I. DISPOSICIONES GENERALES

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

7966 *Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.*

I

El Reglamento (UE) 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 el que se deroga la Directiva 1999/93/CE, contempla la posibilidad de verificación de la identidad del solicitante de un certificado cualificado utilizando otros métodos de identificación reconocidos a escala nacional que garanticen una seguridad equivalente en términos de fiabilidad a la presencia física.

La emergencia sanitaria generada por la crisis de la COVID-19 ha exigido durante el estado de alarma el confinamiento de la ciudadanía y la drástica limitación de los desplazamientos personales, con vistas a frenar el crecimiento de los contagios. De forma transitoria y excepcional, a través de la disposición adicional undécima del Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente a la COVID-19, se habilitó un sistema temporal de identificación remota para la obtención de certificados cualificados, con el fin de contribuir a reducir los desplazamientos de los ciudadanos para realizar trámites, sin mermar sus derechos.

Con el fin de implantar de forma permanente y con plena seguridad jurídica dicha posibilidad, el artículo 7.2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, habilita a que mediante orden ministerial de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se determinen las condiciones y requisitos técnicos de verificación de la identidad a distancia y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación como videoconferencia o vídeo-identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, que permitan la implantación de los citados métodos por parte de los prestadores de servicios electrónicos de confianza, en razón de las especificidades propias de este sector y las obligaciones de seguridad a que están sujetos los prestadores cualificados.

Asimismo, se constata la existencia de una necesidad, manifestada por los prestadores de servicios electrónicos de confianza, de dotar al ordenamiento jurídico español de una norma específica que les permita utilizar esta ventaja competitiva en la provisión de sus servicios, y que les habilite a identificar de forma remota por vídeo a los solicitantes de certificados cualificados, de forma que puedan seguir expandiendo su actividad y competir con los prestadores establecidos en otros países que ya disponen de una normativa nacional a tal efecto. Al respecto, es destacable que España es el país de la Unión Europea con un mayor mercado de prestadores de servicios electrónicos de confianza, tal y como se refleja en la Lista española de Prestadores Cualificados (*Trusted Services List*, o TSL), mantenida por el Ministerio de Asuntos Económicos y Transformación Digital como órgano supervisor.

II

En cuanto a las medidas organizativas y procedimentales que deberán implantar los prestadores, es importante señalar que deben ser proporcionales a los riesgos y

cve: BOE-A-2021-7966
Verificable en https://www.boe.es

adecuadas a la naturaleza de estos servicios, pilares de la construcción de otros servicios digitales de valor añadido. Al respecto, se han de tener en consideración las necesidades procedimentales y de seguridad específicas de la expedición de certificados cualificados de utilización universal y que constituyen un auténtico *alter ego* digital de la persona.

En este sentido, esta orden ministerial especifica el procedimiento que debe seguirse para la identificación remota por vídeo de un solicitante, así como los requisitos y las acciones mínimas que deben llevar a cabo los prestadores para detectar los intentos de suplantación de identidad o posibles manipulaciones de las imágenes o los datos del documento de identidad. Dichos métodos de identificación remota por vídeo no prejuzgan la existencia de otros sistemas de identificación a distancia amparados por el artículo 24.1 del mencionado Reglamento (UE) 910/2014, que no son objeto de regulación en esta orden.

Entre otras medidas, se exige verificar la autenticidad y validez del documento de identidad, así como su correspondencia con el solicitante del certificado. Para ello, el sistema de identificación remota por vídeo empleado en el proceso deberá incorporar los medios técnicos y organizativos necesarios para verificar la autenticidad, vigencia e integridad de los documentos de identificación utilizados, verificar la correspondencia del titular del documento con el solicitante que realiza el proceso, mediante tecnologías como el reconocimiento facial, y verificar que este es una persona viva que no está siendo suplantada; debiendo quedar todos estos requisitos acreditados, en los términos que establece el anexo F11 de la Guía de Seguridad de las TIC CCN-STIC-140, del Centro Criptológico Nacional mediante la certificación del producto. La referencia a la Guía ha de entenderse hecha siempre a la última versión disponible. Así mismo, se exige que el personal encargado de la verificación de la identidad del solicitante verifique la exactitud de los datos del solicitante, utilizando las capturas del documento de identidad utilizado en el proceso, además de cualquier otro medio automático que pudiera ser implementado en los sistemas de identificación remota por vídeo.

