ORDEN DE LA CONSEJERÍA DE ECONOMÍA, EMPLEO Y TRANSFORMACIÓN DIGITAL, POR LA QUE SE ESTABLECEN LAS CONDICIONES DE USO Y LOS REQUISITOS TÉCNICOS DE LA PLATAFORMA DE IDENTIDAD DIGITAL DE LA JUNTA DE EXTREMADURA, EN LO QUE RESPECTA A LA IDENTIFICACIÓN Y FIRMA ELECTRÓNICA NO CRIPTOGRÁFICA EN LAS RELACIONES DE LAS PERSONAS INTERESADAS CON LA ADMINISTRACIÓN DE LA COMUNIDAD AUTÓNOMA DE EXTREMADURA Y SUS ORGANISMOS PÚBLICOS.

El acceso de la Ciudadanía a los servicios que se ofrecen en la Sede Electrónica y Sedes Electrónicas asociadas de la Administración de la Comunidad Autónoma de Extremadura requiere, según la naturaleza y requisitos de los servicios accedidos, la identificación electrónica de la persona y, en algunos casos, la firma electrónica del documento electrónico generado y/o tramitación realizada en la Sede.

La identificación electrónica tiene como finalidad aportar garantías en la identidad pretendida o declarada de una persona en su relación con la Administración por medios electrónicos. La autenticación electrónica, en los términos en que se recoge en esta Orden, es el proceso electrónico que posibilita la identificación electrónica de una persona.

La firma electrónica, por su parte, debe permitir acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados, así como la integridad e inalterabilidad del documento firmado.

Ambos instrumentos, Identificación y Firma, deben servir de garantía jurídica para los interesados y la Administración en su relación administrativa, por cumplir la normativa en materia de procedimiento administrativo, identificación electrónica, seguridad de la información y administración electrónica que resulte aplicable, pero conciliando estas garantías con la facilidad de uso de estos sistemas, lo cual debe potenciar la utilización de medios electrónicos como derecho de la Ciudadanía en su relación con la Administración.

El desarrollo de los sistemas de identificación y firma electrónica en el procedimiento administrativo se encuentra regulado en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante LPACAP), que regulan, por una parte, los sistemas de identificación y firma electrónica admitidos por todas las administraciones públicas y, por otra, la potestad de las administraciones para determinar si admiten otros sistemas que consideren válidos para efectuar determinados trámites o procedimientos de su ámbito de competencia.

A estos sistemas de identificación y firma electrónica complementarios, se les reconocerán plenos efectos jurídicos conforme se establece en el Reglamento (UE) Nº 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 (EIDAS), que

regula, en su artículo 8, los niveles de seguridad de los sistemas de identificación electrónica y, en su artículo 25 los efectos jurídicos de las firmas electrónicas, si bien los citados sistemas deberán observar, además, las prescripciones y requisitos de seguridad que a tal efecto se recogen en el Esquema Nacional de Seguridad (ENS), regulado por Real Decreto 311/2022, de 3 de mayo.

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, lo que aconseja a su vez a adaptar la complejidad y nivel de seguridad de los mecanismos de acceso electrónico en función de la finalidad del acceso, así como nivel de seguridad asociado a los datos e informaciones accedidos.

Así, y en aplicación de lo dispuesto en el artículo 10.4 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 Orden a regular los requisitos que se tienen que cumplir, no sólo con este objetivo, sino para asegurar también la integridad e inalterabilidad de los datos firmados, su correcta realización, así como la identificación del firmante y que la firma está vinculada al mismo.

La Junta de Extremadura viene apostando, desde hace años, por el uso del sistema Cl@ve como plataforma estatal de autenticación y firma electrónica a disposición de las distintas Administraciones Públicas. Sin embargo, se viene observando que determinados sectores de la Ciudadanía siguen encontrando problemas en el uso de la citada plataforma para la firma electrónica en el procedimiento administrativo, puesto que el acceso al certificado electrónico centralizado del ciudadano, que posibilita la firma, requiere su identificación por el sistema de Cl@ve permanente, lo cual supone ciertos inconvenientes para su obtención asociados a los requisitos del Nivel de Registro necesario (presencial o telemático con certificado electrónico cualificado o sistema equivalente), para la obtención del sistema de identificación y credencial asociada.

