I. DISPOSICIONS GENERALS

MINISTERI D'AFERS ECONÒMICS I TRANSFORMACIÓ DIGITAL

7966 *Ordre ETD/465/2021, de 6 de maig, per la qual es regulen els mètodes d'identificació remota per vídeo per a l'expedició de certificats electrònics qualificats.*

I

El Reglament (UE) 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques al mercat interior i pel qual es deroga la Directiva 1999/93/CE, preveu la possibilitat de verificació de la identitat del sol·licitant d'un certificat qualificat utilitzant altres mètodes d'identificació reconeguts a escala nacional que garanteixin una seguretat equivalent en termes de fiabilitat a la presència física.

L'emergència sanitària generada per la crisi de la COVID-19 ha exigit durant l'estat d'alarma el confinament de la ciutadania i la limitació dràstica dels desplaçaments personals, amb vista a frenar el creixement dels contagis. De manera transitòria i excepcional, a través de la disposició addicional onzena del Reial decret llei 11/2020, de 31 de març, pel qual s'adopten mesures urgents complementàries en l'àmbit social i econòmic per fer front a la COVID-19, es va habilitar un sistema temporal d'identificació remota per a l'obtenció de certificats qualificats, amb la finalitat de contribuir a reduir els desplaçaments dels ciutadans per dur a terme tràmits, sense minvar els seus drets.

Amb la finalitat d'implantar de manera permanent i amb plena seguretat jurídica la possibilitat esmentada, l'article 7.2 de la Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança, habilita que mitjançant una ordre ministerial de la persona titular del Ministeri d'Afers Econòmics i Transformació Digital es determinin les condicions i els requisits tècnics de verificació de la identitat a distància i, si escau, altres atributs específics de la persona sol·licitant d'un certificat qualificat, mitjançant altres mètodes d'identificació com la videoconferència o la videoidentificació que aportin una seguretat equivalent en termes de fiabilitat a la presència física, que permetin la implantació dels mètodes esmentats per part dels prestadors de serveis electrònics de confiança, per raó de les especificitats pròpies d'aquest sector i les obligacions de seguretat a què estan subjectes els prestadors qualificats.

Així mateix, es constata l'existència d'una necessitat, manifestada pels prestadors de serveis electrònics de confiança, de dotar l'ordenament jurídic espanyol d'una norma específica que els permeti utilitzar aquest avantatge competitiu en la provisió dels seus serveis, i que els habiliti per identificar de manera remota per vídeo els sol·licitants de certificats qualificats, de manera que puguin seguir expandint la seva activitat i competir amb els prestadors establerts en altres països que ja disposen d'una normativa nacional a aquest efecte. Sobre això, és destacable que Espanya és el país de la Unió Europea amb un mercat més gran de prestadors de serveis electrònics de confiança, tal com es reflecteix en la Llista espanyola de prestadors qualificats *Trusted Services List*, o TSL), que manté el Ministeri d'Afers Econòmics i Transformació Digital com a òrgan supervisor.

II

Pel que fa a les mesures organitzatives i procedimentals que han d'implantar els prestadors, és important assenyalar que han de ser proporcionals als riscos i adequades a la naturalesa d'aquests serveis, pilars de la construcció d'altres serveis digitals de valor afegit. Sobre això, s'han de tenir en consideració les necessitats procedimentals i de seguretat específiques de l'expedició de certificats qualificats d'utilització universal i que constitueixen un autèntic *alter ego* digital de la persona.

En aquest sentit, aquesta Ordre ministerial especifica el procediment que s'ha de seguir per a la identificació remota per vídeo d'un sol·licitant, així com els requisits i les accions mínimes que han de portar a terme els prestadors per detectar els intents de suplantació d'identitat o les possibles manipulacions de les imatges o les dades del document d'identitat. Aquests mètodes d'identificació remota per vídeo no prejutgen l'existència d'altres sistemes d'identificació a distància emparats per l'article 24.1 del Reglament (UE) 910/2014 esmentat, que no són objecte de regulació en aquesta Ordre.

