Despacho 154/2017

Identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a videoconferência

O Gabinete Nacional de Segurança (GNS), no âmbito das suas atribuições de Entidade Supervisora, nos termos descritos no artigo 17.º do REGULAMENTO (UE) N.º 910/2014 DO PARLAMENTO EUROPEU E DO CONSELHO de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno, que revoga a Diretiva 1999/93/CE (Regulamento eIDAS), vem por este meio definir os requisitos e instruções no que concerne ao consignado na alínea d) no n.º 1 do artigo 24.º do referido Regulamento, e que diz respeito à possibilidade dos prestadores qualificados de serviços de confiança, adotarem formas de identificação não presencial, que deem garantias equivalentes, em termos de confiança, à da presença física.

Para os efeitos deste despacho, adota-se a definição de "videoconferência", a que é dada pelo Banco de Portugal e que consta do n.º 1 do artigo 1.º ao anexo A da Instrução n.º 9/2017, ínsito no seu Boletim Oficial n.º 6/2017 Suplemento, de 3 de julho de 2017.

Considerando-se que, apesar da separação física, é adequada a identificação por videoconferência, uma vez que a perceção sensorial das pessoas que participam do processo de identificação, a pessoa a ser identificada e o funcionário que procede à identificação, ficam em contacto direto, através da transmissão de vídeo em tempo real.

Considerando-se que a identificação nestes casos se baseia nos requisitos gerais de identificação definidas para pessoas físicas de acordo com estabelecido na alínea a) do n.º 1 do artigo 24.º do Regulamento eIDAS.

Nestes termos, o GNS vem por este meio definir o seguinte:

1. Fica estabelecido que a avaliação da conformidade dos procedimentos de identificação à distância, através de videoconferência, para os efeitos definidos na alínea d) do n.º 1 do artigo 24.º do Regulamento eIDAS pressupõe o cumprimento cumulativo dos requisitos definidos no Anexo A.

2. O presente despacho tem dois anexos (A e B), que dele fazem parte integrante.

3. O presente despacho entra em vigor no dia seguinte ao da sua assinatura.

Lisboa, 5 de dezembro de 2017

O Diretor-Geral

António José Gameiro Marques

Assinado de forma digital por António José Gameiro Marques
Dados: 2017.12.05 18:32:03 Z

António Gameiro Marques

CALM

Anexo A

Requisitos para os procedimentos e sistemas de identificação por videoconferência

1. Identificação por funcionários treinados

1.1. Identificação através de videoconferência só pode ser realizada por funcionários devidamente treinados, formalmente designados com as funções de confiança de administrador e/ou operador de registo, que integrem a estrutura de pessoal do prestador qualificado de serviços de confiança.

1.2. Estes funcionários devem ter formação periódica nas áreas da fraude e falsificação de documentos de identificação.

2. Instalações

O processo de identificação deve ser efetuado em local com acesso restrito, em espaço físico autónomo, que permita garantir uma gravação adequada e a qualidade da videoconferência.

3. Consentimento

3.1. Antes da identificação por videoconferência, a pessoa a ser identificada deve dar seu consentimento explícito a todo o processo de identificação, bem como a captação de fotografias e/ou captura de imagens dos próprios e do seu documento de identificação.

3.2. Esse consentimento deve ser registrado e gravado.

4. Requisitos técnicos e organizacionais

4.1. A identificação por videoconferência deve ser realizada em tempo real e sem interrupções/pausas.

4.2. A integridade e confidencialidade da comunicação audiovisual entre o funcionário e a pessoa a identificar devem ser devidamente asseguradas, através da utilização de sessões de vídeo protegidas com criptografa "ponta-a-ponta".

4.3. A gravação deve conter a indicação da respetiva data e hora.

4.4. A qualidade da comunicação deve ser adequada para permitir a identificação clara dos elementos e características de segurança do documento de identificação. Para avaliar a qualidade da transmissão das imagens, as estruturas guilhoché[1] e/ou o *microlettering* do documento de identificação avaliado devem ser perfeitamente visualizadas e com elevado grau de definição.

4.5. O sistema deve reconhecer e interpretar a *machine-readable zone* (MRZ) do documento de identificação.

4.6. O prestador qualificado de serviços de confiança deve implementar diversos procedimentos escritos sequenciais (scripts) para condução dos processos de identificação por videoconferência, pelo funcionário.

4.7. O prestador qualificado de serviços de confiança deve disponibilizar publicamente a lista completa dos documentos de identificação aceites para os efeitos previstos neste Despacho.

