

PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança

Despacho n.º 2705/2021

Sumário: Identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a sistemas biométricos automáticos de reconhecimento facial.

Identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a sistemas biométricos automáticos de reconhecimento facial

O Programa do XXII Governo Constitucional identifica como um dos desafios estratégicos a promoção de incentivos da sociedade digital, da criatividade e da inovação, privilegiando a simplificação administrativa, o reforço e a melhoria dos serviços prestados digitalmente pelo Estado, o seu acesso e usabilidade, a par da desmaterialização de mais procedimentos administrativos.

O 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, veio considerar que:

Criar confiança no ambiente em linha é fundamental para o desenvolvimento económico e social. A falta de confiança, nomeadamente devido à perceção de incerteza jurídica, leva os consumidores, as empresas e as autoridades públicas a hesitarem em realizar transações por via eletrónica e em adotar novos serviços.

É fundamental reforçar a confiança nas transações eletrónicas no mercado interno criando uma base comum para a realização de interações eletrónicas em condições seguras entre os cidadãos, as empresas e as autoridades públicas, aumentando assim a eficácia dos serviços públicos e privados em linha, os negócios eletrónicos e o comércio eletrónico na União.

O citado Regulamento prevê que, para a emissão de certificados qualificados, possam ser utilizados outros métodos de identificação reconhecidos a nível nacional que deem garantias equivalentes, em termos de confiança, à da presença física.

O Gabinete Nacional de Segurança (GNS), atento à evolução da robustez das tecnologias de identificação à distância, considera que, apesar da separação física e desde que sejam implementados os mecanismos de segurança necessários, estas tecnologias permitem igualar, ou até mesmo incrementar, a capacidade humana na avaliação e verificação da identidade de pessoas, pelo que, na qualidade de Entidade Supervisora Nacional, designada nos termos do n.º 1 do artigo 17.º do Regulamento acima referido, vem definir requisitos e instruções, relativamente à possibilidade dos prestadores qualificados de serviços de confiança adotarem formas de identificação não presencial, com garantias equivalentes, em termos de confiança, à da presença física.

Na definição dos requisitos de segurança estabelecidos neste despacho, foi objetivo principal a mitigação, de forma substancial, dos riscos conhecidos e ataques mais comuns a este tipo de sistemas.

As linhas fundamentais que permitem mitigar o risco para níveis aceitáveis e atestar que a identificação por sistemas biométricos automáticos de reconhecimento facial iguala a capacidade humana na avaliação da verificação da identidade de pessoas à distância, são as seguintes:

Que a pessoa que está, em tempo real, a efetuar o pedido é titular do documento de identificação exigido para o efeito e que os sistemas de “detecção de vida” (*liveness detection*) são certificados e sujeitos a testes com a respetiva aprovação por laboratório acreditado por norma internacionalmente reconhecida;

Que a comparação biométrica facial é efetuada com base nos dados biométricos do cidadão, em conformidade com normas internacionalmente reconhecidas, dados estes que foram recolhidos presencialmente pela autoridade nacional responsável pela emissão do documento de identificação no momento da sua emissão;

Que o documento de identificação apresentado é autêntico, exigindo uma avaliação aprofundada ao mesmo, regra geral, com recurso a tecnologia de inteligência artificial e de *deep learning*, por forma a assegurar que se trata de um documento oficial, fidedigno e que pertence ao próprio.

Face ao exposto e ao abrigo das competências como Entidade Supervisora, previstas 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, cuja execução na ordem jurídica interna foi assegurada pelo Decreto-Lei n.º 12/2021, de 9 de fevereiro, determino o seguinte:

1 — Os procedimentos de **identificação à distância, através de sistemas biométricos automáticos de reconhecimento facial**, para os efeitos definidos na alínea d) do n.º 1 do artigo 24.º do mesmo Regulamento, requer o cumprimento integral dos requisitos definidos no Anexo A ao presente despacho, através de uma avaliação da conformidade, nos termos definidos no Anexo B.

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

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

19 de fevereiro de 2021. — O Diretor-Geral do GNS, *António Gameiro Marques*, CALM.

ANEXO A

Requisitos para os procedimentos e sistemas biométricos automáticos de reconhecimento facial

1 — Definições:

Template biométrico	Nos termos do vocabulário biométrico normalizado, o template biométrico é um “biometric template”, nos termos definidos no ponto 3.3.22, da norma ISO/IEC 2382-37 (referência [11]).
Referência biométrica Oficial (RBO)	É um template biométrico, obtido a partir da imagem facial de alta definição, que consta nos registos oficiais do cidadão obtida pela(s) autoridade(s) competente(s), de forma presencial, no momento do pedido e atribuição do documento de identificação civil, em conformidade com as especificações estabelecidas na norma ISO/IEC 19794-5 (referência [6]). Nos termos do vocabulário biométrico normalizado, a RBO é uma “biometric reference”, nos termos definidos no ponto 3.3.16, da norma ISO/IEC 2382-37 (referência [11]).
Template biométrico TBID	O TBID é uma amostra biométrica, obtida a partir da fotografia do subscritor que consta no seu documento de identificação oficial, em conformidade com as especificações estabelecidas na norma ISO/IEC 19794-5 (referência [6]). Nos termos do vocabulário biométrico normalizado, o TBID é uma “biometric probe”, nos termos definidos no ponto 3.3.14, da norma ISO/IEC 2382-37 (referência [11]).
Template biométrico TBL	O TBL é uma amostra biométrica, obtida a partir da fotografia de alta definição (selfie) recolhida no processo de deteção de prova de vida, em conformidade com as especificações estabelecidas na norma ISO/IEC 19794-5 (referência [6]). Nos termos do vocabulário biométrico normalizado, o TBL é uma “biometric probe”, nos termos definidos no ponto 3.3.14, da norma ISO/IEC 2382-37 (referência [11]).
Documento de Identificação Oficial (DIO).	É o documento, emitido por entidade competente, que permite provar a identidade do cidadão, perante qualquer entidade pública ou privada, nacional, ou no estrangeiro.
Dados Oficiais do Cidadão (DOC) . . .	Informação eletrónica, obtida de forma segura e autêntica, que inclui a seguinte informação do cidadão: dados biográficos, imagem facial (RBO) e informação de emissão do documento de identificação. Esta informação é recolhida pelas autoridades nacionais competentes pela emissão do documento de identificação, de forma presencial.