Entre d'altres mesures, s'exigeix verificar l'autenticitat i la validesa del document d'identitat, així com la seva correspondència amb el sol·licitant del certificat. Per fer-ho, el sistema d'identificació remota per vídeo emprat en el procés ha d'incorporar els mitjans tècnics i organitzatius necessaris per verificar l'autenticitat, la vigència i la integritat dels documents d'identificació utilitzats, verificar la correspondència del titular del document amb el sol·licitant que efectua el procés, mitjançant tecnologies com el reconeixement facial, i verificar que aquest és una persona viva que no està sent suplantada; tots aquests requisits han de quedar acreditats, en els termes que estableix l'annex F11 de la Guia de seguretat de les TIC CCN-STIC-140, del Centre Criptològic Nacional, mitjançant la certificació del producte. La referència a la Guia s'ha d'entendre feta sempre a l'última versió disponible. Així mateix, s'exigeix que el personal encarregat de la verificació de la identitat del sol·licitant verifiqui l'exactitud de les dades del sol·licitant, utilitzant les captures del document d'identitat emprat en el procés, a més de qualsevol altre mitjà automàtic que pugui ser implementat en els sistemes d'identificació remota per vídeo.

Per contribuir a aquesta finalitat, es preveu la posada a disposició dels prestadors de l'accés a la plataforma d'intermediació del Servei de Verificació i Consulta de Dades, l'organisme responsable del qual és la Secretaria d'Estat de Digitalització i Intel·ligència Artificial, com a mitjà de contrastar les dades d'identitat dels sol·licitants amb una font autèntica, en línia amb les disposicions del Reglament d'execució (UE) 2015/1502 de la Comissió, de 8 de setembre de 2015, sobre la fixació d'especificacions i procediments tècnics mínims per als nivells de seguretat de mitjans d'identificació electrònica d'acord amb el que disposa l'article 8, apartat 3, del Reglament (UE) 910/2014 esmentat.

III

Per tal d'acreditar el compliment dels requisits de seguretat exigibles a les eines utilitzades en els processos d'identificació remota, els prestadors han d'utilitzar productes la funcionalitat de seguretat dels quals estigui certificada segons les metodologies d'avaluació reconegudes per l'Organisme de Certificació de l'ENECSTI (Esquema Nacional d'Avaluació i Certificació de la Seguretat de les Tecnologies de la Informació). És important assenyalar que l'avaluació i la certificació d'un producte de seguretat de les tecnologies de la informació i la comunicació (TIC) és l'únic mitjà objectiu que permet valorar i acreditar la capacitat d'un producte per manejar informació de manera segura.

Amb la finalitat d'adaptar-se de manera àgil a l'avanç continu de la tecnologia, aquesta Ordre ministerial fa referència a les guies tècniques corresponents elaborades i actualitzades pel Centre Criptològic Nacional, en relació amb les característiques i els requisits purament tecnològics aplicables als productes i les eines d'identificació remota per vídeo per garantir un nivell adequat de seguretat d'aquests.

De la mateixa manera, s'han de considerar els estàndards que, si s'escau, siguin adoptats en l'àmbit europeu i internacional, en particular per l'Institut Europeu de Normes de Telecomunicacions (ETSI).

Així mateix, aquesta Ordre ministerial s'ha d'aplicar de manera que es compleixin les obligacions del Reglament (UE) 2016/679 del Parlament Europeu i el Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de les seves dades personals i a la lliure circulació d'aquestes dades, i pel qual es deroga la Directiva 95/46/CE, així com la resta de la normativa sobre protecció de dades personals, particularment la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals. Dins de les obligacions de seguretat que aquesta Ordre imposa als prestadors de serveis de confiança, es preveu una anàlisi de riscos que inclogui

les mesures tècniques i organitzatives adequades respecte de les dades personals, de conformitat amb el Reglament (UE) 2016/679 esmentat.

IV

D'acord amb el que estableix l'article 24.1.d) del Reglament (UE) 910/2014, la seguretat equivalent en termes de fiabilitat a la presència física l'ha de confirmar un organisme d'avaluació de la conformitat acreditat, que ha de verificar el compliment dels requisits legals exigits en aquesta Ordre, incloent-hi, durant el període transitori fins a l'obligatorietat de la certificació assenyalada abans, la comprovació del nivell de seguretat del sistema o producte utilitzat pel prestador d'acord amb la guia CCN-STIC-140. Aquesta comprovació s'ha d'efectuar mitjançant l'avaluació d'altres certificacions, informes, proves de laboratori i altres elements aportats pel fabricant. El resultat d'aquesta s'ha de reflectir en l'informe d'avaluació de la conformitat que el prestador qualificat ha de remetre a l'òrgan de supervisió amb caràcter previ a l'oferiment al públic de la possibilitat d'identificar-se de manera remota.