Para contribuir a este fin, se contempla la puesta a disposición de los prestadores del acceso a la plataforma de intermediación del Servicio de Verificación y Consulta de Datos, cuyo organismo responsable es la Secretaría de Estado de Digitalización e Inteligencia Artificial, como medio de contrastar los datos de identidad de los solicitantes con una fuente auténtica, en línea con las disposiciones del Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del citado Reglamento (UE) 910/2014.

III

Con objeto de acreditar el cumplimiento de los requisitos de seguridad exigibles a las herramientas utilizadas en los procesos de identificación remota, los prestadores utilizarán productos cuya funcionalidad de seguridad esté certificada según las metodologías de evaluación reconocidas por el Organismo de Certificación del ENECSTI (Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información). Es importante señalar que la evaluación y certificación de un producto de seguridad de las Tecnologías de la Información y la Comunicación (TIC) es el único medio objetivo que permite valorar y acreditar la capacidad de un producto para manejar información de forma segura.

Con el fin de adaptarse de forma ágil al continuo avance de la tecnología, esta orden ministerial hace referencia a las correspondientes guías técnicas elaboradas y actualizadas por el Centro Criptológico Nacional, en relación con las características y requisitos puramente tecnológicos aplicables a los productos y herramientas de identificación remota por vídeo para garantizar un adecuado nivel de seguridad de los mismos.

Del mismo modo, se considerarán los estándares que, en su caso, sean adoptados a nivel europeo e internacional, en particular por el Instituto Europeo de Normas de Telecomunicaciones (ETSI).

cve: BOE-A-2021-7966
Verificable en https://www.boe.es

Asimismo, esta orden ministerial deberá aplicarse de manera que se cumplan las obligaciones del Reglamento (UE) 2016/679, del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, así como el resto de la normativa sobre protección de datos personales, particularmente la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Dentro de las obligaciones de seguridad que esta orden impone a los prestadores de servicios de confianza, se contempla un análisis de riesgos que contemple las medidas técnicas y organizativas adecuadas con respecto a los datos personales, conforme al citado Reglamento (UE) 2016/679.

IV

De acuerdo con lo establecido en el artículo 24.1.d) del Reglamento (UE) 910/2014, la seguridad equivalente en términos de fiabilidad a la presencia física deberá ser confirmada por un organismo de evaluación de la conformidad acreditado, que verificará el cumplimiento de los requisitos legales exigidos en esta orden, incluyendo, durante el periodo transitorio hasta la obligatoriedad de la certificación anteriormente señalada, la comprobación del nivel de seguridad del sistema o producto utilizado por el prestador de acuerdo con la guía CCN-STIC-140. Esta comprobación se realizará mediante la evaluación de otras certificaciones, informes, pruebas de laboratorio y otros elementos aportados por el fabricante. El resultado de la misma se reflejará en el informe de evaluación de la conformidad que el prestador cualificado remitirá al órgano de supervisión con carácter previo al ofrecimiento al público de la posibilidad de identificarse de manera remota.

V

Esta norma, dictada al amparo de la habilitación legal contenida en el artículo 7.2 de la Ley 6/2020, de 11 de noviembre, se compone de doce artículos, una disposición transitoria y dos disposiciones finales, y se adecua a los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia, a los que debe sujetarse el ejercicio de la potestad reglamentaria, de conformidad con lo dispuesto en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Por lo que se refiere a los principios de necesidad y eficacia, esta orden ministerial es el instrumento óptimo para llevar a cabo el desarrollo reglamentario previsto, debido a que es preciso dotar al sector de una regulación específica y susceptible de ágil adaptación que recoja los requisitos técnicos, organizativos y procedimentales aplicables a los métodos de identificación remota por vídeo.