En este mismo sentido, la 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, recoge que 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.

Lo anterior viene a reforzar la necesidad y oportunidad de plantear los requisitos de un nuevo sistema de firma basado en la propia identificación electrónica de la persona y en la categorización del nivel de seguridad asociado al procedimiento y/o sistema de información en el que se despliegue este nuevo sistema de identificación y firma electrónica no criptográfica, siendo, en cualquier caso, complementario al uso de certificados a través de la integración de los sistemas corporativos de identificación y firma autonómicos con la plataforma estatal Cl@ve.

Las citadas necesidad y oportunidad de puesta en marcha de sistemas de identificación y firma electrónica complementarios que, por otra parte, no hacen más que adaptar los mismos a las tendencias actuales en otros ámbitos como el empresarial, financiero, universitario, etc., en la autenticación de accesos a sus servicios, se pone de manifiesto, además, en las últimas modificaciones efectuadas sobre los artículos 9 y 10 de la Ley 39/2015, que recogen como sistemas de identificación y/o firma previstos y habilitados, 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.

Por su parte, un sistema de identificación y firma electrónica no criptográfica en la Administración deberá cumplir con el ENS para garantizar la seguridad de los datos (informaciones) y los servicios, teniendo en cuenta que el sistema debe contar, entre sus propósitos, con la capacidad de comprobar la autenticidad de la identidad de los usuarios del mismo en el proceso de autenticación, así como garantizar la procedencia y la integridad de la información firmada electrónicamente, ofreciendo las bases para garantizar el no repudio; todo ello con un grado de confianza en la identidad pretendida o declarada de una persona que sea coherente con el nivel de riesgo y seguridad asociados al procedimiento y/o sistema de información en el que despliega sus efectos el sistema de identificación y firma electrónica no criptográfica.

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 lo que respecta al ámbito de aplicación de la presente Orden y a las medidas de seguridad que resultarían aplicables al sistema de identificación y firma electrónica no criptográfica que se regula en la misma, que deben ser coherentes con el nivel de seguridad de los procedimientos y/o sistemas de información que hagan uso del mismo, el ENS establece cuáles son los requisitos de seguridad a observar por los sistemas de información que implanten mecanismos de autenticación para usuarios externos a la Organización, no resultando necesario el uso de certificados digitales para la autenticación de la identificación electrónica de este tipo de usuarios en el acceso a los mismos y, en atención a lo expuesto anteriormente, tampoco para la firma electrónica cuando no se requiera que la misma sea avanzada basada en un certificado cualificado.

Así mismo, también resulta posible el uso de este sistema complementario cuando, aun habiéndose utilizado un certificado electrónico en el proceso de identificación, no se quiera realizar una firma electrónica con dicho certificado, proceso que puede llegar a requerir conocimientos avanzados de las tecnologías utilizadas para evitar los problemas de restricciones de compatibilidad de navegadores, máquinas virtuales Java y versiones de sistemas operativos.

Teniendo en cuenta estas consideraciones, con la presente Orden se pretende ampliar genéricamente el uso de este sistema de firma electrónica no criptográfica a todos los usuarios registrados, tanto en la plataforma estatal Cl@ve, como en la plataforma de Identidad Digital de la Junta de Extremadura, en aquellos casos en los que el registro en esta plataforma complementaria se haya realizado electrónicamente y sin el uso de medios no criptográficos, puesto que la plataforma articula un medio de identificación electrónica que establece un grado sustancial de confianza en la identidad pretendida o declarada de la persona registrada, que se consigue con las especificaciones técnicas de configuración del sistema de identificación electrónica no criptográfica y que resultan coherentes con lo regulado en el ENS respecto de los mecanismos de autenticación de usuarios (externos), entre otros controles técnicos, y cuyo objetivo es reducir sustancialmente el riesgo de uso indebido o alteración de la identidad.

A su vez, tanto el sistema de identificación, como el de firma electrónica por medios no criptográficos que se regula en la presente Orden, vienen a implementar los sistemas previstos en los artículos 9.2.c) y 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, garantizando esta Administración, así mismo, la posibilidad de utilización de alguno de los sistemas previstos en los apartados 2.a) y 2.b) de los mencionados artículos 9 y 10, para todos los procedimientos en todos sus trámites, aun cuando adicionalmente se permita alguno de los previstos al amparo de lo dispuesto en los apartados 2.c) y que se regulan a través de la presente Orden.