V

Aquesta norma, dictada a l'empara de l'habilitació legal que conté l'article 7.2 de la Llei 6/2020, d'11 de novembre, es compon de dotze articles, una disposició transitòria i dues disposicions finals, i s'adequa als principis de necessitat, eficàcia, proporcionalitat, seguretat jurídica, transparència i eficiència, als quals s'ha de subjectar l'exercici de la potestat reglamentària, de conformitat amb el que disposa l'article 129 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.

Pel que fa als principis de necessitat i eficàcia, aquesta Ordre ministerial és l'instrument òptim per portar a terme el desplegament reglamentari previst, a causa del fet que cal dotar el sector d'una regulació específica i susceptible d'adaptació àgil que reculli els requisits tècnics, organitzatius i procedimentals aplicables als mètodes d'identificació remota per vídeo.

Pel que fa al principi de proporcionalitat, aquesta Ordre ministerial estableix els requisits apropiats exigibles als sistemes d'identificació a distància de manera que es garanteixi la seguretat del tràfic jurídic i el nivell de protecció adequat dels usuaris i l'activitat econòmica.

En el procediment d'elaboració d'aquesta Ordre s'ha tingut en compte el que disposen la Llei 50/1997, de 27 de novembre, del Govern, i la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques. Es va sotmetre el text a consulta prèvia als subjectes directament afectats, en concret, els prestadors qualificats de serveis electrònics de confiança i als organismes d'avaluació de la conformitat acreditats, per tal de garantir l'encert i la legalitat de la norma, d'acord amb l'article 26.1 de la Llei 50/1997; s'ha sotmès al tràmit d'audiència i informació pública que preveu l'article 26.6 de la Llei esmentada, i s'ha possibilitat així la participació activa dels destinataris potencials. En totes dues fases s'han rebut nombroses observacions que s'han tingut en compte en l'elaboració d'aquest text. Per tot això, es considera complert el principi de transparència.

Amb relació al principi d'eficiència, aquesta Ordre ministerial no imposa càrregues administratives innecessàries, i el seu desplegament s'ha produït amb la màxima celeritat possible.

Finalment, s'han sol·licitat informes, de conformitat amb el que preveu l'article 26.5 de la Llei 50/1997, dels departaments ministerials i organismes públics següents: Ministeri de Defensa, Ministeri de l'Interior, Ministeri d'Hisenda, Ministeri de Justícia i Ministeri de Sanitat, així com de l'Agència Espanyola de Protecció de Dades.

En virtut d'això, amb l'aprovació prèvia del ministre de Política Territorial i Funció Pública i d'acord amb el Consell d'Estat, disposo:

Article 1. *Objecte.*

Aquesta Ordre té per objecte regular les condicions i els requisits tècnics mínims aplicables a la verificació de la identitat i, si escau, altres atributs específics, de la persona sol·licitant d'un certificat qualificat mitjançant mètodes d'identificació remota per vídeo d'acord amb el que preveuen l'article 7.2 de la Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança, i l'article 24.1.d) del Reglament (UE) 910/2014, del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques al mercat interior i pel qual es deroga la Directiva 1999/93/CE. Tot això s'entén sense perjudici de l'existència d'altres mètodes d'identificació a distància emparats per l'article 24.1 del Reglament (UE) 910/2014 no inclosos en l'àmbit d'aplicació d'aquesta Ordre.

Article 2. *Àmbit d'aplicació subjectiu.*

Aquesta Ordre s'aplica als prestadors qualificats públics i privats de serveis electrònics de confiança establerts a Espanya.

Així mateix, s'aplica als prestadors qualificats residents o domiciliats en un altre Estat membre que tinguin un establiment permanent situat a Espanya, sempre que ofereixin serveis no supervisats per l'autoritat competent d'un altre Estat membre de la Unió Europea.

L'execució dels procediments d'identificació remota per vídeo es pot externalitzar, i el prestador que expedeix el certificat qualificat manté la plena responsabilitat amb relació a l'aplicació d'aquesta Ordre.