Verificação biométrica 1:1	<p>É um processo de comparação biométrica de um-para-um (1:1) que se realiza efetuando a comparação entre a amostra biométrica recolhida no momento, que irá ser comparada com a referência biométrica existente, previamente registada e que consta nos sistemas da entidade. Se os resultados da comparação biométrica coincidirem (nos termos definidos), o utilizador é “verificado” positivamente.</p> <p>Nos termos do vocabulário biométrico normalizado, a verificação biométrica 1:1 é uma “biometric verification”, nos termos definidos no ponto 3.8.3, da norma ISO/IEC 2382-37 (referência [11]).</p>
Sujeito biométrico	<p>É uma pessoa que se submete a um processo de captura biométrica.</p> <p>Nos termos do vocabulário biométrico normalizado, é um “biometric capture subject”, nos termos definidos no ponto 3.7.3, da norma ISO/IEC 2382-37 (referência [11]).</p>
Impostor biométrico	<p>É um sujeito biométrico subversivo, que desenvolve ataques biométricos.</p> <p>Nos termos do vocabulário biométrico normalizado, é um “biometric impostor”, nos termos definidos no ponto 3.7.13, da norma ISO/IEC 2382-37 (referência [11]).</p>
Falsa correspondência	<p>É uma comparação biométrica entre uma amostra biométrica (impostor biométrico) e uma referência biométrica (genuína) provenientes de diferentes sujeitos biométricos, à qual, <u>erradamente</u> é atribuída uma correspondência positiva (Match).</p> <p>Nos termos do vocabulário biométrico normalizado, é um “false match”, nos termos definidos no ponto 3.9.8, da norma ISO/IEC 2382-37 (referência [11]).</p>
Taxa de falsas correspondências (FMR)	<p>É a proporção (regra geral em percentagem) de falsas correspondências, em relação ao universo de comparações biométricas realizadas.</p> <p>Nos termos do vocabulário biométrico normalizado, é um “false match rate”, nos termos definidos no ponto 3.9.9, da norma ISO/IEC 2382-37 (referência [11]).</p>
Falsa não-correspondência	<p>É uma comparação biométrica entre uma amostra biométrica (genuína) e uma referência biométrica (genuína) provenientes do mesmo sujeito biométrico, à qual, <u>erradamente</u> é atribuída uma não correspondência (No Match).</p> <p>Nos termos do vocabulário biométrico normalizado, é um “false non-match”, nos termos definidos no ponto 3.9.10, da norma ISO/IEC 2382-37 (referência [11]).</p>
Taxa de falsas não-correspondências (FNMR).	<p>É a proporção (regra geral em percentagem) de falsas não correspondências, em relação ao universo de comparações biométricas realizadas.</p> <p>Nos termos do vocabulário biométrico normalizado, é um “false non-match rate”, nos termos definidos no ponto 3.9.11, da norma ISO/IEC 2382-37 (referência [11]).</p>
Taxa de falhas na aquisição (FTAR)	<p>É a proporção (regra geral em percentagem) das tentativas de aquisição em que o sistema falha para produzir uma amostra com qualidade suficiente.</p> <p>Nos termos do vocabulário biométrico normalizado, é um “failure-to-acquire rate”, nos termos definidos no ponto 3.9.4, da norma ISO/IEC 2382-37 (referência [11]).</p>
Artefacto	<p>É um objeto ou representação artificial que apresenta uma cópia das características ou padrões biométricos de um indivíduo.</p> <p>Nos termos do vocabulário biométrico normalizado, é um “artefact”, nos termos definidos no ponto 3.1, da norma ISO/IEC 30107-1 (referência [7]).</p>
Prova de vida	<p>Representa o estado de “estar vivo”, em tempo real. É evidenciado por características anatómicas, reações involuntárias e voluntárias, funções fisiológicas ou comportamentos.</p> <p>Nos termos do vocabulário biométrico normalizado, é “liveness”, nos termos definidos no ponto 3.2, da norma ISO/IEC 30107-1 (referência [7]).</p>
Deteção de prova de vida.	<p>É a medição e análise de características anatómicas ou reações (involuntárias ou voluntárias) do sujeito, de modo a determinar se a amostra biométrica que está a ser recolhida em tempo real, pertence a uma pessoa.</p> <p>Nos termos do vocabulário biométrico normalizado, é “liveness detection”, nos termos definidos no ponto 3.3, da norma ISO/IEC 30107-1 (referência [7]).</p>



Subscritor	Nos termos deste despacho é a pessoa que solicita serviço e se submete ao processo de verificação biométrica. O subscritor é um “biometric applicant” e um 3.7.3 “biometric capture subject”, nos termos definidos no ponto 3.7.1 e 3.7.3, da norma ISO/IEC 2382-37 (referência [11]).
DMZ	No âmbito da segurança informática, uma DMZ (<i>demilitarized zone</i>), é um segmento de rede (física ou lógica) que separa através de firewall(s), uma rede interna (confiável) de uma rede pública (não confiável). Este segmento de rede pode ter um ou mais dispositivos/sistemas. Regra geral, neste segmento estão colocados os serviços expostos ao exterior, limitando assim o potencial dano em caso de comprometimento de algum destes serviços por um atacante.
Deep learning	É um ramo da inteligência artificial (AI), assente em sistemas/redes com capacidade de aprender com os dados, identificar padrões e tomar decisões com o mínimo de intervenção humana.