En al ámbito Autonómico, el Decreto 225/2014, de 14 de octubre, de régimen jurídico de administración electrónica de la Comunidad Autónoma de Extremadura, regula, en su Capítulo V, la identificación y autenticación electrónica en la relación entre ciudadanos y administración pública. Concretamente establece los posibles sistemas de identificación y firma electrónica tanto de los ciudadanos, autoridades y empleados públicos, como en actuaciones administrativas automatizadas.

En lo que respecta al ámbito material de la presente Orden, el artículo 35.2 del citado Decreto 225/2014, de 14 de octubre, recoge que, la admisión de otros sistemas de firma electrónica a los que se refiere el artículo 13.2.c de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos) deberán aprobarse mediante Orden del titular de la Consejería competente en materia de administración electrónica, en la que se establezcan los criterios que permitan identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que la firma está vinculada al firmante de manera única y

a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

El Decreto de la Presidenta 16/2023, de 20 de julio, por el que se modifican la denominación y las competencias de las Consejerías que conforman la Administración de la Comunidad Autónoma de Extremadura, recoge que la Consejería de Economía, Empleo y Transformación Digital ejercerá las competencias en materia de política tecnológica de carácter corporativo y administración electrónica.

Por lo tanto, y en virtud de lo anterior,

DISPONGO

Artículo 1. Objeto y ámbito de aplicación.

1. El objeto de esta Orden es establecer las condiciones de uso y los requisitos técnicos de la plataforma de Identidad Digital de la Junta de Extremadura, en lo que respecta a la identificación y firma electrónica no criptográfica en las relaciones de las personas interesadas con la administración de la Comunidad Autónoma de Extremadura y sus Organismos Públicos.
2. Las disposiciones establecidas en esta Orden son de aplicación:
    a) A la Administración de la Comunidad Autónoma de Extremadura.
    b) A los Organismos Públicos vinculados o dependientes de la misma, sujetos a derecho público. Los restantes organismos públicos estarán sujetos a la presente norma, en su caso, cuando ejerzan potestades públicas.
3. Los órganos de la Administración Pública de la Comunidad Autónoma de Extremadura y sus Organismos Públicos dependientes, únicamente podrán utilizar como sistema de identificación y firma electrónica no criptográfica el sistema corporativo implementado por el Centro Directivo competente en materia de administración electrónica y que podrá ofrecerse como servicio a aplicaciones integradas, una vez verificado por dicho Centro Directivo, que se cumplen los criterios de uso y demás condiciones que se recogen en la presente Orden.

Artículo 2. Criterios de uso.

1. El sistema para acreditar la identidad de usuarios signatarios por medios electrónicos no criptográficos será válido en función de la categorización (nivel de seguridad) del sistema de información y procedimiento o trámite administrativo que lo use. La determinación del nivel de seguridad del sistema de

información se llevará a cabo conforme a las prescripciones del ENS, mientras que la determinación del nivel de seguridad del procedimiento o trámite administrativo se delimitará a la evaluación del mismo como activo de información del sistema de información que tendrá en cuenta, además, la evaluación objetiva del riesgo asociada al tratamiento de datos realizado en el procedimiento o trámite, conforme a la normativa de protección de datos. Sólo aquellos procedimientos o trámites que tengan una catalogación baja o media podrán incorporar el sistema de firma no criptográfica.

2. Puesto que existen sistemas de información, como plataformas de tramitación, sedes electrónicas, etc., que habilitan la tramitación electrónica de múltiples procedimientos y/o trámites con distintos niveles de seguridad, cuando difieran los niveles de seguridad del procedimiento o trámite administrativo y del sistema de información que lo soporta, prevalecerá el primero de ellos, puesto que es el nivel de seguridad asociado al procedimiento o trámite administrativo concreto el que debe determinar el grado de confianza necesario en la identidad pretendida o declarada por la persona interesada para el acceso al mismo.

3. El uso de este sistema de identificación y firma electrónica no criptográfica será posible en sistemas de información y/o procedimientos y trámites administrativos en tramitación electrónica con niveles de seguridad bajo o medio. Para este último nivel, la firma electrónica no criptográfica será posible cuando no se requiera que la misma sea avanzada.