5. Documentos de identificação permitidos

Apenas são permitidos documentos de identificação com características de segurança elevadas, claramente identificáveis e de acordo com os requisitos definidos no ponto seguinte, do qual constem a fotografia e a assinatura do titular do mesmo, emitido por autoridade pública competente.

6. Caraterísticas e elementos de segurança do documento de identificação

Dependendo do tipo de documento, os recursos de segurança ótica podem incluir:

a. Características difrativas: Hologramas e *Identigrams*;

b. Tecnologias de personalização: *Multiple Laser Image* (MLI) e tipografia segura;

c. Material: Fio de segurança personalizado e tintas opticamente variável;

d. Impressão de segurança: *Microlettering* e estruturas guilhoché.

[1] Estrutura de ornato composto de traços ondeados que se cruzam e entrelaçam com simetria, comummente utilizado em documentos de identificação.

7. Procedimentos para verificação do documento de identificação

7.1. O funcionário deve verificar o estado do documento de identificação, garantindo que não está danificado.

7.2. O funcionário deve verificar o estado do documento de identificação, garantindo que não foi manipulado e, em particular, que não possui uma foto sobreposta.

7.3. O funcionário deve verificar que o documento de identificação utilizado contém os recursos de segurança ótica visivelmente identificáveis.

7.4. O funcionário deve solicitar à pessoa a identificar para inclinar o documento horizontalmente e/ou verticalmente na frente da câmara.

7.5. O funcionário deve verificar pelo menos três elementos de segurança (de diferentes categorias) dos referidos no ponto anterior.

7.6. O funcionário deve verificar outros elementos, tais como: o *layout* do cartão, o número, tamanho e espaçamento de caracteres e fonte tipográfica, em comparação com o espécime do documento em análise.

7.7. O funcionário deve verificar o conteúdo das características individuais encontradas no documento, nomeadamente, a comparação de fotos primárias e secundárias (*Identigram*)

8. Verificação da pessoa a ser identificada

8.1. O funcionário deve certificar-se que a fotografia e a descrição pessoal no documento de identificação usado correspondem à pessoa a ser identificada.

8.2. O funcionário deve certificar-se sobre a veracidade da informação contida no documento de identificação;

8.3. O funcionário deve certificar-se sobre a veracidade da informação fornecida pela pessoa durante a entrevista.

8.4. O tipo e sequência das questões efetuadas pelo funcionário não pode ser idêntica em sessões de identificação consecutivas.

8.5. O funcionário deve efetuar a verificação cruzada entre a informação fornecida pela pessoa identificada e a informação resultante do cálculo automático da leitura dos caracteres da MRZ.

9. Interrupção do processo de identificação de vídeo

9.1. Caso não se verifiquem as condições técnicas necessárias à boa condução do processo de comprovação da identificação, nomeadamente: nos casos de existência de fraca qualidade de imagem, de condições deficientes de luminosidade ou som, ou de interrupções na transmissão do vídeo; a videoconferência deve ser interrompida e considerada sem efeito.

9.2. Sempre que o documento de identificação apresentado durante a videoconferência ofereça dúvidas quanto ao seu teor, autenticidade, atualidade, exatidão ou suficiência, a videoconferência não produz os efeitos de comprovação dos elementos identificativos a que se destina.

9.3. Sempre que, durante a videoconferência, existam suspeitas quanto à veracidade dos elementos de identificação, a videoconferência não produz os efeitos de comprovação dos elementos identificativos a que se destina.

10. Transmissão de um de fator de autenticação secundário

10.1. Durante a videoconferência deve ser enviado ao cliente um código único descartável (One Time Password (OTP)) de duração limitada, especialmente produzido para este efeito, gerada centralmente e enviada para a pessoa a identificar (por e-mail ou SMS).

10.2. O procedimento de identificação é concluído, depois do OTP ser devolvido e considerado bem-sucedido pelo sistema.

11. Retenção e gravação

Todo o processo de identificação de vídeo, em todos os seus passos individuais, deve ser registado e mantido pelo TSP pelo período legalmente previsto para os prestadores qualificados de serviços de confiança

12. Proteção de dados

Os prestadores de serviços de confiança devem cumprir todas as disposições legais relativas à matéria da proteção de dados pessoais.

Anexo B

Certificação dos procedimentos e sistemas de identificação por videoconferência

O prestador de serviços de confiança, que pretenda passar a identificar pessoas físicas através de procedimentos de identificação à distância com recurso a videoconferência, de acordo com o previsto na alínea d) no n.º 1 do artigo 24.º do regulamento eIDAS, deve apresentar à entidade supervisora um relatório de avaliação da conformidade emitido por um organismo de avaliação da conformidade que ateste o cumprimento dos requisitos previstos no Anexo A deste despacho.