2 — Acrónimos:

APCER	Attack presentation classification error rate.
BPCER	Bona fide presentation classification error rate.
BPD	Boundary protection device.
CC	Common Criteria for Information Technology Security Evaluation.
CSP	Cloud Service Provider.
DMZ	Demilitarized zone.
DOVID	Diffraction Optically Variable Image Device.
EAL	Evaluation Assurance Level.
eMRTD	Electronic Machine-Readable Travel Document.
FMR	False Match(ing) Rate.
FNMR	False Non-Match(ing) Rate.
FRVT	Face Recognition Vendor Test.
FTAR	failure-to-acquire rate.
IARPA	Intelligence Advanced Research Projects Activity.
ICAO	International Civil Aviation Organization.
IPSEC	Internet Protocol Security.
MLI	Multiple Laser Image.
MRZ	Machine Readable Zone.
NIST	National Institute of Standards and Technology.
OCR	Optical Character Recognition.
OTP	One Time Password.
OWASP	Open Web Application Security Project.
QTSP	Prestador Qualificado de Serviços de Confiança (Qualified Trust Service Provider).
RBO	Referência biométrica oficial.
sBIO	Sistema biométrico automático de reconhecimento facial.
SMS	Short Message Service.
ssC	Subsistema interface cliente.
ssF	Subsistema biométrico de comparação facial.
ssID	Subsistema validação documento ID.
ssL	Subsistema biométrico de deteção prova de vida — Liveness detection.
ssR	Subsistema de registo biométrico.
TBID	Template biométrico extraído a partir da fotografia do documento de identificação.
TBL	Template biométrico extraído a dos dados de deteção de prova de vida.
VPN	Virtual Private Network.

3 — Referências:

[1]	ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (V1.2.2).
[2]	ICAO Doc 9303: ICAO Doc 9303 and ISO/IEC 7501 multipart standard: Machine Readable Travel Documents.
[3]	Doc 9303-p9: Machine Readable Travel Documents, Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs, Seventh Edition, 2015, ICAO.

[4]	Doc 9303-p2: Machine Readable Travel Documents, Part 9: Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs, Seventh Edition, 2015, ICAO.
[5]	ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, V2.2.1 (2018-04).
[6]	ISO/IEC 19794-5: Information technology — Biometric data interchange formats — Part 5: Face image data; 2011.
[7]	ISO/IEC 30107-1: Information technology — Biometric presentation attack detection — Part 1: Framework; 2016.
[8]	ISO/IEC 30107-3: Information technology — Biometric presentation attack detection — Part 3: Testing and reporting, 2017.
[9]	ISO/IEC 17025: General requirements for the competence of testing and calibration laboratories, 2017.
[10]	ISO/IEC JTC1 SC17 WG3: TECHNICAL REPORT, Portrait Quality (Reference Facial Images for MRTD), Version 1.0, April 2018, ISO/IEC JTC1 SC17 WG3.
[11]	ISO/IEC 2382-37 — Information technology — Vocabulary — Part 37: Biometrics, Second edition, 2017-02.
[12]	ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements, 2013.
[13]	ISO/IEC 27017 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services, 2015.
[14]	ISO/IEC 27018 — Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, 2019.

4 — Modelo funcional:

Este capítulo apresenta, sob o ponto de vista funcional, o sistema biométrico automático de reconhecimento facial (sBIO), de modo a poder ser facilmente identificado o âmbito, os componentes e as diversas atividades desenvolvidas por cada um destes componentes/sub-sistemas.

O sBIO faz parte integrante do serviço de registo previsto para a implementação dos serviços de emissão de certificados do Prestador Qualificado de Serviços de Confiança (QTSP), descrito na norma ETSI EN 319 411-1 (referência [1]).

A construção deste modelo funcional, teve como objetivo a segmentação lógica /funcional e não representa qualquer exigência de arquitetura física que os Prestadores Qualificados de Serviços de Confiança (QTSP) terão que implementar para cumprir os requisitos aqui previstos.

Para os efeitos definidos neste Despacho, considera-se que o sBIO, deverá ser composto pelos subsistemas enunciados a seguir:

Subsistema de registo biométrico (ssR).

Subsistema interface cliente (ssC).

Subsistema biométrico de verificação facial (ssF).

Subsistema biométrico de deteção prova de vida — liveness detection (ssL).

Subsistema validação documento ID (ssID).

Estes subsistemas interagem, genericamente, de acordo com a figura descrita a seguir:

