sellado realizado con un 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, 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 al procedimiento o servicio electrónico.

La Administración General del Estado, sus organismos públicos o entidades de derecho público vinculados o dependientes de la misma deberán disponer de las medidas técnicas, organizativas y procedimentales necesarias para garantizar dicha integridad a lo largo del tiempo de igual manera que se hace en los casos de firma criptográfica.

2. Asimismo, se garantizará también la integridad 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 firmante con el contenido firmado, almacenando dichas evidencias 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 del organismo y del resto de medidas técnicas que aseguren su inalterabilidad, de acuerdo con lo previsto en el apartado anterior.

3. En los supuestos previstos en los párrafos a) a d) del apartado segundo de esta Resolución, los sistemas a los que se refiere esta resolución facilitarán a la persona firmante un justificante de firma sellado con un sello electrónico, conforme al artículo 19 del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, y acompañado de un 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 Punto de Acceso General de la Administración General del Estado o en la Sede Funciona, en tanto no se destruyan de acuerdo con la normativa vigente.

Quinto. *Acreditación de la autenticidad de la expresión de la voluntad y consentimiento de la persona usuaria.*

1. Para acreditar la autenticidad de la expresión de la voluntad y consentimiento del firmante, se requerirá:

a) La autenticación del firmante, inmediatamente previa a la firma, utilizando el servicio AutenticA.
La autenticación, inmediatamente previa al acto de firma, deberá de hacerse con certificado electrónico u otro mecanismo que disponga de un nivel de calidad en la autenticación sustancial o alto, conforme a lo establecido en el Reglamento eIDAS.
b) La verificación previa por parte del firmante de los datos a firmar. Estos datos se obtendrán a partir de aquella información presentada por el firmante y de cuya veracidad se hace responsable, así como de los documentos electrónicos que, eventualmente, presente en el procedimiento o servicio electrónico que requiere la firma.
El firmante 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 firmante como justificante de la firma.
c) La acción explícita por parte del firmante de manifestación de consentimiento y expresión de su voluntad de firma.
Cuando las aplicaciones hagan uso de los sistemas de firma previstos en esta Resolución, se deberá requerir de forma expresa la expresión del consentimiento y la voluntad de firma del firmante, mediante la inclusión de frases que pongan aquéllos de manifiesto de manera inequívoca, y la exigencia de acciones explícitas de aceptación por parte del firmante (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 firmante debe marcar, y un botón «Firmar y enviar» que debe pulsar para realizar la firma).

Sexto. *Garantía de no repudio en el proceso de firma y gestión de las evidencias de autenticación.*

1. Para garantizar el no repudio de la firma por parte del firmante, un sistema de firma previsto en esta Resolución 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 firmante, mediante el servicio AutenticA, 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 firmante.
c) DNI/NIF/NIE del firmante.
d) Sistema de identificación sustancial o alto empleado.
e) Resultado exitoso de la autenticación.
f) Petición al proveedor externo de servicios de identificación o, en su caso, de validación y respuesta devuelta y firmada por éste.
g) Fecha y hora de la firma.
h) Resumen criptográfico de los datos firmados, realizado con un algoritmo de hash que cumpla las especificaciones del esquema nacional de seguridad.
i) Referencia al justificante de firma, en su caso, 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. 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.

2. Con relación a la gestión de las evidencias de autenticación, a pesar de que el sistema de firma proporcionará a los sistemas de información asociados al procedimiento o servicio 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.

En el caso de utilizar un sistema de identificación que requiera la consulta a un proveedor de servicios de identificación externo o a un proveedor de servicios de validación externo, las evidencias últimas no residen en el propio sistema de firma, sino en los sistemas de los proveedores de servicios de identificación o validación externos.

Con objeto de que los proveedores de esos servicios de identificación o validación 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 o servicio electrónico que requiere la firma, descrita en el apartado anterior.

A tal efecto, los proveedores de servicios de identificación o validación deberán salvaguardar dichas evidencias durante el plazo mínimo de cinco años. La solicitud de certificación de dichas evidencias se realizará conforme a la declaración de prácticas validación o declaración de política de certificación del proveedor.

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

1. Una vez acreditada la expresión de la voluntad y el consentimiento para firmar del firmante, 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 firmante, para lo cual el sistema de firma sellará los datos a firmar, con un sello electrónico, conforme al artículo 19 del Reglamento de actuación y funcionamiento del sector público por medios electrónicos 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 o servicio electrónico que requiere la firma.

2. En el proceso de firma se entregará al firmante bien el documento firmado electrónicamente, o bien, 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:

1.º Contener los datos del firmante tales como nombre, primer apellido y, en su caso, segundo apellido.

2.º Opcionalmente, contener los datos a firmar expresamente por el firmante, pudiendo contener una referencia de los documentos anexos, o, en su defecto, un hash del documento firmado.

3.º Garantizar la autenticidad del documento firmado, incluyendo en el justificante de firma un código seguro de verificación (CSV), y garantizando que este documento, o bien, el justificante, se pueda consultar en línea mediante un sistema de cotejo de CSV cuya dirección se incluya en el propio justificante de firma.

4.º En caso de que la consulta en línea, mediante código CSV, permita acceder al justificante de firma y no al documento firmado en sí, el justificante deberá contener los datos firmados expresamente por el firmante.