   Así mismo, también resultará posible el uso de este sistema complementario de firma electrónica no criptográfica cuando, aun habiéndose utilizado un certificado electrónico en el proceso de identificación, no se quiera realizar una firma electrónica con dicho certificado.

4. La implantación del sistema de identificación y firma electrónica no criptográfica de la Junta de Extremadura 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.

Artículo 3. Registro en la plataforma de Identidad Digital

1. La validez y usabilidad del sistema de identificación y firma electrónica no criptográfica estará basado en el registro previo del usuario que permita garantizar su identidad con un nivel de confianza básico en el proceso de registro.

   El nivel básico de confianza en el registro podrá escalar a fuerte en función del mecanismo de acreditación de la identidad utilizado (que podrá ser electrónico o no) para su registro o con posterioridad al mismo.

   Los mecanismos y niveles de registro asociados a los mismos se recogen como Anexo II a esta Orden.

2. La plataforma validará, previa información al interesado, los datos identificativos declarados por el usuario en el proceso de registro contra los servicios de intermediación de datos de la Administración del Estado, salvo que el mecanismo de acreditación de la identidad utilizado por el usuario en el proceso de registro haga innecesaria tal validación, por constituir evidencia suficiente de la identidad del usuario. Así mismo, solicitará su autorización para la remisión de comunicaciones a su número (a través de SMS) y/o dispositivo móvil (a través de App), correo electrónico u otros medios que puedan utilizarse para reforzar el proceso de acreditación de la identidad en el proceso de registro.

3. El nivel de registro, en base a la modalidad de registro utilizada, determinará el grado de confianza en la identidad pretendida o declarada de una persona y, por consiguiente, el nivel de seguridad máximo con el que puede interactuar teniendo en cuenta, además, las credenciales utilizadas.

4. El uso de este sistema de firma electrónica no criptográfica estará habilitado para todos los usuarios registrados, tanto en la plataforma Estatal Cl@ve, como en la plataforma de Identidad Digital de la Junta de Extremadura y siempre que el nivel de seguridad del sistema de información y/o procedimientos o trámites administrativos desplegados en el mismo lo permita. Esto es, nivel de seguridad bajo o medio que no requiera firma electrónica avanzada que tendrá en cuenta, además, el nivel en Cl@ve o nivel en Plataforma de Identidad Digital del usuario registrado, conforme se recoge en Anexo II a esta Orden.

Artículo 4. Descripción del sistema de identificación y firma electrónica no criptográfica.

1. El mecanismo de identificación y firma electrónica no criptográfica basará su validez en el envío de códigos de un solo uso (OTP, de sus siglas en inglés) al número de teléfono móvil del usuario previamente registrado en la plataforma Estatal Cl@ve o en la plataforma de Identidad Digital de la Junta de Extremadura. El proceso de registro garantiza la exclusividad del número de móvil por usuario, salvo excepciones que deberán justificarse y documentarse en la plataforma. Este mecanismo será complementario a otros disponibles también para el usuario, de conformidad con lo regulado en los artículos 9.2 y 10.2 de la Ley 39/2015, de 1 de octubre.

   En función de la evolución tecnológica y normativa en el ámbito de la Identificación Electrónica, así como la propia evolución de la plataforma de identidad digital de la Junta de Extremadura, podrán incorporarse otros mecanismos de autenticación, como códigos de respuesta rápida (QR, de sus siglas en inglés) validados desde App móvil asociada a usuario, envío de credenciales digitales desde cartera (Wallet) de dispositivo móvil, etc., siempre que los mismos aporten, al menos, las mismas garantías (nivel bajo o superior) para la verificación de la identidad pretendida o declarada por las personas interesadas.

2. Estos métodos de autenticación reforzada o segundo factor de autenticación se utilizarán en el proceso electrónico de autenticación del acceso de usuario externo al sistema de información y se renovarán en el momento que dicho usuario deba proceder a la firma electrónica no criptográfica de la solicitud, declaración, etc., constituyendo esta renovación (nuevo SMS, código QR en App, etc.) la manifestación expresa de conformidad con el contenido del documento o informaciones objeto de firma y voluntad del usuario.