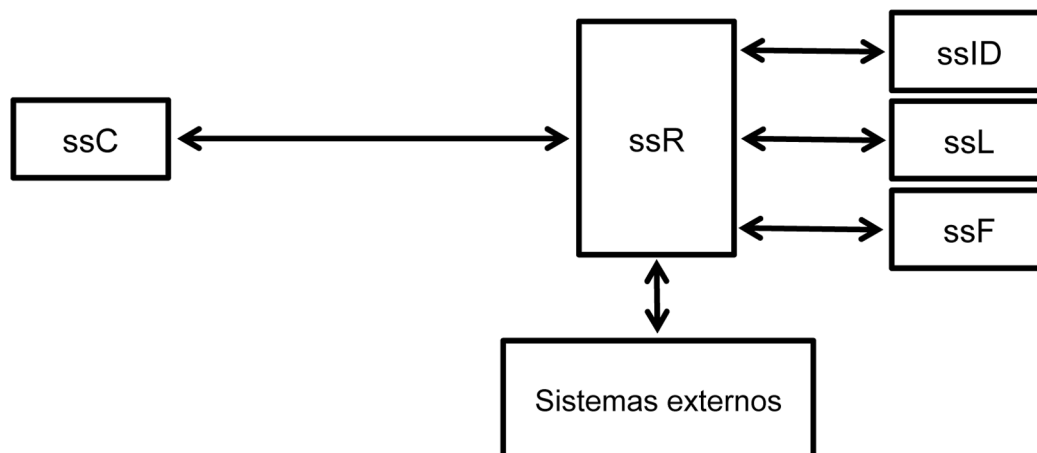


Figura 1 — Relação entre os subsistemas/sistemas externos do sistema sBIO

Estes subsistemas desenvolvem as seguintes ações:

4.1 — Subsistema de registo biométrico (ssR):

Subsistema responsável pelo controlo global de todas as ações desenvolvidas no procedimento de identificação à distância com recurso a sistemas biométricos automáticos de reconhecimento facial.

Este subsistema interage com todos os outros subsistemas, com serviço de registo para emissão de certificados e com os sistemas das autoridades nacionais responsáveis pela emissão do documento de identificação.

4.2 — Subsistema interface cliente (ssC):

Subsistema responsável pela recolha e envio de todos os dados do subscritor, necessários para o procedimento de identificação à distância com recurso a sistemas biométricos automáticos de reconhecimento facial, designadamente, a recolha e envio da(s) fotografia(s) do documento de identificação, a recolha e envio dos dados para a deteção da prova de vida (*liveness detection*).

Nos casos em que o documento de identificação contém informação eletrónica em chip sem contacto (eMRTD em conformidade com as normas ICAO), procede à recolha e envio dos dados constantes no mesmo.

4.3 — Subsistema biométrico de verificação facial (ssF):

Subsistema responsável pela verificação e validação dos dados biométricos recolhidos com a Referência Biométrica Oficial (RBO) existente. Este subsistema desenvolve dois processos de comparação biométrica de um-para-um (1:1).

A comparação principal, em que é feita entre a RBO e o template biométrico TBL, extraído da fotografia (selfie) recolhida para a deteção da prova de vida TBL, e a secundária, realizada entre a RBO e o template biométrico extraído TBID a partir da fotografia que consta na parte visível do documento de identificação.

4.4 — Subsistema biométrico de deteção prova de vida — *liveness detection* (ssL):

Subsistema responsável pela verificação da existência efetiva, em tempo real, do subscritor, devendo garantir que consegue detetar e resistir a ataques de apresentação (*presentation attacks*) biométricos diversos, designadamente, através de fotos, vídeos de alta resolução, máscaras faciais humanas, etc. É também responsável pela extração do template biométrico TBL a partir da fotografia/selfie recolhida.

4.5 — Subsistema validação documento ID (ssID):

Subsistema responsável pela interpretação e validação da autenticidade do documento de identificação oficial apresentado, validando, entre outros, as letras, os algarismos, os símbolos, a *Machine Readable Zone* (MRZ).

É também responsável pela extração do template biométrico TBID, a partir da fotografia do cidadão que consta no documento de identificação recolhida.

5 — Requisitos gerais:

Para os efeitos previstos neste documento, considera-se que a entidade que se submete ao processo de identificação, é uma pessoa física e passa a ser designada de subscritor, a entidade que verifica a identidade do subscritor, é um prestador qualificado de serviços de confiança, designada de QTSP.

Quanto um subscritor, demonstra com sucesso, a existência, posse ou controlo de mais que um mecanismo de autenticação requeridos pelo QTSP para validar a sua identidade, passa a ser designado por titular.

Neste capítulo, pretende-se sistematizar e definir os requisitos do SBIO, bem como os passos necessários para que um subscritor com o seu documento de identificação oficial, em tempo real, proceda uma operação de validação biométrica automática à distância junto do QTSP.

Por último importa realçar e recordar os fatores de segurança fundamentais, que permitem identificar e autenticar alguém de forma remota e que recorrentemente explicitada, por autores especializados na temática, designadamente:

- Algo que a pessoa (cidadão) é;
- Algo que a pessoa tem;
- Algo que a pessoa sabe.

Os referidos fatores estão materializados na figura seguinte.



Figura 2 — Categorias dos fatores de autenticação

5.1 — Requisitos sobre o fluxo do procedimento entre o subscritor e o sBIO

Todas as fases previstas neste fluxo (não necessariamente por esta ordem), devem ser obtidas com SUCESSO, pelo que, sempre que tal não se verifique, o processo de identificação deve ser cancelado.

5.1.1 — Identificação (Registo) do subscritor

5.1.1.1 — Regista telemóvel.

5.1.1.2 — Recebe um código OTP.

5.1.1.3 — Insere código OTP recebido.

5.1.2 — Recolha dos dados do documento de identificação

5.1.2.1 — Obtenção da(s) fotografia(s) em alta definição do documento oficial de identificação, com o detalhe suficiente para a realização das avaliações posteriores.

5.1.3 — Recolha dos dados para deteção de prova de vida

5.1.3.1 — Obtenção da(s) fotografia(s)/selfie(s) de alta definição, com o detalhe suficiente para a realização das avaliações posteriores.

5.1.4 — Recolha dos dados oficiais do cidadão

5.1.4.1 — Esta operação poderá ser efetuada de duas formas, dependendo das circunstâncias:

5.1.4.1.1 — Pelo dispositivo (acionado pelo cidadão), para os casos em que o documento de identificação é um eMRTD.