En cuanto al principio de proporcionalidad, esta orden ministerial establece los requisitos apropiados exigibles a los sistemas de identificación a distancia de forma que se garantice la seguridad del tráfico jurídico y el adecuado nivel de protección de los usuarios y actividad económica.

En el procedimiento de elaboración de esta orden se ha tenido en cuenta lo dispuesto en la Ley 50/1997, de 27 de noviembre, del Gobierno, y en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Se sometió el texto a consulta previa a los sujetos directamente afectados, en concreto, los prestadores cualificados de servicios electrónicos de confianza y a los organismos de evaluación de la conformidad acreditados, con objeto de garantizar el acierto y la legalidad de la norma, de acuerdo con el artículo 26.1 de la Ley 50/1997, y se ha sometido al trámite de audiencia e información pública previsto en el artículo 26.6 de la citada ley, posibilitando así la participación activa de los potenciales destinatarios. En ambas fases se han recibido numerosas observaciones que se han tenido en cuenta en la elaboración de este texto. Por lo anterior, se considera cumplido el principio de transparencia.

cve: BOE-A-2021-7966
Verificable en https://www.boe.es

En relación con el principio de eficiencia, esta orden ministerial no impone cargas administrativas innecesarias, y su desarrollo se ha producido con la mayor celeridad posible.

Por último, se han recabado informes, de conformidad con lo previsto en el artículo 26.5 de la Ley 50/1997, de los siguientes departamentos ministeriales y organismos públicos: Ministerio de Defensa, Ministerio del Interior, Ministerio de Hacienda, Ministerio de Justicia y Ministerio de Sanidad, así como de la Agencia Española de Protección de Datos.

En su virtud, con la aprobación previa del Ministro de Política Territorial y Función Pública y de acuerdo con el Consejo de Estado, dispongo:

Artículo 1. *Objeto.*

Esta orden tiene por objeto regular las condiciones y requisitos técnicos mínimos aplicables a la verificación de la identidad y, si procede, otros atributos específicos, de la persona solicitante de un certificado cualificado mediante métodos de identificación remota por vídeo de acuerdo con lo previsto en el artículo 7.2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y en el artículo 24.1.d) del Reglamento (UE) 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 el que se deroga la Directiva 1999/93/CE. Lo anterior se entenderá sin perjuicio de la existencia de otros métodos de identificación a distancia amparados por el artículo 24.1 del Reglamento (UE) 910/2014 no incluidos en el ámbito de aplicación de esta orden.

Artículo 2. *Ámbito de aplicación subjetivo.*

Esta orden se aplicará a los prestadores cualificados públicos y privados de servicios electrónicos de confianza establecidos en España.

Así mismo, se aplicará a los prestadores cualificados residentes o domiciliados en otro Estado miembro que tengan un establecimiento permanente situado en España, siempre que ofrezcan servicios no supervisados por la autoridad competente de otro Estado miembro de la Unión Europea.

La ejecución de los procedimientos de identificación remota por vídeo podrá ser externalizada, manteniendo el prestador que expide el certificado cualificado la plena responsabilidad en relación con la aplicación de esta orden.

Artículo 3. *Protección de datos de carácter personal.*

Los tratamientos de datos de carácter personal de las personas físicas se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, así como en el resto de la normativa sobre protección de datos personales.

Artículo 4. *Modalidades de identificación remota por vídeo.*

El proceso de identificación remota por vídeo se podrá realizar de forma asistida, con la mediación síncrona de un operador, o de forma no asistida, sin necesidad de interacción en línea entre un operador y el solicitante, con revisión posterior de un operador.