3. El mecanismo de autenticación solicitado y/o remitido al usuario (código SMS, código QR, etc.) tendrá una validez limitada en el tiempo y estará asociado al usuario, procedimiento, trámite y, en su caso, documento objeto de firma electrónica no criptográfica, dejando constancia de ello en la propia firma electrónica o metadatos asociados a la misma.

   La autenticación satisfactoria por parte del usuario producirá la firma electrónica y generará un justificante de la firma electrónica no criptográfica realizada que se pondrá a disposición de la persona interesada y del sistema, aplicación o servicio desde el que se haya invocado la firma.

4. El justificante, sellado electrónicamente por el Órgano u Organismo, incluirá los datos identificativos de la persona firmante, la identificación del documento firmado, la indicación de la fecha y hora en que se ha efectuado la firma y un código electrónico de autenticidad que permitirá comprobar su validez a través del servicio de verificación de integridad de documentos de la sede electrónica de la Administración de la Comunidad Autónoma de Extremadura. Será un documento legible de acuerdo con la norma técnica de interoperabilidad de catálogo de estándares y preferiblemente en formato PDF.

Artículo 5. Requisitos técnicos del sistema de identificación y firma electrónica no criptográfica.

1. Se procede a la aprobación de los requisitos técnicos del sistema de identificación y firma electrónica no criptográfica de la Administración de la Comunidad Autónoma de Extremadura, recogidos como Anexo I, para su uso en sistemas de información y/o procedimientos y trámites administrativos, conforme a las condiciones de seguridad, al ámbito de aplicación, y otras relativas a los niveles de confianza en la identificación electrónica, que se recogen en esta Orden.

2. La actualización o actualizaciones que, en lo sucesivo, resulten procedentes de los requisitos técnicos del sistema de identificación y firma electrónica no criptográfica que se recogen como Anexo I a la presente Orden, se llevarán a cabo mediante resolución del Centro Directivo competente en materia de Administración Electrónica, previo informe del Responsable de Privacidad y Seguridad de la Junta de Extremadura sobre los controles y niveles de seguridad asociados a los mecanismos nuevos o actualizados y entrarán en vigor desde su publicación en el Diario Oficial de Extremadura (https://doe.juntaex.es), sin

perjuicio de cualesquiera otros requisitos que resulten pertinentes para su eficacia jurídica.

Artículo 6. Mecanismos de identificación y firma electrónica no criptográfica.

1. Los mecanismos de identificación y firma electrónica no criptográfica aprobados a través de la presente Orden para su uso en los sistemas de información y/o procedimientos y trámites administrativos de la Administración de la Comunidad Autónoma de Extremadura y sus Organismos Públicos dependientes son los publicados en el Anexo II de la presente Orden.
2. La actualización o actualizaciones que, en lo sucesivo, resulten procedentes de los mecanismos de identificación y firma electrónica no criptográfica que se recogen como Anexo II a la presente Orden, se llevarán a cabo mediante resolución del Centro Directivo competente en materia de Administración Electrónica, previo informe del Responsable de Privacidad y Seguridad de la Junta de Extremadura sobre los controles y niveles de seguridad asociados a los mecanismos nuevos o actualizados y entrarán en vigor desde su publicación en el Diario Oficial de Extremadura (https://doe.juntaex.es), sin perjuicio de cualesquiera otros requisitos que resulten pertinentes para su eficacia jurídica.
3. En cualquier caso, los mecanismos aprobados deberán cumplir con los requisitos técnicos del sistema de identificación y firma electrónica no criptográfica regulados y aprobados en el artículo 5 y, en general, en la presente Orden.

Disposición final primera. Desarrollo y ejecución.

Se faculta al Centro Directivo competente en materia de Administración Electrónica a dictar las instrucciones necesarias para el desarrollo y cumplimiento de lo dispuesto en esta Orden.

Disposición final segunda. Entrada en vigor.

Esta Orden entra en vigor el día siguiente a su publicación en el Diario Oficial de Extremadura.

ANEXO I. Requisitos técnicos del sistema de identificación y firma electrónica no criptográfica.