5.1.4.1.2 — Pelo QTSP, nos casos em que tem a necessária autorização para aceder aos dados oficiais do cidadão, disponibilizados pela entidade pública competente pela emissão.

5.1.5 — Verificação do documento de identificação

5.1.5.1 — Verificação autenticidade do documento de identificação, com recurso a tecnologias automáticas fiáveis. Extração do template biométrico TBID.

5.1.6 — Deteção de prova de vida

5.1.6.1 — Verificação da existência efetiva, em tempo real, do subscritor.

5.1.6.2 — Extração do template biométrico TBL.

5.1.7 — Verificação biométrica do subscritor

5.1.7.1 — Execução de processos de comparação biométrica de um-para-um (1:1) entre a referência biométrica oficial (RBO), com:

5.1.7.1.1 — O template biométrico TBL, extraído dos dados de prova de vida.

5.1.7.1.2 — O template biométrico TBID, extraído da foto do documento de identificação.

5.1.8 — Fator de autenticação secundário

5.1.8.1 — O subscritor introduz um fator de autenticação secundário do seu conhecimento prévio, ou seja, da categoria “Algo que a pessoa sabe”, que não tenha sido transacionado neste procedimento.

5.1.9 — Envio de OTP para fecho de procedimento

5.1.9.1 — O processo de identificação à distância fica concluído, com a introdução de um código OTP recebido para o efeito.

5.1.9.2 — Após conclusão do processo, o subscritor passa a titular e fica na posse das credenciais adequadas para o âmbito ao qual foi requerido o procedimento.

5.2 — Requisitos de segurança

5.2.1 — Organizacionais

Para além das fases tradicionais internacionalmente reconhecidas (por exemplo, a *framework* estabelecida pela OWASP Foundation) de desenvolvimento de produtos/sistemas, o sBIO deve ser implementado e monitorizado, com os seguintes requisitos adicionais:

5.2.1.1 — Incluir um teste piloto, com as seguintes características:

5.2.1.1.1 — O teste piloto é realizado, preferencialmente, em ambiente de produção.

5.2.1.1.2 — Os resultados do teste piloto, devem estar devidamente documentados.

5.2.1.1.3 — Incluir os resultados da avaliação de todos os subsistemas, para todos os processos de identificação dos subscritores, bem como, os dados da *performance* demonstrados.

5.2.1.1.4 — O teste piloto deve ser realizado num universo mínimo de 50 pessoas.

5.2.1.2 — Incluir uma atividade de acompanhamento permanente, com recurso a funcionários do QTSP ou entidade especializada para o efeito, de modo a estabelecer contacto posterior com titular, com o objetivo de confirmar a validade/veracidade das ações realizadas pelo sBIO.

5.2.1.3 — A atividade de acompanhamento é feita por amostragem, acumulativa, com as seguintes características:

5.2.1.3.1 — Até 100 processos, amostragem de 10 %.

5.2.1.3.2 — De 101 a 1000 processos, amostragem de 1 %.

5.2.1.3.3 — A partir de 1001 a 10000 processos, amostragem de 0,1 %.

A partir dos 10001 processos, amostragem de 0,01 %. Por cada intervalo de 10000 processos é verificada/acompanhada uma pessoa.

5.2.2 — Proteção de dados

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

5.2.3 — Avaliação de risco e continuidade do negócio

5.2.3.1 — O QTSP deverá efetuar uma avaliação de risco ao sistema sBIO, que inclua os cenários ataque mais comuns a este tipo de sistemas.

5.2.3.2 — A avaliação de risco deverá ser integrada na avaliação de risco existente para a prestação de serviços de confiança.

5.2.3.3 — O QTSP deverá elaborar um plano de continuidade de negócio para o sBIO.

5.2.3.4 — O plano de continuidade de negócio deverá ser integrado no plano existente para a prestação de serviços de confiança.

5.2.4 — Gestão da segurança

5.2.4.1 — O sBIO deve ser gerido e operado adequadamente, seguindo as melhores práticas internacionais, devendo ser estabelecidas políticas e procedimentos de segurança, com vista à operação segura do mesmo.

5.2.4.2 — O sBIO deve garantir que os serviços disponibilizados, são geridos e operados de forma segura, devendo, o fabricante, para cada um dos subsistemas, disponibilizar a documentação relevante. Considera-se informação relevante, a seguinte.

5.2.4.2.1 — Guias para a instalação dos subsistemas.

5.2.4.2.2 — Guias para a administração dos subsistemas.

5.2.4.2.3 — Guias para a utilização dos subsistemas.

5.2.4.3 — O sBIO deve suportar a implementação de funções com diferentes privilégios.

5.2.4.4 — O sBIO deve disponibilizar e integrar centralmente, no mínimo, as funções/roles de Administrador de segurança, administrador de sistemas e auditor de sistemas.

5.2.4.5 — Cada uma das funções, tem como atribuição genérica, o disposto no “REQ-7.215” da norma ETSI EN 319401(referência [5]).

5.2.4.6 — O sBIO deve conseguir associar os utilizadores às funções.

5.2.4.7 — O sBIO (e subsistemas) devem ter os relógios sincronizados, com os sistemas em uso pelo QTSP para a gestão do ciclo de vida dos certificados.

5.2.4.8 — O sBIO deverá utilizar chaves criptográficas, para garantir as funções de autenticidade, integridade e confidencialidade do sistema e subsistemas. O uso não autorizado, a modificação ou substituição destas chaves poderão resultar numa perda de segurança no sistema como um todo, pelo que as chaves criptográficas utilizadas, devem ser geridas de forma segura durante o seu ciclo de vida. Para o efeito devem estar documentados:

5.2.4.8.1 — Todos os processos criptográficos utilizados.

