Proyecto de Orden sobre los métodos de identificación no presencial para la expedición de certificados electrónicos cualificados

I

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 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, la disposición final quinta del Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia, que modifica el artículo 13 de la Ley 59/2003, de 19 de diciembre, de firma electrónica habilita a que mediante orden ministerial de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se regulen las condiciones y requisitos técnicos 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 a los solicitantes de certificados cualificados, de forma que puedan seguir expandiendo su actividad y competir con los prestadores de 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.

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

II

En cuanto a las medidas organizativas y procedimentales que deberán implantar los prestadores, es importante señalar que deben ser proporcionadas a los riesgos y 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 específicas de la expedición de certificados cualificados de utilización universal y que constituyen un auténtico *alter ego* digital de la persona, necesidades que no pueden ser satisfechas mediante métodos provenientes de otros sectores o ámbitos particulares con requisitos procedimentales, regulatorios o de seguridad diferentes.

En este sentido, esta orden ministerial especifica el procedimiento que debe seguirse para la identificación no presencial 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. Entre otras medidas, se exige verificar la autenticidad y validez del documento de identidad, así como su correspondencia con el solicitante del certificado. 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 externa al proceso, en línea con las disposiciones del Reglamento de Ejecución (UE) 2015/1502 y la *Guidance for the application of the levels of assurance which support the eIDAS Regulation* elaborada por la Red de Cooperación establecida por la Decisión de Ejecución (UE) 2015/296.

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 o sistemas 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 o sistema de seguridad TIC es el único medio objetivo que permite valorar y acreditar la capacidad de un producto para manejar información de forma segura.

A tal fin, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará, modificará, publicará y mantendrá actualizadas las correspondientes guías técnicas y, en particular, la guía CCN-STIC-140 para la certificación de estos productos o sistemas.

IV

De acuerdo con lo establecido en el artículo 24.1 d) del Reglamento (UE) 910/204, 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 citada 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 publico de la posibilidad de identificarse de manera remota.

V

Esta norma se compone de once artículos y dos disposiciones finales, y se adecúa 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 evolucionable de forma ágil que recoja los requisitos técnicos, organizativos y procedimentales aplicables a los métodos de identificación no presenciales.

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 los adecuados niveles de protección de los usuarios y actividad económica.

En el procedimiento de elaboración de la 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. Si bien se prescindió del trámite de consulta pública de acuerdo con lo previsto en el artículo 26.2 de la Ley 50/1997, de 27 de noviembre, por tratarse de una norma que regula aspectos parciales de una materia, 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, de 27 de noviembre, y se ha sometido al procedimiento de audiencia pública previsto en el artículo 26.6 de dicha 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.

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

La orden ministerial se dicta en virtud de la habilitación para el desarrollo normativo establecida en la disposición final quinta del Real Decreto-ley 28/2020, de 22 de septiembre.

En su virtud, de acuerdo con el Consejo de Estado y al amparo de la habilitación contenida en artículo 13 de la Ley 59/2003, de 19 de diciembre,

DISPONGO:

Artículo 1. *Objeto*.

Esta orden tiene por objeto regular las condiciones y requisitos técnicos mínimos aplicables a la verificación de la identidad, así como de los atributos específicos, de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación distintos a la presencia física que aporten una seguridad equivalente en términos de fiabilidad, de acuerdo con lo previsto en el artículo 13.6 de la Ley 59/2003, de 19 de diciembre, de firma electrónica 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.

Artículo 2. *Ámbito de aplicación.*

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 que tengan un establecimiento permanente situado en España, siempre que ofrezcan servicios no supervisados por la autoridad competente de otro país de la Unión Europea.

La ejecución de los procedimientos de identificación no presencial podrá ser externalizada, manteniendo el prestador que expide el certificado cualificado la plena responsabilidad.

Artículo 3. *Modalidades de la identificación remota por video.*

El proceso de identificación se podrá realizar de forma asistida, con la mediación síncrona de un agente, o de forma no asistida, sin necesidad de interacción en línea del solicitante, con revisión posterior de un agente.

Artículo 4. *Evaluación de la conformidad y comprobación del cumplimiento de requisitos.*

1. El cumplimiento de los requisitos establecidos en la presente orden deberá ser confirmado por un organismo de evaluación de la conformidad acreditado. El organismo de evaluación 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 al órgano supervisor que incluya 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 documentación e información adicionales sobre cualquier aspecto de la solución de identificación remota por video, con carácter previo o posterior a su implantación.

Artículo 5. *Requisitos generales de seguridad*.

El prestador cualificado de servicios electrónicos de confianza:

1. Dispondrá de 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 que pudiera influir en el perfil de riesgo del procedimiento de identificación.

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

3. 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 evidencias producidas durante el proceso de identificación.

4. Empleará un producto o sistema de identificación remota por vídeo que cumpla los requisitos mínimos de seguridad indicados en el anexo de la guía técnica CCN-STIC-140 que elaborará el Centro Criptológico Nacional. El prestador cualificado deberá seguir las indicaciones de configuración y uso seguro del producto.