I. *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 mecanismos de identificación y firma electrónica no criptográficos, se garantizará la integridad de la información presentada mediante sellado realizado con el sello electrónico cualificado del órgano u organismo competente, al que se añadirá un sello de tiempo realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado, siendo inmediata su incorporación al sistema de información asociado a dicho procedimiento. El órgano u organismo de la Administración de la Comunidad Autónoma 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, para lo cual, al sellado realizado conforme se indica en el párrafo anterior, se adicionarán 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 (copia auténtica de documento sellado electrónicamente con el sello de órgano) que contendrá 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 de verificación de integridad de documentos de la sede electrónica de la Administración de la Comunidad Autónoma de Extremadura, en tanto no se acuerde la destrucción de dichos documentos con arreglo a la normativa que resulte de aplicación o por decisión judicial.

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

Será posible la acreditación de la identidad y de la autenticidad de la expresión de la voluntad y consentimiento del interesado por cualquiera de los mecanismos de identificación y firma electrónica no criptográfica recogidos en la presente Orden, sin perjuicio de cualesquiera otros que resulten válidos, de conformidad con la normativa europea, estatal y autonómica de aplicación y con los niveles de seguridad de los sistemas de información y/o procedimientos y trámites en que se integren.

El nivel de seguridad asociado al usuario registrado en la Plataforma de Identidad Digital de la Junta de Extremadura condicionará el nivel de seguridad de los sistemas de información y/o trámites o procedimientos en los que se podrá usar el mecanismo de identificación y firma electrónica no criptográfica asignado al usuario.

La correlación entre el nivel de seguridad asociado al usuario registrado, las modalidades de registro posibles, el mecanismo de identificación y firma electrónica (criptográfico o

no criptográfico) utilizado y el nivel de seguridad de los sistemas de información y/o procedimientos o trámites administrativos en que puede utilizarse el citado sistema se recogen en el Anexo II, que desarrolla los mecanismos de identificación y firma electrónica no criptográfica que se regulan en el artículo 6 de la presente Orden para su uso en los sistemas de información y/o procedimientos y trámites administrativos de la Administración de la Comunidad Autónoma de Extremadura y sus Organismos Públicos dependientes.

En el ámbito material del proceso de firma electrónica no criptográfica, para acreditar la autenticidad de la expresión de la voluntad y consentimiento del interesado se requerirá:

II.1. Verificación de la identidad del interesado. Autenticación.

La verificación de la identidad del interesado a quien le corresponde el acto de la firma se llevará a cabo en el momento inmediatamente previo del propio acto, mediante una nueva autenticación o utilizando mecanismos de contraste, autenticación reforzada o segundo factor de autenticación, que garanticen la verificación.

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

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, por lo que tendrá la posibilidad de consultarlos en un formato legible con carácter previo a la firma.

II.3. Acción explícita, por parte del interesado, de manifestación de consentimiento y expresión de su voluntad de firma.

Se requerirá la expresión explícita del consentimiento y la voluntad de firma del interesado en el procedimiento, mediante la inclusión de texto que recoja de manera inequívoca dicha expresión, además de la aceptación explícita por parte del interesado.

III. Garantía de no repudio.

III.1. Garantías en el proceso de firma.

Para garantizar el no repudio, 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 firmante en el momento de proceder a la firma.

El sistema incluirá mecanismos que permitan contrastar la identidad del firmante (autenticación) 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, esto es: autenticación de la persona firmante, expresión de voluntad y consentimiento y actuación de firma, para lo cual, por cada proceso de firma no criptográfica, se conservará la siguiente información:

a) Fecha y hora de la autenticación.

b) Nombre y apellidos de la persona interesada.
c) DNI/NIF/NIE de la persona interesada.
d) Mecanismo de identificación (autenticación) empleado y nivel de seguridad asociado al mismo de entre los recogidos en el Anexo II de la presente Orden.
e) Resultado exitoso de la autenticación junto con las correspondientes evidencias técnicas la autenticación realizada.
f) Fecha y hora de la manifestación de voluntad de firma.
g) Resumen criptográfico de los datos objeto de firma con un algoritmo de hash que cumpla las especificaciones del Esquema Nacional de Seguridad.
h) CSV asociado al justificante de firma electrónica.

La anterior información será firmada con un certificado de sello electrónico que garantiza su integridad, incorporando un sello de tiempo acorde la normativa de aplicación, y será almacenada como evidencia de la voluntad de firma, autenticación del firmante, integridad de los datos firmados y vinculación entre los tres elementos anteriores.