5.2.4.8.2 — O ciclo de vida das chaves criptográficas utilizadas (geração, arquivo e destruição).

5.2.4.8.3 — A dimensão, algoritmos e esquemas criptográficos utilizados.

5.2.5 — Auditoria e controlo

Cada subsistema deverá gerar registos de auditoria. O QTSP deve documentar quais as ações sujeitas a registos de auditoria.

5.2.5.1 — No mínimo, os subsistemas devem recolher registos de auditoria, sobre as seguintes ações:

5.2.5.1.1 — Os eventos nucleares das funções do subsistema.

5.2.5.1.2 — Eventos relacionados com a gestão das chaves criptográficas.

5.2.5.1.3 — Alteração dos parâmetros e eventos sujeitos a registo.

5.2.5.2 — Os subsistemas devem garantir a integridade e autenticidade dos registos de auditoria.

5.2.5.3 — Os subsistemas devem implementar mecanismos para garantir que não existe destruição não autorizada dos registos de auditoria.

5.2.5.4 — Todos os registos de auditoria, contém, no mínimo, os seguintes parâmetros:

5.2.5.4.1 — Dia e hora do evento.

5.2.5.4.2 — Tipo de evento.

5.2.5.4.3 — Entidade (utilizador, administrador ou processo) responsável pela ação.

5.2.5.4.4 — Sucesso ou falha do evento.

5.2.6 — Performance

O QTSP, deve monitorizar, o desempenho do sBIO (e subsistemas), de modo a determinar, em ambiente de produção, a exatidão da verificação biométrica dos diversos subsistemas, designadamente, as seguintes taxas:

5.2.6.1 — As taxas de falhas nos diferentes tipos de aquisição (FTAR), designadamente:

5.2.6.1.1 — Fotografia(s) do documento de identificação.

5.2.6.1.2 — Detecção da prova de vida.

5.2.6.2 — As taxas de falhas de falsas não-correspondências (FNMR).

5.2.6.3 — As taxas de falhas na classificação dos ataques de apresentação (BPCER).

5.2.7 — Geração de alertas

Os subsistemas devem gerar alertas e notificar em tempo oportuno, sempre que se identifiquem eventos que possam ter impacto significativo na capacidade sistema desenvolver as funções para o qual foi concebido.

5.2.7.1 — O QTSP deverá elaborar e manter atualizada uma política de notificação de alertas, onde esteja previsto quais as situações e respetivas métricas, em que eventuais tentativas de fraude (realizadas por impostor biométrico) ao sistema, são comunicadas às autoridades judiciais nacionais.

No mínimo, devem ser gerados alertas e notificações para os responsáveis do sistema, nos seguintes casos, consoante o subsistema:

5.2.7.2 — Subsistema ssC:

5.2.7.2.1 — Tentativas sucessivas falhadas por parte do mesmo subscritor.

5.2.7.2.2 — Tentativas sucessivas falhadas por parte do mesmo dispositivo.

5.2.7.2.3 — Tempo excessivo na conclusão do processo.

5.2.7.3 — Subsistema ssF:

5.2.7.3.1 — O resultado da comparação entre a RBO e o TBL obtido, é anormalmente díspar.

5.2.7.3.2 — O resultado da comparação entre a RBO e o TBID obtido, é anormalmente díspar.

5.2.7.4 — Subsistema ssL:

5.2.7.4.1 — Sempre que se verifiquem resultados que indiciam uma potencial atividade fraudulenta.

5.2.7.5 — Subsistema ssID:

5.2.7.5.1 — Sempre que se verifiquem resultados indiciadores da utilização de um documento de identificação manipulado.

5.2.8 — Documentos de identificação permitidos

Apenas são permitidos documentos de identificação:

5.2.8.1 — Emitido por autoridade pública competente.

5.2.8.2 — 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.

5.2.8.3 — Em conformidade com a Norma Doc 9303-p2 da ICAO (referência [4]),

Nos casos em que o documento de identificação também incorpore informação eletrónica sobre os dados biográficos, dados biométricos e informação descritiva da emissão, passível de ser recolhida por radiofrequência, conforme indicado em 5.3.4.9:

5.2.8.3.1 — Os mesmos são armazenados num chip sem contacto após assinatura eletrónica dos mesmos.

5.2.8.3.2 — Os mesmos, estão em conformidade com especificações previstas para os eMRTD, na norma Doc 9303-p9 da ICAO (referência [3]).

5.2.9 — Consentimento

5.2.9.1 — Antes da iniciação do processo de identificação por sistema biométrico, 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.

5.2.9.2 — O QTSP deve explicitamente informar o subscritor sobre as condições, termos e duração da informação retida.

5.2.9.3 — Esse consentimento deve ser registado e guardado.

5.2.10 — Comunicação

O QTSP deve disponibilizar publicamente a lista completa dos documentos de identificação aceites para os efeitos previstos neste Despacho.

5.3 — Requisitos específicos

5.3.1 — Sistema biométrico de reconhecimento facial (sBIO)

5.3.1.1 — O processo global de identificação deve poder ser parametrizável, de modo a limitar/interromper a conclusão do processo, pelos seguintes fatores:

5.3.1.1.1 — Duração máxima permitida para realizar o processo.

5.3.1.1.2 — Número máximo de tentativas permitidas por utilizador.

5.3.1.1.3 — Número máximo de tentativas permitidas por dispositivo.

5.3.1.2 — O sBIO deverá eliminar de forma segura todos os dados recolhidos, que contenham informação biométrica, após conclusão do processo (com e sem sucesso).