5. El cumplimiento de lo dispuesto en el apartado anterior deberá ser certificado siguiendo 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), por un organismo acreditado según la norma ISO/IEC 17065.

6. Notificará inmediatamente al órgano supervisor, 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.

Artículo 6. *Requisitos del personal y plan de formación*.

1. El personal encargado de la verificación de la identidad del solicitante de un certificado cualificado mediante identificación remota por video 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 7.

b) Formación sobre la legislación 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.

La citada formación, cuya duración no podrá ser inferior a quince horas, se recibirá por el citado personal de forma periódica, al menos anualmente. En cualquier

caso, se actualizará el aprendizaje siempre que se produzca un cambio tecnológico o legislativo.

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

Artículo 7. *Requisitos de los documentos de identidad utilizados en el proceso de identificación*.

La identificación del solicitante se acreditará mediante el Documento Nacional de Identidad o, en el caso de los extranjeros, mediante Tarjeta de Identidad de Extranjero, pasaporte o documento oficial de identidad extranjero expedido por las autoridades del país de origen, acompañado, en su caso, del Número de Identidad de Extranjero, siempre que incluya una fotografía, cuyas características de seguridad sean comprobables en el proceso de identificación remota por vídeo de forma que se garantice la detección de falsificaciones y manipulaciones.

Artículo 8. *Requisitos de las instalacione*s.

El equipamiento que forme parte de los sistemas de información encargados del proceso de identificación se ubicará en estancias separadas específicas para su función, con acceso protegido, a las que solo tendrá acceso el 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.

Artículo 9. *Condiciones generales del proceso de identificació*n.

1. Se informará al solicitante, de manera clara y comprensible, de los términos y condiciones del proceso de identificación remota por video, así como de las recomendaciones de seguridad aplicables.

2. Se recabará el consentimiento expreso del solicitante, incluyendo el consentimiento a la grabación íntegra del proceso de identificación.

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 y 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 video no se ha utilizado un único dispositivo

g) existan indicios de que la transmisión de video no se ha realizado en tiempo real

5. En caso de que el agente interrumpa o no considere válido el proceso de identificación, se indicará la causa dejando constancia por escrito.

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 agentes.

7. Si el proceso de identificación se realiza de forma no asistida, un agente supervisará a posteriori el proceso de identificación grabado y comprobará las evidencias 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 revisión de todas las evidencias recabadas en el proceso de identificación, incluyendo el vídeo, la comprobación de caracteres aleatorios enviados al solicitante, la existencia de elementos de seguridad del documento de identidad extraidos del mismo durante la realización del video y la comparación biométrica realizada.

Artículo 10. *Requisitos para la verificación de la identidad del solicitante, sus atributos 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 documento de identificación 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 el supuesto de que, por problemas técnicos ajenos al prestador la consulta a la mencionada plataforma no fuese posible, el prestador podrá continuar con el proceso de identificación dejando constancia por escrito de la incidencia.

4. Se tomarán las medidas adecuadas para detectar una posible manipulación de la imagen de video, del documento de identidad o del solicitante. Para ello se implantarán las siguientes medidas:

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 6 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. 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 video 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 agente, a través 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 video 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 su caso, 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.

Artículo 11. *Requisitos de la grabación y de conservación de evidencias.*

1. El proceso de identificación 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 garantizará la integridad, la autenticidad, la confidencialidad y la conservación a largo plazo de la grabación, así como otras evidencias obtenidas durante el proceso de identificación remota, mediante la utilización de servicios de confianza cualificados.

4. Se conservará una copia de la grabación del proceso íntegro de identificación durante un periodo mínimo de tiempo de 15 años desde la extinción de la vigencia del certificado obtenido por este medio.

5. Se conservarán, por el mismo periodo de tiempo, 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.

6. Se conservarán, por el mismo periodo de tiempo, el resultado automático de la verificación realizada por la aplicación, asi como la evaluación y observaciones

realizadas por el agente junto a su decisión de aprobación o rechazo de la identificación.

7. Se conservarán las grabaciones de los procesos de identificación incompletos que no hayan llegado a término por sospecha de intento de fraude durante un mínimo de tiempo de 5 años desde la grabación, especificándose la causa por la que no llegaron a completarse, de conformidad con la política establecida al efecto.

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

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. 8ª, 21ª y 29ª de la Constitución Española, respectivamente.

Disposición final segunda. *Entrada en vigor.*

Esta orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

La obligación establecida en el apartado 5 del artículo 5 relativa a la certificación de la seguridad del producto o sistema de identificación remota por vídeo siguiendo 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), será efectiva desde el 1 de enero de 2022. Hasta esa fecha, el cumplimiento de los requisitos de seguridad se demostrará mediante otras certificaciones, informes o pruebas en laboratorios o entidades especializadas, que se revisarán por el organismo de evaluación de la conformidad, quien incluirá el resultado en el informe de evaluación de la conformidad.