Article 3. *Protecció de dades de caràcter personal.*

Els tractaments de dades de caràcter personal de les persones físiques s'han de fer amb subjecció estricta al que disposa el Reglament (UE) 2016/679 del Parlament Europeu i el Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de les seves dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE, així com a la resta de la normativa sobre protecció de dades personals.

Article 4. *Modalitats d'identificació remota per vídeo.*

El procés d'identificació remota per vídeo es pot fer de manera assistida, amb la mediació síncrona d'un operador, o de manera no assistida, sense necessitat d'interacció en línia entre un operador i el sol·licitant, amb la revisió posterior d'un operador.

Article 5. *Avaluació de la conformitat i comprovació del compliment de requisits.*

1. El compliment dels requisits que estableix aquesta Ordre l'ha de confirmar un organisme d'avaluació de la conformitat acreditat. L'organisme d'avaluació ha de reflectir en l'informe, de manera detallada, com compleix el prestador els requisits definits en aquesta Ordre.

2. El prestador qualificat de serveis de confiança ha de remetre una sol·licitud per a la posada en operació de procediments d'identificació remota per vídeo a la Secretaria d'Estat de Digitalització i Intel·ligència Artificial, dependent del Ministeri d'Afers Econòmics i Transformació Digital, com a òrgan supervisor. La sol·licitud esmentada ha d'incloure una descripció detallada del sistema i la seva operació, la declaració de pràctiques actualitzada, així com l'informe d'avaluació de la conformitat, amb caràcter previ al seu oferiment al públic.

3. L'òrgan supervisor pot requerir al prestador que aporti, en el termini de deu dies hàbils, documentació i informació addicionals sobre qualsevol aspecte de la solució d'identificació remota per vídeo, amb caràcter previ o posterior a la seva implantació.

4. El prestador pot començar a operar mitjançant procediments d'identificació remota per vídeo a partir de la data de notificació de la resolució estimatòria. El termini màxim per resoldre i notificar és de sis mesos, transcorreguts els quals la sol·licitud s'entén desestimada.

5. Per als prestadors que inicïin la seva activitat de prestació de serveis de confiança qualificats amb posterioritat a l'entrada en vigor d'aquesta Ordre, els tràmits a què es refereix aquest article es poden integrar en el procediment de qualificació que regula l'article 21 del Reglament (UE) 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014.

Article 6. *Requisits generals de seguretat.*

El prestador qualificat de serveis electrònics de confiança:

a) Ha de disposar d'un model de gestió contínua del risc que inclou una anàlisi de riscos específica que es revisa amb una periodicitat mínima anual i, en tot cas, sempre que es produeixi un canvi en el sistema, en els procediments organitzatius, en l'estat de la tecnologia, o en qualsevol altre aspecte que pugui influir en el perfil de risc del procediment d'identificació.

Aquesta anàlisi ha de tenir en compte la naturalesa, l'àmbit, el context i els fins del tractament de les dades personals, així com els riscos de diversa probabilitat i gravetat per als drets i les llibertats de les persones físiques de conformitat amb el que exigeix la normativa de protecció de dades personals.

Així mateix, ha de fer una avaluació d'impacte en la protecció de dades personals quan de l'anàlisi duta a terme sigui probable que el tractament representi un alt risc per als drets i les llibertats de les persones, de conformitat amb el que preveu la normativa esmentada.

b) Ha d'adoptar mesures tècniques i organitzatives addicionals a les indicades en aquesta Ordre quan el resultat de l'anàlisi de riscos efectuada així ho requereixi.

Amb relació a les dades de caràcter personal, ha d'adoptar les mesures tècniques i organitzatives apropiades, segons el que estableix l'article 32 del Reglament (UE) 2016/679 del Parlament Europeu i el Consell, de 27 d'abril de 2016.

Aquestes mesures s'han d'actualitzar sense dilació indeguda quan es tingui coneixement de vulnerabilitats que puguin donar lloc a bretxes de seguretat.

c) Ha d'avaluar i documentar les característiques de seguretat del conjunt del sistema, incloent-hi tots els elements substantius de la plataforma d'identificació, els canals de comunicació, i la generació i conservació de proves produïdes durant el procés d'identificació.

d) Ha d'utilitzar un producte d'identificació remota per vídeo que compleixi els requisits mínims de seguretat indicats en l'annex F.11 de la Guia de seguretat de les TIC CCN-STIC-140, del Centre Criptològic Nacional, de categoria alta. El prestador qualificat ha de seguir les indicacions de configuració i ús segur del producte. El compliment d'aquesta obligació ha de ser certificat seguint metodologies d'avaluació reconegudes per l'Organisme de Certificació de l'ENECSTI (Esquema Nacional d'Avaluació i Certificació de la Seguretat de les Tecnologies de la Informació), per un organisme acreditat segons la norma ISO/IEC 17065.

e) Ha de notificar immediatament a l'òrgan supervisor, i en tot cas abans de 24 hores des del seu coneixement, qualsevol violació de la seguretat o pèrdua d'integritat que tingui impacte en el servei.