Por último, con el mismo propósito de auditoría para asegurar la garantía de no repudio, se almacenarán las evidencias de las actuaciones de autenticación, referencias y vinculación al CSV del justificante de firma durante el plazo mínimo de cinco años.

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

IV.1. Sellado electrónico 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 electrónica no criptográfica sellará los datos a firmar con un sello electrónico de órgano, que adicionará, a su vez, un sello de tiempo realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado, poniendo el resultado de este proceso a disposición del sistema de información asociado al procedimiento electrónico que requiere la firma.

IV.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, preferiblemente en formato PDF, y que deberá cumplir los siguientes 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.
- Alternativamente, la autenticidad del organismo emisor y del justificante de firma se podrá garantizar mediante dos documentos: el primero de ellos con sellado electrónico del justificante en formato PAdES (en el caso de que el justificante tenga formato PDF) y, el segundo, con la utilización de un código seguro de verificación (CSV) incorporado en el justificante que lo haga accesible para su consulta en línea mediante el sistema de cotejo de CSV de la Administración u Organismo competente, cuya dirección esté incluida en el propio justificante. También resultaría posible que un mismo documento justificante incorpore los dos mecanismos de garantía de autenticidad.

ANEXO II. Mecanismos de identificación y firma electrónica no criptográfica.

Los mecanismos de identificación electrónica aprobados a través de la presente Orden para su uso en los sistemas de información y/o procedimientos y trámites administrativos, dirigidos a la Ciudadanía y Empresas, de la Administración de la Comunidad Autónoma de Extremadura y sus Organismos Públicos dependientes, son los recogidos en la siguiente tabla de características:

Nivel en Plataforma[1]	**Nivel de Registro**	**Modo de Registro**	**Credencial habilitada**	**Nivel de Seguridad (máximo)**
Bajo	Básico	Telemático a partir de datos conocidos, verificados y con número móvil vinculado[2] a usuario.	Contraseña[3] + OTP[4]	BAJO
				MEDIO. Si no requiere firma electrónica avanzada.
Medio	Fuerte	Presencial, telemático con certificado electrónico cualificado o sistemas equivalentes. Video-identificación[5].	Contraseña + OTP Certificado electrónico cualificado	MEDIO. (Sustancial[6]).
Alto	Fuerte	Presencial, telemático con certificado electrónico cualificado o sistemas equivalentes.	DNI electrónico. Otros certificados cualificados en soporte Hardware	ALTO

Con independencia de los niveles de registro y seguridad anteriores, solo será posible la realización de firmas electrónicas no criptográficas cuando el sistema de información y/o procedimiento o trámite administrativo 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. Tanto las credenciales habilitadas, como los modos de registro de los niveles de seguridad más altos abarcan y son aplicables a los niveles inferiores.

El nivel en plataforma se obtiene a partir del Nivel de Registro, Modalidad de Registro y Credencial utilizada para la Autenticación en Plataforma de Identidad Digital.

La plataforma de Identidad Digital de Extremadura admitirá, además, los usuarios registrados en la plataforma estatal Cl@ve y Credenciales que facilita la misma, siendo coincidentes los Niveles en Plataforma recogidos en la tabla Anterior en Cl@ve, habilitando en consecuencia el acceso a los mismos niveles de seguridad.

[1] Nivel de autenticación en Plataforma de Identidad Digital de la Junta de Extremadura.
[2] El número de móvil vinculado al usuario lo es con carácter exclusivo, no pudiendo aparecer el mismo número vinculado a ningún otro usuario en plataforma.
[3] Se seguirán las recomendaciones del Esquema Nacional de Seguridad para la conformación de contraseñas de usuarios externos.
[4] Clave de un solo uso comunicada al móvil de usuario registrado en plataforma. De sus siglas en inglés (One Time Password).
[5] Mecanismos de video-identificación en línea coherentes con la evolución de EIDAS 2 y cumpliendo los requisitos de ETSI (Isntituto Europeo de Telecomunicaciones Electrónicas) para los servicios que provean prueba de identidad.
[6] Coincidente con el nivel de seguridad sustancial en la identificación, según Reglamento EIDAS.