Artículo 5. *Evaluación de la conformidad y comprobación del cumplimiento de requisitos.*

1. El cumplimiento de los requisitos establecidos en esta orden deberá ser confirmado por un organismo de evaluación de la conformidad acreditado. El organismo de evaluación

cve: BOE-A-2021-7966
Verificable en https://www.boe.es

deberá reflejar en el informe, de manera pormenorizada, cómo cumple el prestador los requisitos definidos en esta orden.

2. El prestador cualificado de servicios de confianza remitirá solicitud para la puesta en operación de procedimientos de identificación remota por vídeo a la Secretaría de Estado de Digitalización e Inteligencia Artificial, dependiente del Ministerio de Asuntos Económicos y Transformación Digital, en cuanto órgano supervisor. Dicha solicitud incluirá una descripción detallada del sistema y su operación, la declaración de prácticas actualizada, así como el informe de evaluación de la conformidad, con carácter previo a su ofrecimiento al público.

3. El órgano supervisor podrá requerir al prestador para que aporte, en el plazo de diez días hábiles, documentación e información adicionales sobre cualquier aspecto de la solución de identificación remota por vídeo, con carácter previo o posterior a su implantación.

4. El prestador podrá comenzar a operar mediante procedimientos de identificación remota por vídeo a partir de la fecha de notificación de la resolución estimatoria. El plazo máximo para resolver y notificar será de seis meses, transcurridos los cuales la solicitud se entenderá desestimada.

5. Para los prestadores que inicien su actividad de prestación de servicios de confianza cualificados con posterioridad a la entrada en vigor de esta orden, los trámites a los que se refiere este artículo se podrán integrar en el procedimiento de cualificación regulado en el artículo 21 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Artículo 6. *Requisitos generales de seguridad.*

El prestador cualificado de servicios electrónicos de confianza:

a) Dispondrá de un modelo de gestión continua del riesgo que incluirá un análisis de riesgos especifico que se revisará con una periodicidad mínima anual y, en todo caso, siempre que se produzca un cambio en el sistema, en los procedimientos organizativos, en el estado de la tecnología, o en cualquier otro aspecto que pudiera influir en el perfil de riesgo del procedimiento de identificación.

Este análisis deberá tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento de los datos personales, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas conforme a lo exigido por la normativa de protección de datos personales.

Asimismo, realizará una evaluación de impacto en la protección de datos personales cuando del análisis realizado resulte probable que el tratamiento suponga un alto riesgo para los derechos y libertades de las personas, conforme a lo previsto en la citada normativa.

b) Adoptará medidas técnicas y organizativas adicionales a las indicadas en esta orden cuando el resultado del análisis de riesgos efectuado así lo requiera.

En relación con los datos de carácter personal, adoptará las medidas técnicas y organizativas apropiadas, según lo establecido en el artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016.

Estas medidas se actualizarán sin dilación indebida cuando se tenga conocimiento de vulnerabilidades que puedan dan lugar a brechas de seguridad.

c) Evaluará y documentará las características de seguridad del conjunto del sistema, incluyendo todos los elementos sustantivos de la plataforma de identificación, los canales de comunicación, y la generación y conservación de pruebas producidas durante el proceso de identificación.

d) Empleará un producto de identificación remota por vídeo que cumpla los requisitos mínimos de seguridad indicados en el anexo F.11 de la Guía de Seguridad de las TIC CCN-STIC-140, del Centro Criptológico Nacional de categoría alta. El prestador cualificado deberá seguir las indicaciones de configuración y uso seguro del producto. El cumplimiento de dicha obligación deberá ser certificado siguiendo metodologías de

cve: BOE-A-2021-7966
Verificable en https://www.boe.es

evaluación reconocidas por el Organismo de Certificación del ENECSTI (Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información), por un organismo acreditado según la norma ISO/IEC 17065.

e) Notificará inmediatamente al órgano supervisor, y en cualquier caso antes de 24 horas desde su conocimiento, cualquier violación de la seguridad o pérdida de integridad que tenga impacto en el servicio.