Així mateix, en cas de violació de la seguretat de les dades personals, el responsable del tractament l'ha de notificar a l'Agència Espanyola de Protecció de Dades sense dilació indeguda de conformitat amb el que preveu el Reglament (UE) 2016/679 del Parlament Europeu i el Consell, de 27 d'abril de 2016.

Article 7. *Requisits del personal i pla de formació.*

1. L'operador encarregat de la verificació de la identitat del sol·licitant d'un certificat qualificat mitjançant identificació remota per vídeo ha de disposar de:

a) Formació específica sobre les característiques verificables pel mètode d'identificació, els seus procediments, mètodes de prova i mètodes comuns de falsificació, amb la finalitat d'assegurar que disposa de la capacitació suficient per detectar fraus potencials en el procés d'identificació i en els documents d'identitat que preveu l'article 8.

b) Formació sobre la normativa vigent en matèria de protecció de dades personals i serveis de confiança.

c) Formació en el maneig de l'eina i la interpretació de la informació i les dades que subministra.

2. El prestador qualificat de serveis electrònics de confiança ha de disposar d'un pla de formació que s'ha de revisar sempre que es produeixi algun canvi tecnològic o normatiu i, com a mínim, anualment pel que fa als seus continguts i a la seva eficàcia.

La formació que preveu l'apartat anterior, la durada de la qual no pot ser inferior a quinze hores, s'ha de rebre de manera periòdica i almenys una vegada l'any.

Article 8. *Requisits dels documents d'identitat utilitzats en el procés d'identificació.*

La identitat del sol·licitant s'ha d'acreditar mitjançant els documents d'identitat que preveu la Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança. Els documents d'identitat utilitzats han d'incloure una fotografia i disposar de característiques de seguretat comprovables automàticament en el procés d'identificació remota per vídeo, de manera que es garanteixi la detecció de falsificacions i manipulacions.

Article 9. *Requisits de les instal·lacions.*

1. Els servidors i l'equipament que formin part dels sistemes d'informació que suporten el procés d'identificació s'han d'ubicar en estances protegides, amb accés restringit al personal autoritzat. S'han de controlar els accessos de manera que només s'hi pugui accedir per les entrades previstes i vigilades, i s'ha d'identificar tot el personal que accedeixi a les estances esmentades, i registrar-ne les entrades i sortides.

Si els servidors són ubicats en un país extracomunitari, el prestador qualificat de serveis de confiança ha de garantir, en la mesura que pugui comportar l'existència de transferències internacionals de dades, que es compleixin els requisits que estableix el capítol V del Reglament (UE) 2016/679 del Parlament Europeu i el Consell, de 27 d'abril de 2016.

2. En cas que el personal involucrat en el procés d'identificació remota per vídeo dugui a terme la seva activitat en la modalitat de treball a distància, igualment s'ha de garantir la seguretat del procés, de la informació i la protecció de dades de conformitat amb la normativa aplicable.

Article 10. *Condicions generals del procés d'identificació.*

1. S'ha d'informar el sol·licitant, de manera clara i comprensible, dels termes i les condicions del procés d'identificació remota per vídeo, de les recomanacions de seguretat aplicables, així com del que preveu l'article 13 del Reglament (UE) 2016/679 del Parlament Europeu i el Consell, de 27 d'abril de 2016.

2. S'ha de recaptar el consentiment exprés del sol·licitant, incloent-hi el consentiment a la gravació íntegra del vídeo i al tractament i a la conservació de categories especials de dades personals. En aquest sentit, s'ha d'informar el sol·licitant d'altres alternatives per a la identificació que no requereixin el tractament i la conservació de la seva imatge i les

seves dades biomètriques, incloses en tot cas les que preveu l'article 24.1 del Reglament (UE) 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014.