5.3.1.3 — Exceciona-se a obrigatoriedade de eliminação referida no número anterior, para o caso da fotografia(s) do documento de identificação oficial (DOC), desde que garantidas as seguintes condições:

5.3.1.3.1 — Com o consentimento expresso do subscritor ou por permissão legal expressa.

5.3.1.3.2 — Os dados armazenados não ficam associados ao subscritor.

5.3.1.3.3 — Os dados armazenados são cifrados, utilizando mecanismos criptográficos fortes.

5.3.1.3.4 — O armazenamento é feito por um período máximo de 30 dias.

5.3.1.3.5 — Deve constar na política de retenção de dados em uso pelo QTSP.

Nota. — Esta exceção é incorporada pelo facto de, por regra, os subsistemas ssID estarem assentes em mecanismos de inteligência artificial e de *deep learning*, pelo que, com o objetivo de se tornarem evolutivamente mais robustos, é desejável que possam “apreender” com o maior número possível de registos, daí a “necessidade” de não serem eliminados de imediato.

5.3.1.4 — O sBIO deverá garantir que regista e arquiva de forma segura os resultados de todas as verificações realizadas, com especial incidência:

5.3.1.4.1 — O resultado da verificação entre a RBO e o TBL.

5.3.1.4.2 — O resultado da verificação entre a RBO e o TBID.

5.3.1.4.3 — O resultado da avaliação da deteção prova de vida.

5.3.1.4.4 — O resultado da avaliação da autenticidade do documento de identificação.

5.3.1.5 — De modo a complementar a identificação inequívoca dos subscritores, garantir a utilização de pelo menos, um fator de autenticação adicional, da categoria “algo que a pessoa sabe”, que não tenha sido transacionado durante o processo de identificação.

5.3.2 — Comunicação entre subsistemas e sistemas externos

5.3.2.1 — A transação de dados entre os subsistemas deve ser efetuada com recurso a canais autênticos e seguros.

5.3.2.2 — A autenticidade, integridade e confidencialidade das transações devem ser devidamente asseguradas, através da utilização de protocolos que implementem criptografia “ponta-a-ponta”.

5.3.2.3 — As transações de dados entre os subsistemas e/ou sistemas externos que não se encontrem na mesma rede, devem ser asseguradas através ligações site-to-site VPN IPsec, com recurso a dispositivos em *hardware*, preferencialmente, com certificação CC EAL4+.

5.3.2.4 — Nos casos em que os subsistemas e/ou sistemas externos estão alojados em fornecedores de serviços na nuvem (CSP), é dado cumprimento ao ponto anterior, quando o CSP contratado implementa um programa alargado de conformidade, baseado nos principais referenciais internacionais para serviços na “nuvem”, devendo, no mínimo, ter certificação ativa em:

5.3.2.4.1 — ISO/IEC 27001 (referência [12]).

5.3.2.4.2 — ISO/IEC 27017 (referência [13]).

5.3.2.4.3 — ISO/IEC 27018 (referência [14]).

5.3.2.5 — O requisito previsto no ponto 5.3.2.3 não se aplica às transações entre os subsistemas ssR e ssC.

5.3.3 — Subsistema ssR

5.3.3.1 — O ssR deve garantir o registo inequívoco de cada subscritor, atribuindo um identificador único a cada processo.

5.3.3.2 — Deve ter a capacidade de gerar centralmente e enviar ao subscritor, códigos únicos descartáveis (OTP) de duração limitada, especialmente produzidos para o efeito, através de SMS ou mensagem e correio eletrónico.

5.3.3.3 — Deve agregar os registos de auditoria dos acessos/ações realizados em todos os subsistemas.

5.3.3.4 — Deve permitir visualizar e realizar de forma simples e intuitiva (*user friendly*) consultas filtradas sobre os registos de auditoria referidos no número anterior.

5.3.3.5 — O acesso aos registos de auditoria está disponível apenas aos titulares das funções de auditor de sistemas.

5.3.3.6 — Este subsistema deve estar implementado numa DMZ (*demilitarized zone*), com recurso a BPD (*Firewall*) certificados, com um nível mínimo de CC EAL4+.

5.3.3.7 — A DMZ deve garantir a segregação do tráfego gerado com o subsistema interface cliente (exposto à internet) e o tráfego com os restantes subsistemas

5.3.3.8 — A DMZ deve, preferencialmente, ser implementada com recurso a dois BPD;

5.3.4 — Subsistema ssC

5.3.4.1 — Antes de iniciar o processo de identificação, o ssC deve efetuar os testes necessário no dispositivo, de modo a garantir que as câmaras do dispositivo têm as características e resolução necessária para a recolha da informação necessária.

5.3.4.2 — O ssC deve ser intuitivo, fornecer informação relevante e amigável.

5.3.4.3 — Deve seguir uma metodologia de desenvolvimento adequada, de modo a assegurar que os riscos de falha do sistema sejam mínimos.

5.3.4.4 — Deve implementar mecanismos para comprovar a posse do dispositivo por parte do subscritor.

5.3.4.5 — Deve implementar mecanismos de identificação do dispositivo utilizado pelo subscritor.

5.3.4.6 — Deve permitir a introdução de fatores de autenticação adicionais.

5.3.4.7 — O ssC deve permitir recolher e marcar com a data e hora da recolha, nas condições adequadas, a(s) fotografia(s) do documento de identificação, de modo a garantir:

5.3.4.7.1 — A correta avaliação sobre a sua autenticidade;

5.3.4.7.2 — A extração do template biométrico TBID.

5.3.4.8 — O ssC deve permitir recolher e marcar com a data e hora da recolha, a(s) fotografia(s) do subscritor, de modo a garantir:

5.3.4.8.1 — Uma avaliação inequívoca da deteção da prova de vida.

5.3.4.8.2 — A extração do template biométrico TBL.