Asimismo, en caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la Agencia Española de Protección de Datos sin dilación indebida conforme a lo previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016.

Artículo 7. *Requisitos del personal y plan de formación.*

1. El operador encargado de la verificación de la identidad del solicitante de un certificado cualificado mediante identificación remota por vídeo contará con:

a) Formación específica sobre las características verificables por el método de identificación, sus procedimientos, métodos de prueba y métodos comunes de falsificación, con el fin de asegurar que dispone de la capacitación suficiente para detectar potenciales fraudes en el proceso de identificación y en los documentos de identidad contemplados en el artículo 8.

b) Formación sobre la normativa vigente en materia de protección de datos personales y servicios de confianza.

c) Formación en el manejo de la herramienta e interpretación de la información y datos que suministra.

2. El prestador cualificado de servicios electrónicos de confianza dispondrá de un plan de formación que se revisará siempre que se produzca un cambio tecnológico o normativo y, como mínimo, anualmente en lo relativo a sus contenidos y eficacia.

La formación prevista en el apartado anterior, cuya duración no podrá ser inferior a quince horas, se recibirá de forma periódica y como mínimo una vez al año.

Artículo 8. *Requisitos de los documentos de identidad utilizados en el proceso de identificación.*

La identidad del solicitante se acreditará mediante los documentos de identidad previstos en la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Los documentos de identidad utilizados deberán incluir una fotografía y disponer de características de seguridad automáticamente comprobables en el proceso de identificación remota por vídeo de forma que se garantice la detección de falsificaciones y manipulaciones.

Artículo 9. *Requisitos de las instalaciones.*

1. Los servidores y equipamiento que formen parte de los sistemas de información que soportan el proceso de identificación se ubicarán en estancias protegidas, con acceso restringido al personal autorizado. Se controlarán los accesos de forma que solamente pueda accederse por las entradas previstas y vigiladas, y se identificará a todo el personal que acceda a dichas estancias, registrándose las entradas y salidas.

Si los servidores se encuentran ubicados en un país extracomunitario, el prestador cualificado de servicios de confianza deberá garantizar, en la medida en que pueda suponer la existencia de transferencias internacionales de datos, que se cumplan los requisitos establecidos en el capítulo V del Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016.

2. En el caso de que el personal involucrado en el proceso de identificación remota por vídeo desarrolle su actividad en la modalidad de trabajo a distancia, se deberá del

cve: BOE-A-2021-7966
Verificable en https://www.boe.es

mismo modo garantizar la seguridad del proceso, de la información y la protección de datos de conformidad con la normativa aplicable.

Artículo 10. *Condiciones generales del proceso de identificación.*

1. Se informará al solicitante, de manera clara y comprensible, de los términos y condiciones del proceso de identificación remota por vídeo, de las recomendaciones de seguridad aplicables, así como de lo previsto en el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016.

2. Se recabará el consentimiento expreso del solicitante, incluyendo el consentimiento a la grabación íntegra del vídeo y al tratamiento y conservación de categorías especiales de datos personales. En este sentido, se deberá informar al solicitante de otras alternativas existentes para la identificación que no requieran el tratamiento y la conservación de su imagen y sus datos biométricos, incluidas en todo caso las contempladas en el artículo 24.1 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

3. Se adoptarán las medidas adecuadas que garanticen la privacidad de todo el proceso de identificación del solicitante.

4. El proceso de identificación se interrumpirá o no se considerará válido cuando concurra alguna de las siguientes circunstancias:

a) Existan indicios de falsedad, manipulación o falta de validez del documento de identificación.

b) Existan indicios de falta de correspondencia entre el titular del documento y el solicitante.