3. S'han d'adoptar les mesures adequades que garanteixin la privacitat de tot el procés d'identificació del sol·licitant.

4. El procés d'identificació s'ha d'interrompre o no s'ha de considerar vàlid quan hi concorri alguna de les circumstàncies següents:

a) Que hi hagi indicis de falsedat, manipulació o falta de validesa del document d'identificació.

b) Que hi hagi indicis de falta de correspondència entre el titular del document i el sol·licitant.

c) Que la qualitat de la imatge o el so impedeixin o dificultin verificar l'autenticitat i la integritat del document d'identificació i la correspondència entre el titular del document i el sol·licitant.

d) Que les condicions, la seguretat o la qualitat de la comunicació impedeixin o dificultin completar el procés amb la fiabilitat adequada.

e) Que hi hagi indicis d'ús d'arxius pregravats.

f) Que hi hagi indicis que per a la transmissió de vídeo no s'ha utilitzat un únic dispositiu.

g) Que hi hagi indicis que la transmissió de vídeo no s'ha efectuat en temps real o que el procés no s'ha efectuat en unitat d'acte.

h) Que hi hagi indicis que el sol·licitant està sent coaccionat o intimidat.

i) Qualsevol altra en què hi hagi un dubte raonable sobre la seguretat del procés d'identificació que s'està efectuant.

5. En cas que l'operador interrompi o no consideri vàlid el procés d'identificació, se n'ha d'indicar la causa i deixar-ne constància fefaent en el sistema.

6. Si el procés d'identificació s'efectua de manera assistida, el prestador ha de disposar d'un procediment per portar a terme l'entrevista d'identificació del sol·licitant del certificat i d'una guia de diàleg per als operadors.

7. Si el procés d'identificació s'efectua de manera no assistida, un operador ha de supervisar *a posteriori* el procés d'identificació gravat i ha de comprovar les proves i les imatges generades pel sistema per acceptar o rebutjar la validesa del procés d'identificació.

8. L'operador de registre ha de basar la seva decisió d'aprovació o denegació de la sol·licitud d'emissió del certificat en la revisió de totes les proves recaptades en el procés d'identificació, incloent-hi, almenys, el vídeo, la comprovació de caràcters aleatoris enviats al sol·licitant, l'existència d'elements de seguretat del document d'identitat que s'hagin extret d'aquest durant el procés d'identificació i la comparació biomètrica efectuada.

Article 11. *Requisits per a la verificació de la identitat del sol·licitant i del document d'identitat.*

1. S'ha de verificar l'autenticitat, la vigència i la integritat física i lògica del document d'identificació utilitzat i la correspondència del titular del document amb el sol·licitant.

2. S'han de prendre mesures per reduir al mínim el risc que la identitat del sol·licitant no coincideixi amb la identitat reclamada, i s'ha de tenir en compte el risc de documents perduts, robats, suspesos, revocats o expirats.

3. Durant el procés de registre, quan el sol·licitant presenti el document nacional d'identitat (DNI) o el número d'identitat d'estranger (NIE), els prestadors han de comprovar les dades d'identitat del sol·licitant, utilitzant el número del document, a través de la plataforma d'intermediació del Servei de Verificació i Consulta de Dades que la Secretaria d'Estat de Digitalització i Intel·ligència Artificial posa a disposició dels organismes públics o, si no n'hi ha, a través de la plataforma que l'òrgan de supervisió ha de posar a disposició dels prestadors qualificats que no tinguin accés al Servei esmentat.

En cas de problemes tècnics vinculats a la plataforma de comprovació i aliens al prestador, s'han de fer almenys tres intents de consulta i s'han de conservar les respostes rebudes, d'acord amb l'article 12.5 d'aquesta Ordre.