5.3.4.9 — Quando aplicável, o ssC deve permitir recolher por radiofrequência os dados constantes no chip sem contacto do documento de identificação eletrónico (eMRTD), de modo a garantir a correta interpretação:

5.3.4.9.1 — Dos dados biográficos.

5.3.4.9.2 — Da referência biométrica RBO.

5.3.4.9.3 — Da informação relativa à emissão.

5.3.4.10 — O ssC deve processar e transmitir para o ssR de forma segura e autêntica:

5.3.4.10.1 — Os dados recolhidos relativos ao documento de identificação.

5.3.4.10.2 — Os dados recolhidos necessários à deteção da prova de vida.

5.3.4.10.3 — Quando aplicável, os dados recolhidos do chip sem contacto do eMRTD.

5.3.5 — Subsistema ssF

5.3.5.1 — Com base nos recursos de digitais obtidos no processo de recolha realizado através do ssC, este subsistema deve efetuar as seguintes verificações biométricas:

5.3.5.1.1 — Principal, entre o referência biométrica RBO e o template TBL.

5.3.5.1.2 — Secundária, entre o referência biométrica RBO e o template biométrico TBL.

5.3.5.2 — O ssF apenas utiliza algoritmos de verificação biométrica facial que tenham sido submetidos a testes independentes de medição da precisão, através de programa de testes internacionalmente reconhecido.

5.3.5.3 — Os testes previstos no ponto anterior devem assegurar valores de exatidão da verificação biométrica (verificações 1:1):

5.3.5.3.1 — Na verificação principal (RBO e TBL), o valor máximo admitido da taxa de falsos negativos (FNMR) é de 4 %, para uma taxa de falsos positivos (FMR) de 0,00001 %, ou seja, FNMR = 4 % @ FMR de 1/10000000;

5.3.5.3.2 — Na verificação secundária (RBO e TBID), o valor máximo admitido da taxa de falsos negativos (FNMR) é de 2 % para uma taxa de falsos positivos (FMR) = 0,0001 %, ou seja, FNMR = 2 % @ FMR de 1/1000000;

5.3.6 — Subsistema ssl

5.3.6.1 — Este subsistema deve estar certificado por entidade acreditada no âmbito da norma ISO/IEC 17025:2017 (referência [9]).

5.3.6.2 — A certificação referida no número anterior, é exigida para artefactos de nível 1 e 2, no âmbito do descrito na norma ISO/IEC 30107-3 (referência [8]).

5.3.6.3 — Tendo em consideração que para este subsistema, é exigida a certificação, nos termos referidos nos números 5.3.6.1 e 5.3.6.2, não serão definidos neste despacho métricas para os valores máximos admitido da taxa de falsos negativos (BPCER), devendo estas referências serem monitorizadas, tal como referido no requisito 5.2.6 deste despacho.

5.3.6.4 — Relativamente aos valores relacionados com a exatidão da verificação biométrica da deteção de prova de vida, considera-se que a taxa de erros de classificação de ataques (APCER), deve ser tendencialmente de zero (0), ou seja, nenhuma tentativa de ataque deve poder ser materializada.

5.3.6.5 — A(s) fotografia(s) recolhidas para efeitos de prova de vida devem ser apagadas após conclusão do processo de identificação;

5.3.6.6 — Deve garantir, a partir da imagem de alta definição da selfie (foto Mugshot), com dimensão mínima de 300 dpi:

5.3.6.6.1 — A extração do template biométrico TBL, com um mínimo de 90 pixels de distância entre os olhos e um tamanho mínimo de 640 kB a 24 bits por pixel.

5.3.6.6.2 — Em conformidade com as especificações estabelecidas na ISO/IEC 19794-5 (referência [6]).

5.3.7 — Subsistema ssID

5.3.7.1 — O ssID, deve estar assente num sistema de reconhecimento de caracteres (OCR), que permita, através das imagens/fotografias dos documentos de identificação extrair:

5.3.7.1.1 — O template biométrico TBID, a partir da fotografia do cidadão, em conformidade com as especificações estabelecidas na ISO/IEC 19794-5 (referência [6]).

5.3.7.1.2 — Letras, algarismos e símbolos constantes no documento de identificação, incluindo a MRZ.

5.3.7.2 — O ssID, deverá ter capacidade para verificar a presença e autenticidade dos mecanismos de segurança ótica do documento de identificação.

5.3.7.3 — O ssID deverá ter capacidade para detetar a adulteração documento de identificação, designadamente, dos dados impressos e da fotografia.

5.3.7.4 — O ssID, deverá ter capacidade para interpretar e verificar a MRZ com os dados relevantes do documento de identificação.

5.3.7.5 — O ssID, deverá ter capacidade de comparação dos dados extraídos, com os dados de emissão oficiais existentes.

ANEXO B

Certificação dos sistemas biométricos automáticos de reconhecimento facial

O prestador qualificado de serviços de confiança (QTSP) que pretenda passar a identificar pessoas físicas através de procedimentos de identificação à distância com recurso a sistemas biométricos de reconhecimento facial, 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 con-



formidade emitido por um organismo de avaliação da conformidade que ateste o cumprimento dos requisitos previstos no Anexo A deste despacho.

Para o efeito, no respetivo relatório deverá constar uma matriz de avaliação que inclua, obrigatoriamente, os seguintes campos.

Requisitos (cap. 5)	QTSP — Descrição do cumprimento	OAC			
		Conformidade		Descrição da avaliação	Metodologia utilizada
		Sim	Não		
5					
5.1					
5.1.1					
5.1.1.1					
5.1.1.2					
5.1.1.3					
5.1.2					
5.1.2.1					
5.1.3					
5.1.3.1					
...					

314017911