c) La calidad de la imagen o el sonido impidan o dificulten verificar la autenticidad e integridad del documento de identificación y la correspondencia entre el titular del documento y el solicitante.

d) Las condiciones, seguridad o la calidad de la comunicación impidan o dificulten completar el proceso con la fiabilidad adecuada.

e) Existan indicios de uso de archivos pregrabados.

f) Existan indicios de que para la transmisión de vídeo no se ha utilizado un único dispositivo.

g) Existan indicios de que la transmisión de vídeo no se ha realizado en tiempo real o de que el proceso no se ha realizado en unidad de acto.

h) Existan indicios de que el solicitante está siendo coaccionado o intimidado.

i) Cualquier otra en la que exista una duda razonable sobre la seguridad del proceso de identificación que se está realizando.

5. En caso de que el operador interrumpa o no considere válido el proceso de identificación, se indicará la causa dejando constancia fehaciente en el sistema.

6. Si el proceso de identificación se realiza de forma asistida, el prestador dispondrá de un procedimiento para llevar a cabo la entrevista de identificación del solicitante del certificado y una guía de diálogo para los operadores.

7. Si el proceso de identificación se realiza de forma no asistida, un operador supervisará a posteriori el proceso de identificación grabado y comprobará las pruebas e imágenes generadas por el sistema para aceptar o rechazar la validez del proceso de identificación.

8. El operador de registro deberá basar su decisión de aprobación o denegación de la solicitud de emisión del certificado en la revisión de todas las pruebas recabadas en el proceso de identificación, incluyendo, al menos, el vídeo, la comprobación de caracteres aleatorios enviados al solicitante, la existencia de elementos de seguridad del documento de identidad extraídos del mismo durante el proceso de identificación y la comparación biométrica realizada.

cve: BOE-A-2021-7966
Verificable en https://www.boe.es

Artículo 11. *Requisitos para la verificación de la identidad del solicitante y del documento de identidad.*

1. Se verificará la autenticidad, vigencia e integridad física y lógica del documento de identificación utilizado y la correspondencia del titular del documento con el solicitante.

2. Se tomarán medidas para reducir al mínimo el riesgo de que la identidad del solicitante no coincida con la identidad reclamada, teniendo en cuenta el riesgo de documentos perdidos, robados, suspendidos, revocados o expirados.

3. Durante el proceso de registro, cuando el solicitante presente el Documento Nacional de Identidad (DNI) o el Número de Identidad de Extranjeros (NIE), los prestadores comprobarán los datos de identidad del solicitante, utilizando el número del documento, a través de la plataforma de intermediación del Servicio de Verificación y Consulta de Datos que la Secretaría de Estado de Digitalización e Inteligencia Artificial pone a disposición de los organismos públicos o, en su defecto, a través de la plataforma que el órgano de supervisión pondrá a disposición de los prestadores cualificados que no tengan acceso al citado servicio.

En caso de problemas técnicos vinculados a la plataforma de comprobación y ajenos al prestador, se realizarán al menos tres intentos de consulta y se conservarán las respuestas recibidas, de acuerdo con el artículo 12.5 de esta orden.

4. Se tomarán las medidas adecuadas para detectar una posible manipulación de la imagen de vídeo, del documento de identidad o del solicitante, garantizándose su prueba de vida. Para ello, se implantarán al menos:

a) Medidas procedimentales que hagan patente dicha manipulación con la introducción de un código único, aleatorio e impredecible y de un solo uso generado al efecto y remitido al solicitante. El código constará de un mínimo de seis caracteres o sistema con entropía equivalente. El prestador comprobará que el dispositivo móvil al que se remite el código se encuentra en posesión del usuario durante el proceso de identificación. El órgano supervisor podrá poner a disposición de los prestadores una plataforma tecnológica de verificación de la asociación del usuario con el dispositivo móvil.

b) En el caso de la identificación remota por vídeo asistida, medidas organizativas que hagan patente dicha manipulación a través de la interacción con el documento de identidad utilizado y con el solicitante, según las indicaciones del operador, a través de interacciones y actuaciones físicas que figurarán en un protocolo que incluirá acciones tanto comunes como aleatorias y diferenciadas.

c) En el caso de la identificación remota por vídeo no asistida, el sistema requerirá al solicitante la realización activa de interacciones y actuaciones físicas, que figurarán en un protocolo que incluirá acciones tanto comunes como aleatorias y diferenciadas.