4. S'han de prendre les mesures adequades per detectar una possible manipulació de la imatge de vídeo, del document d'identitat o del sol·licitant, en què se'n garanteixi la prova de vida. Per fer-ho, s'han d'implantar, almenys:

a) Mesures procedimentals que facin patent la manipulació esmentada amb la introducció d'un codi únic, aleatori i impredictible i d'un sol ús generat a aquest efecte i remès al sol·licitant. El codi ha de constar d'un mínim de sis caràcters o d'un sistema amb una entropia equivalent. El prestador ha de comprovar que el dispositiu mòbil al qual es remet el codi està en possessió de l'usuari durant el procés d'identificació. L'òrgan supervisor pot posar a disposició dels prestadors una plataforma tecnològica de verificació de l'associació de l'usuari amb el dispositiu mòbil.

b) En el cas de la identificació remota per vídeo assistida, mesures organitzatives que facin patent la manipulació esmentada a través de la interacció amb el document d'identitat utilitzat i amb el sol·licitant, segons les indicacions de l'operador, a través d'interaccions i actuacions físiques que han de figurar en un protocol que ha d'incloure accions tant comunes com aleatòries i diferenciades.

c) En el cas de la identificació remota per vídeo no assistida, el sistema ha de requerir al sol·licitant l'execució activa d'interaccions i actuacions físiques, que han de figurar en un protocol que ha d'incloure accions tant comunes com aleatòries i diferenciades.

5. En el cas de persones físiques que actuïn a través d'un representant, així com de persones jurídiques, s'han de comprovar les dades relatives a la constitució i personalitat jurídica, o a la persona o entitat representada, així com l'extensió i la vigència de les facultats de representació del sol·licitant d'un certificat qualificat, d'acord amb la legislació aplicable. Aquesta comprovació es pot dur a terme en un procés diferent a la identificació del sol·licitant, si bé en tot cas de manera prèvia a l'expedició del certificat.

Article 12. *Requisits de la gravació i de conservació de proves.*

1. El vídeo que es faci, de manera assistida o sense assistència, s'ha de gravar íntegrament i sense interrupcions.

2. S'han de constatar de manera fefaent la data i l'hora de la gravació mitjançant l'ús d'un segell qualificat de temps.

3. S'ha de conservar una còpia de la gravació del vídeo durant un període mínim de temps de quinze anys des de l'extinció de la vigència del certificat obtingut per aquest mitjà.

4. S'han de conservar, per un període mínim de temps de 15 anys, fotos o captures de pantalla del sol·licitant i del document d'identitat utilitzat, en què han de ser clarament recognoscibles tant la persona com l'anvers i el revers del document d'identitat.

5. S'ha de conservar, per un període mínim de temps de quinze anys, el resultat automàtic de la verificació efectuada per l'aplicació, així com l'avaluació i les observacions fetes per l'operador juntament amb la seva decisió d'aprovació o de rebuig de la identificació.

6. S'han de conservar totes les proves dels processos d'identificació incomplets que no hagin arribat a terme per sospita d'intent de frau durant un termini de 5 anys des de l'execució del procés d'identificació, i s'ha d'especificar la causa per la qual no es van arribar a completar, de conformitat amb la política que s'estableixi a aquest efecte.

7. S'han de garantir la integritat i l'autenticitat de la gravació, així com de les altres proves obtingudes durant el procés d'identificació remota, mitjançant la utilització de serveis de confiança qualificats, així com la seva confidencialitat. La conservació s'ha de fer mitjançant el bloqueig de les dades, de conformitat amb el que preveu l'article 32 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

8. La gravació i les imatges obtingudes durant el procés d'identificació han de complir les condicions de qualitat i nitidesa suficients per garantir-ne l'ús en investigacions o anàlisis posteriors.

Disposició transitòria única.

Fins a l'1 de juliol de 2022, en què entra en vigor l'article 6.d), el compliment dels requisits de seguretat s'ha de demostrar mitjançant altres certificacions, informes o proves en laboratoris o entitats especialitzades, que ha de revisar un organisme d'avaluació de la conformitat, que n'ha d'incloure el resultat en l'informe d'avaluació de la conformitat.

Disposició final primera. *Títol competencial.*

Aquesta Ordre es dicta a l'empara de les competències exclusives que corresponen a l'Estat en matèria de legislació civil, de telecomunicacions i de seguretat pública, de conformitat amb el que disposa l'article 149.1. 8a, 21a i 29a de la Constitució espanyola, respectivament.

Disposició final segona. *Entrada en vigor.*

Aquesta Ordre entra en vigor l'endemà de la publicació en el «Butlletí Oficial de l'Estat», llevat del que disposa l'article 6.d) que entra en vigor l'1 de juliol de 2022.

Madrid, 6 de maig de 2021.– La vicepresidenta segona del Govern i ministra d'Afers Econòmics i Transformació Digital, Nadia Calviño Santamaría.