5. En el caso de personas físicas que actúen a través de representante, así como de personas jurídicas se comprobarán los datos relativos a la constitución y personalidad jurídica, o a la persona o entidad representada, así como la extensión y vigencia de las facultades de representación del solicitante de un certificado cualificado, de acuerdo con la legislación aplicable. Esta comprobación se podrá realizar en un proceso distinto a la identificación del solicitante, si bien en cualquier caso de forma previa a la expedición del certificado.

Artículo 12. *Requisitos de la grabación y de conservación de pruebas.*

1. El vídeo realizado, de forma asistida o sin asistencia, se grabará íntegramente y sin interrupciones.

2. Se constatará de manera fehaciente la fecha y hora de la grabación mediante el uso de un sello cualificado de tiempo.

3. Se conservará una copia de la grabación del vídeo durante un periodo mínimo de tiempo de quince años desde la extinción de la vigencia del certificado obtenido por este medio.

cve: BOE-A-2021-7966
Verificable en https://www.boe.es

4. Se conservarán, por un periodo mínimo de tiempo de 15 años, fotos o capturas de pantalla del solicitante y del documento de identidad utilizado, en las que serán claramente reconocibles tanto la persona como el anverso y el reverso del documento de identidad.

5. Se conservará, por un periodo mínimo de tiempo de quince años, el resultado automático de la verificación realizada por la aplicación, así como la evaluación y observaciones realizadas por el operador junto a su decisión de aprobación o rechazo de la identificación.

6. Se conservarán todas las pruebas de los procesos de identificación incompletos que no hayan llegado a término por sospecha de intento de fraude durante un plazo de 5 años desde la ejecución del proceso de identificación, especificándose la causa por la que no llegaron a completarse, de conformidad con la política establecida al efecto.

7. Se garantizará la integridad y autenticidad de la grabación, así como de las otras pruebas obtenidas durante el proceso de identificación remota, mediante la utilización de servicios de confianza cualificados, así como su confidencialidad. La conservación se realizará mediante el bloqueo de los datos, conforme a lo previsto en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

8. La grabación y las imágenes obtenidas durante el proceso de identificación reunirán las condiciones de calidad y nitidez suficientes para garantizar su uso en investigaciones o análisis posteriores.

Disposición transitoria única.

Hasta el 1 de julio de 2022 en que entre en vigor el artículo 6.d), el cumplimiento de los requisitos de seguridad se demostrará mediante otras certificaciones, informes o pruebas en laboratorios o entidades especializadas, que se revisarán por un organismo de evaluación de la conformidad, quien incluirá el resultado en el informe de evaluación de la conformidad.

Disposición final primera. *Título competencial.*

Esta orden se dicta al amparo de las competencias exclusivas que corresponden al Estado en materia de legislación civil, de telecomunicaciones y de seguridad pública, conforme a lo dispuesto en el artículo 149.1. 8.ª, 21.ª y 29.ª de la Constitución Española, respectivamente.

Disposición final segunda. *Entrada en vigor.*

La presente orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado», salvo lo dispuesto en el artículo 6.d) que entrará en vigor el 1 de julio de 2022.

Madrid, 6 de mayo de 2021.–La Vicepresidenta Segunda del Gobierno y Ministra de Asuntos Económicos y Transformación Digital, Nadia Calviño Santamaría.

cve: BOE-A-2021-7966
Verificable en https://www.boe.es